



UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Game for Cyber Crime Prevention

Inês Gonçalves Fatelo Lopes

Report to obtain the Master Degree in
Game Design and Development
(2nd Cycle Degree)

Advisor: Prof. Doutor Frutuoso Silva
Co-advisor: Prof. Doutor Pedro Inácio

Covilhã, October 2017

Acknowledgements

At the conclusion point of a great stage of my life, I would like to thank everyone that helped, supported and advised me throughout the journey:

- First of all, I would like to thank my advisor, Professor Frutuoso Silva, and co-advisor, Professor Pedro Inácio, for the opportunity to work in this big and amazing project, for always supporting my ideas and for their availability and help throughout the project;
- A special thanks to TaC and its Executive Director, Professor Yuliya Morenets, for always supporting and believing in this project, for the great advises and for always being receptive to our ideas;
- I would like to thank my family, specially my parents Madalena and Artur, my brother Alexandre and my grandparents for supporting me at all times and believing in my future;
- I would like to thank my wonderful boyfriend Gonçalo for all the love and support given throughout this project, as a partner and as a game developer. I would like to thank him for being my greatest source of motivation, my number one fan and also my number one critic and for always making me strive to be better;
- I would like to thank all my friends for always believing in me, for being supportive and for the stress relieved with the help of your company;
- Lastly, I would like to thank not people, but videogames in general. I feel honored to be able to work in a field that I have loved since I was a little girl. I am also thankful to videogames for always bringing my moral up during the most stressful times of this phase.

Thank you all.

Resumo Alargado

Este resumo alargado tem como objetivo apresentar o conteúdo deste relatório de uma forma detalhada em Língua Portuguesa, visto que o documento está escrito na Língua Inglesa.

Introdução

No primeiro capítulo do relatório é apresentado um resumo do projeto através do seu enquadramento e da discussão da motivação por detrás da escolha do mesmo. Na introdução são apontados os objetivos do projeto, a metodologia utilizada, e os resultados esperados.

Equadramento, Motivação e Objectivos

Atualmente, as tecnologias fazem cada vez mais parte do quotidiano das gerações mais novas da sociedade. Desde bastante novas, as crianças vão tendo contacto com aparelhos como *smartphones* ou tablets e o mundo virtual, nomeadamente a Internet. Chegando à adolescência, estes jovens têm uma vida virtual ativa através dos seus computadores e telemóveis e, muitas vezes, esta não é acompanhada pelos pais (até porque muitos destes não acompanham os avanços tecnológicos). Assim sendo, estes adolescentes estão expostos a várias ameaças informáticas através dos seus dispositivos. Para educar estes jovens, alertando-os dos riscos que podem correr com os seus *smartphones* e na Internet, existem várias organizações e projetos que se focam na cyber-segurança, bem como em alertar os pais e educadores dos mesmos. De modo a suportar as ações pedagógicas sobre cyber-segurança tomadas por este tipo de organizações ou por educadores, pretendeu-se o design e o desenvolvimento de um videojogo direcionado para jovens que aborde as ameaças informáticas a que estes estão expostos e que fomente neles uma melhor conduta online. O objetivo principal deste projeto foi desenhar e desenvolver um protótipo de videojogo para *smartphone* que atente em instruir bons hábitos de cyber-segurança nos jovens e que chame a atenção para os riscos online. Este protótipo servirá como suporte para um conceito de um jogo completo que permita que jovens jogadores consigam, sozinhos, assumir ações responsáveis na Internet.

Trabalhos Relacionados

Atualmente, relativamente à cyber-segurança, existe uma quantidade considerável de videojogos. Porém, a maior parte destes jogos são de carácter totalmente educativo (por exemplo, quizzes) e, dos que não são, há vários jogos que usam a temática da cyber-segurança, mas não transmitem conhecimentos alguns, sendo totalmente lúdicos. Além destes pontos, junta-se o facto de que a vasta maioria destes jogos terem como público-alvo crianças. Relembrando que o público-alvo do projeto são adolescentes, a forma de como os temas são abordados na maior parte dos jogos existentes é infantil e desmotiva jogadores mais velhos. Neste capítulo aborda-se alguns jogos relacionados com o projeto, onde são analisados alguns aspetos positivos e negativos desses jogos já existentes e relevantes para o contexto do projeto. Posteriormente

é apresentada a inovação a que o projeto se propõe relativamente a projetos prévios e é feita uma análise ao público-alvo.

Jogos Relacionados

Dos jogos existentes sobre o tema, há vários que podem ser tomados como referências na evolução do projeto. Do vasto número de jogos são destacados três, seguidamente descritos:

- Digital Compass: [1] Um jogo sobre cidadania digital indicado para crianças dos 9 aos 12 anos. Este jogo permite aos jogadores incorporar vários personagens de cariz jovem com problemas informáticos, em que o jogador pode guiar cada personagem por uma história relacionada com uma temática da cidadania digital, tomando decisões que vão influenciar o desenlace da mesma. No final de cada história existem minijogos relacionados com cada tema. Este jogo foi tomado em consideração pois permite educar o jogador relativamente à cidadania digital através de uma aplicação real da temática e da possibilidade de tomar opções mais ou menos seguras digitalmente.
- Dizigen: [2] Um jogo focado no cyberbullying que tem como alvo o público adolescente. O jogador encarna um personagem que frequenta uma escola onde lhe são lecionados conceitos sobre segurança online. Para além de alguns quizzes sobre o mundo digital feitos ao jogador na sala de aula, a narrativa principal do jogo envolve um amigo do personagem principal que sofre de cyberbullying e cabe ao jogador tomar decisões na narrativa do jogo face ao problema do amigo. Este jogo foi tomado em consideração pois incute boas práticas nos passos a tomar na proximidade de um caso de cyberbullying através de uma narrativa interativa, logo o jogador aprende com as suas ações.
- Cybersecurity Lab: [3] Um jogo que pretende instruir adolescentes na temática da cybersegurança, dando a possibilidade ao jogador de assumir o papel de um trabalhador numa rede social recém-criada, sendo o encarregado da segurança da mesma. Este jogo combina com sucesso a parte teórica com a parte lúdica do jogo e é indicado para um público adolescente. Este jogo foi tomado como referência para o projeto porque, ao colocar o jogador numa posição ativa na cybersegurança de uma empresa, faz com que este ponha os seus conhecimentos à prova e que, ao mesmo tempo, aprenda acerca da temática. Como foi referido anteriormente, tem também uma boa componente lúdica que eleva o jogo educativo a um patamar entusiasmante para o jogador.

Inovação do Projeto

O presente projeto pretende inovar na área em que se insere ao não ser mais um jogo educacional que se foca em testar os conhecimentos do jogador através de perguntas. Para este projeto pretendeu-se desenvolver um jogo que, com uma narrativa imersiva, torne o jogador numa personagem ativa em decisões na realidade da cybersegurança, utilizando conhecimen-

tos previamente adquiridos e também aprendendo novos com o desenlace provocado pelas suas decisões no jogo. O jogo compromete-se a abordar a temática da cyber-segurança aplicando-a a exemplos reais, para que o jogador se possa rever nas situações e desta forma conhecer as melhores práticas a ter.

Análise ao Público-Alvo

O público-alvo deste projeto são os adolescentes, nomeadamente jovens com idades compreendidas entre os 14 e os 17 anos. Considerando o público, foram analisados os jogos mais jogados em plataformas como a PlayStore, a Stream e a Twitch, assim como um trabalho de investigação sobre os jogos mais jogados pelos alunos do Ensino Básico ao Ensino Superior, de forma a perceber os hábitos de jogo deste público. Com os resultados apresentados no trabalho de investigação acima referido, foi possível concluir que 80% dos estudantes do ensino secundário secundário inquiridos (14 a 17 anos) gostariam de usar jogos em atividades escolares. Foi também possível analisar os tipos de jogo que estes gostariam de ver num jogo educacional e concluiu-se que esses tipos de jogo seriam Estratégia, Ação e Aventura.

Game Design

No terceiro capítulo são definidos os temas sobre cibersegurança que vão de encontro aos objetivos do jogo e do público-alvo. Neste capítulo é discutida a conceptualização do jogo, assim como é também estabelecido o design para o mesmo. Tendo em conta a vastidão de temáticas da cibersegurança, foi necessário selecionar os temas mais importantes a abordar no projeto, considerando o público-alvo e a relevância desses temas no dia-a-dia dos jovens. Alguns exemplos dos temas escolhidos são a segurança na utilização de redes sociais, a importância da partilha de informação ou ficheiros pessoais ou a segurança de passwords, entre outros.

Conceptualização do Jogo

Tendo em mente os tipos de jogos referenciados pelo público alvo para jogos educacionais, tentou-se unir esses três tipos de jogos (Estratégia, Ação e Aventura), concebendo a ideia para um jogo de investigação que se encaixa no tema de cibersegurança. Este jogo de investigação abordaria alguns problemas de cibersegurança, apresentando-os como um cibercrime. O jogador assume então o papel de um ciber-detetive e, para ajudar a vítima do crime, deve resolver o caso, jogando alguns minijogos relacionados a temáticas da cibersegurança. A versão completa deste jogo deve conter vários níveis, nos quais cada um representa um caso. O protótipo criado no âmbito deste projeto representa um nível desse jogo completo e deverá servir de modelo para níveis a serem desenvolvidos no futuro.

Design do Jogo Principal

Com o conceito de jogo de detetive mencionado acima em mente, foi feito um game design inicial, o qual foi refinado com a evolução do projeto. Para o desenrolar do caso deste jogo,

foram então estabelecidas as seguintes etapas: Introdução - *cutscene* animada que ilustra as acções que levaram ao cibercrime; Receção do Caso - No departamento de cibersegurança, o jogador, no papel de detetive, aceita o caso e recebe tarefas para cumprir (minijogos); Resolução do Caso - O jogador deve resolver os minijogos para progredir na resolução do caso; Conclusão do Caso - Quando todos os objectivos estiverem cumpridos, uma *cutscene* é apresentada para ilustrar a conclusão do caso.

O que é o jogo?

Este é um jogo de investigação que pretende ensinar cibersegurança a adolescentes.

Onde é que o jogo decorre?

Este jogo passa-se no departamento de cibersegurança da polícia. Este departamento contém uma sala de espera, um escritório principal comum, o escritório da ciber-detetive e um ciber-laboratório com salas de investigação.

O que é que o jogador controla?

O jogador controla a personagem da ciber-detetive do departamento, assim como as suas acções no decorrer da investigação.

Qual é o objetivo principal do jogo?

O objetivo do jogo é resolver ciber-crimes recorrendo a minijogos sobre cibersegurança, minijogos esses que podem ser encontrados nas salas de investigação do laboratório. Para vencer os minijogos o jogador tem de por os seus conhecimentos de cibersegurança em prática.

Enredo do Protótipo

O *ransomware* foi o tema principal escolhido para o cibercrime do nível desenvolvido. Foi então criado um enredo para ligar o crime às etapas da sua resolução, para produzir uma história com lógica. O enredo está dividido em duas partes: a ocorrência do crime, na casa da vítima (um adolescente) e a sua resolução, no departamento de cibersegurança. Decidiu-se que a vítima do crime deveria ser um adolescente, de modo a que o público-alvo do jogo se possa relacionar com o personagem. O enredo corresponde a um caso completo, que é seguidamente explicado:

- 1. Primeira Parte: Ocorrência do Crime (Casa da Vítima):** Um adolescente navega nas redes sociais com o seu *smartphone* e no *feed* de uma rede social encontra um anúncio para um site que vende sapatilhas de marca a um preço incrivelmente baixo. O jovem decide então visitar o site e comprar umas sapatilhas. Antes de deixar o jovem avançar com a compra, o site propõe um desconto de 10% na compra se o rapaz descarregar uma aplicação. Sem suspeitar, o jovem descarrega e instala a aplicação. Depois da instalação, o jovem é surpreendido com uma mensagem de *ransomware*. Esta mensagem declara ter

encriptado todos os ficheiros do dispositivo e exige o pagamento de uma quantia alta de dinheiro em troca da password de descriptação. Assustado, o jovem decide ir procurar ajuda na polícia.

2. **Segunda Parte: A Resolução do Crime (Departamento de Segurança):** O adolescente explica a situação à ciber-detetive e pede-lhe ajuda, ao que esta aceita. A detective decide então analisar a rede social do adolescente para encontrar o anúncio para o site malicioso. Para alcançar esse objetivo, o jogador tem de resolver o minijogo das redes sociais, no qual é confrontado com situações de partilha de informação nas redes sociais. Depois de resolver o minijogo das redes sociais, a detective decide então investigar o site malicioso e os seus sinais de *phishing*, de forma a descobrir os seus criadores. Para isso, o jogador tem de completar o minijogo de deteção de *Phishing*, no qual é confrontado com várias situações onde tem de encontrar sinais que indiquem esquemas de *phishing*. Depois de passar o minijogo anterior, obtém acesso a informação dos possíveis suspeitos do crime. Assim, com conhecimento dos criadores do site e de informações pessoais dos mesmos, a detetive tenta descobrir a password para descriptar os ficheiros do jovem. Para isso, o jogador tem de resolver o minijogo das Passwords, no qual o jogador é confrontado com a temática da criação de passwords seguras. Depois de resolver os três minijogos, a detective consegue finalmente descriptar os ficheiros do adolescente e limpar o *ransomware* do seu *smartphone*. O dispositivo é então devolvido ao adolescente.

Minijogos

Com o enredo estabelecido, foi possível escolher os temas dos minijogos de forma a se encaixarem na história, como são listados seguidamente:

- **Minijogo das Redes Sociais:** Para permitir ao jogador testar os seus conhecimentos, a ideia para este jogo foi colocar o jogador a tomar decisões relativamente a escolhas seguras no que toca a aceitar pedidos de amizade, responder a mensagens e fazer publicações nas redes sociais.
- **Minijogo do *Phishing*:** Para testar a capacidade do jogador na deteção de sinais de tentativa de *phishing*, este jogo apresenta alguns ecrãs de e-mails e sites com esta tentativa de fraude e é pedido ao jogador que encontre os sinais suspeitos.
- **Minijogo das Passwords:** De forma a demonstrar, de maneira simplificada, o processo que os *hackers* usam para decifrar palavras-chave. Neste jogo, o jogador deve, com elementos de informação pessoal de alguns *hackers*/suspeitos, com uma lista das 10 palavras de dicionário mais utilizadas em passwords e uma lista das 10 passwords mais comuns, tentar decifrar palavras-chave.

Desenvolvimento do Protótipo

O quarto capítulo deste documento contém informação acerca de todos os componentes do protótipo desenvolvido, apresenta todas as ferramentas utilizadas para o projeto, enumera as funcionalidades do jogo e dos seus minijogos, descreve o mundo do jogo e as suas localizações-chave, apresenta os personagens do jogo, clarifica a sua interface, ilustra as animações cinemáticas e explica a jogabilidade.

Testes

Para avaliar a qualidade do protótipo e a sua eficácia na aprendizagem sobre o tema da cibersegurança, foram implementados alguns testes ao público-alvo do projeto. No quinto capítulo deste documento são analisados os resultados desses testes, mais concretamente testes de experiência do utilizador e testes para avaliar eficiência do jogo a ensinar conteúdos sobre cibersegurança.

Os testes foram aplicados numa escola a alunos do 9º ano, com idades compreendidas entre 14 a 17 anos (o segmento alvo deste projeto). Os alunos foram submetidos a um teste de conhecimentos duas vezes, uma antes de jogarem o jogo e outra depois de jogarem.

Os estudantes foram acompanhados enquanto jogavam o jogo e puderam fazer comentários acerca da sua experiência com o mesmo. Depois de jogar, estes alunos responderam a um questionário de forma a avaliar o jogo. Com os resultados destes questionários foi possível avaliar a qualidade da experiência de utilizador do jogo. Com os resultados dos testes de conhecimentos, foi possível analisar a evolução feita pelos estudantes depois de jogarem o protótipo. Foi possível concluir que, apesar da falta de noção dos perigos cibernéticos, os jovens mostram interesse e preocupação face à cibersegurança e a perigos online. Conseguiu-se também verificar uma melhoria nos resultados dos testes de conhecimento feitos pelos alunos. Pode-se com isso concluir e confirmar que o protótipo pode ser usado não só como jogo, mas como ferramenta de ensino, pois consegue lecionar conceitos sobre cibersegurança de uma forma mais cativante para os alunos e recorrendo às tecnologias que os jovens tanto gostam e usam no seu dia-a-dia..

Conclusões

No sexto e último capítulo são apresentadas as conclusões principais do projeto, assim como são propostas algumas melhorias como trabalho futuro.

Com este projeto foi possível conceptualizar a ideia de um jogo de investigação sobre cibersegurança para adolescentes e desenvolver um protótipo de um nível desse mesmo jogo. O protótipo foi testado com o público-alvo e foi provado que este contribui para aumentar o conhecimento dos jovens acerca de cibersegurança, tornando o protótipo numa boa base para a criação de um jogo completo. Como principal trabalho futuro, para além de um ou outro melhoramento do nível desenvolvido, pretende-se a criação do jogo completo, ou seja, mais níveis que abordem

as várias temáticas identificadas como importantes a ser leccionadas sobre a cibersegurança para o público-alvo.

Abstract

Technologies are increasingly becoming a part of the daily lives of younger generations and with no supervised usage of these technologies, teenagers are exposed to various threats. To create awareness in the youth, an educational game about cyber-security was designed and a game prototype was created. The game designed was a detective game, where the player takes the role of a detective to investigate a cyber-crime and to solve the case the player must play several mini-games. Each mini-game has a specific thematic about cyber-security, for example, sharing information in social networks, phishing and the importance of creating strong passwords. In these mini-games the player makes decisions and learn based on that. This prototype was tested by teenagers and there was an improvement of their cyber-security knowledge. A cyber-security educational game may grow cyber-security awareness in younger generations.

Keywords

Cyber Crime Prevention, Cyber Security, Game Prototype, Smartphone Educational Videogame, Detective Game, Minigames, Unity, Blender, Game Design, Game Development, Ransomware, Phishing, Social Network Secure Usage, Password Security, Cyber Security Learning

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 1 |
| 1.1 | Scope and Motivation | 1 |
| 1.2 | Objectives | 1 |
| 1.3 | Methodology and Expected Product | 2 |
| 1.4 | Report Structure | 2 |
| 2 | Related Work | 5 |
| 2.1 | Introduction | 5 |
| 2.2 | Related Games | 5 |
| 2.2.1 | Digital Compass | 5 |
| 2.2.2 | Digizen | 6 |
| 2.2.3 | Cybersecurity Lab | 6 |
| 2.3 | Innovation of Project | 9 |
| 2.4 | Target Audience Analysis | 9 |
| 2.5 | Conclusions | 9 |
| 3 | Game Design | 11 |
| 3.1 | Introduction | 11 |
| 3.2 | Themes Selection | 11 |
| 3.3 | Concept | 12 |
| 3.4 | Game Design Overview | 12 |
| 3.4.1 | Initial Draft and Evolution | 12 |
| 3.4.2 | <i>What is the game?</i> | 13 |
| 3.4.3 | <i>Where does the game take place?</i> | 14 |
| 3.4.4 | <i>What does the player control?</i> | 14 |
| 3.4.5 | <i>What is the main focus?</i> | 14 |
| 3.5 | Prototype Storyline | 14 |
| 3.6 | Mini Games | 15 |
| 3.6.1 | Social Network Mini Game | 15 |
| 3.6.2 | Phishing Detector Mini Game | 15 |
| 3.6.3 | Password Decoder Mini Game | 16 |
| 3.7 | Conclusions | 16 |
| 4 | Prototype Development | 17 |
| 4.1 | Introduction | 17 |
| 4.2 | Development Tools | 17 |
| 4.2.1 | <i>Storyboard That</i> | 17 |

| | | |
|----------|---|-----------|
| 4.2.2 | <i>Unity</i> | 17 |
| 4.2.3 | <i>Blender</i> | 17 |
| 4.2.4 | <i>Vegas Pro 13</i> | 18 |
| 4.2.5 | <i>Microsoft PowerPoint</i> | 18 |
| 4.3 | Game World | 18 |
| 4.3.1 | Key Location 1: Cyber Detective Office | 18 |
| 4.3.2 | Key Location 2: Cyber-security Department Common Room | 19 |
| 4.3.3 | Key Location 3: Cyber Laboratory | 20 |
| 4.3.4 | Key Location 4: Password Room | 22 |
| 4.3.5 | Key Location 5: Social Networks Room | 23 |
| 4.3.6 | Key Location 6: Phishing Room | 24 |
| 4.3.7 | Cutscene Location 1: Teen Room | 24 |
| 4.3.8 | Cutscene Location 2: Police Station Outdoor | 25 |
| 4.4 | Game Characters | 26 |
| 4.4.1 | The Teenager | 26 |
| 4.4.2 | The Cyber-security Detective | 26 |
| 4.5 | User Interface | 27 |
| 4.5.1 | Camera of the Game | 27 |
| 4.5.2 | User Interface Detail 1: Starting Menu | 28 |
| 4.5.3 | User Interface Detail 2: Walking Joystick | 28 |
| 4.5.4 | User Interface Detail 3: Rotation Joystick | 29 |
| 4.5.5 | User Interface Detail 4: Missions Window | 29 |
| 4.5.6 | User Interface Detail 5: Mission Markers | 30 |
| 4.5.7 | Mini game User Interfaces: <i>Social Network Analysis</i> | 31 |
| 4.5.8 | Mini game User Interfaces: <i>Phishing Detector</i> | 32 |
| 4.5.9 | Mini game User Interfaces: <i>Password Decoder</i> | 32 |
| 4.6 | Animated Cutscenes | 33 |
| 4.6.1 | Initial Cutscene | 33 |
| 4.6.2 | Ending Cutscene | 34 |
| 4.7 | Gameplay | 35 |
| 4.7.1 | Main Victory Conditions | 35 |
| 4.7.2 | Victory Conditions: <i>Social Network Analysis</i> | 35 |
| 4.7.3 | Victory Conditions: <i>Phishing Detector</i> | 35 |
| 4.7.4 | Victory Conditions: <i>Password Decoder</i> | 36 |
| 4.8 | Conclusions | 36 |
| 5 | Tests | 37 |
| 5.1 | Introduction | 37 |
| 5.2 | Usability Tests | 37 |

| | | |
|----------|--|-----------|
| 5.3 | Education Efficiency | 39 |
| 5.4 | Conclusions | 41 |
| 6 | Conclusions and Future Work | 43 |
| 6.1 | Main Conclusions | 43 |
| 6.2 | Future Work | 43 |
| | Bibliografia | 45 |
| A | Preliminary Storyboard | 47 |
| A.1 | Interactive Narrative | 47 |
| A.2 | Detective Game | 49 |
| B | Plot Storyboard | 53 |
| C | Social Network Notifications List | 57 |
| C.1 | Friend Requests | 57 |
| C.2 | Messages | 59 |
| C.3 | Scheduled Posts | 60 |
| D | Phishing Detector Screens List | 61 |
| E | Password Decoder - Password Elements Lists | 63 |
| E.1 | Suspects | 63 |
| E.2 | Top 10 Most Common Used Passwords | 63 |
| E.3 | Top 10 Dictionary Words Most Used in Passwords | 64 |
| F | Knowledge Quiz | 65 |
| G | Questionnaire | 71 |

List of Figures

| | | |
|------|---|----|
| 2.1 | Screen of an interactive moment of one of the Digital Compass game stories. . . | 6 |
| 2.2 | Digizen game screen - interaction via quiz. | 6 |
| 2.3 | CyberLab game screen for the server protection against cyber attack game, showing a tutorial for a virus attack. | 7 |
| 2.4 | CyberLab Game Screen of the programming challenge. | 7 |
| 2.5 | CyberLab game screen: presentation of results for the decipher passwords challenge. | 8 |
| 2.6 | CyberLab game screen for the social engineering challenge, namely for distinguishing the website of Google from a phishing attempt. | 8 |
| 4.1 | Rendered images of the model of the Cyber Detective Office. | 19 |
| 4.2 | Examples of American police station interiors which the department was based on. | 19 |
| 4.3 | Rendered images of the model of the Cyber-security Department Common Room. | 20 |
| 4.4 | Examples of sci-fi/Futuristic laboratories of which the cyber laboratory was based on. | 21 |
| 4.5 | Rendered images of the model of the Cyber Laboratory. | 21 |
| 4.6 | Image of the <i>matrix raining code</i> , from which the walls from the Password Room were based of. | 22 |
| 4.7 | Rendered images of the model of the Phishing Room. | 23 |
| 4.8 | Rendered images of the model of the Social Networks Room. | 23 |
| 4.9 | Rendered images of the model of the Phishing Room. | 24 |
| 4.10 | Rendered images of the model of the Room of the Teen. | 25 |
| 4.11 | Police station images. | 25 |
| 4.12 | Elaine, Porl and Ed, from left to right, the characters from the Cartoon Character Pack 1 [4]. | 26 |
| 4.13 | Rendered images of the game characters. | 27 |
| 4.14 | Illustrative image of the camera perspective of the game. | 28 |
| 4.15 | Screenshot showing the interface of the starting menu. | 28 |
| 4.16 | Close-ups of the game joysticks. | 29 |
| 4.17 | Screenshots of the Missions button and window. | 30 |
| 4.18 | The Back to Menu Dialog boxes. | 30 |
| 4.19 | Screenshots showing the different mission markers. | 31 |
| 4.20 | The <i>Social Network Analysis</i> mini game main interface. | 31 |
| 4.21 | The <i>Phishing Detector</i> mini game main interface. | 32 |
| 4.22 | The <i>Password Decoder</i> mini game main interface. | 33 |
| 4.23 | Illustrative frames of the initial cutscene. | 34 |
| 4.24 | Illustrative frames of the ending cutscene. | 34 |

| | | |
|-----|--|----|
| A.1 | Storyboard images illustrating the interactive narrative idea. | 48 |
| A.2 | Storyboard images illustrating the Detective Game idea. | 52 |
| B.1 | Storyboard images illustrating the prototype plot. | 55 |
| C.1 | Possible friend request notifications. | 58 |
| C.2 | Possible message notifications. | 59 |
| C.3 | Possible scheduled post notifications. | 60 |
| D.1 | Possible Phishing screens. | 61 |

List of Tables

| | | |
|-----|--|----|
| 5.1 | Flow of the Game Evaluation - Results | 38 |
| 5.2 | Thematic of the Game Evaluation - Results | 38 |
| 5.3 | Graphics and Mini Games Evaluation - Results | 39 |
| 5.4 | Didactic Evaluation - Results | 39 |
| 5.5 | Quiz Scores Improvement per Question | 40 |
| 5.6 | Ordered Quiz Scores Improvement | 40 |

Acronyms

| | |
|------------|---|
| GDD | Game Design Document |
| TaC | Together against Cybercrime International |
| UBI | Universidade da Beira Interior |
| UI | User Interface |

Glossary

cutscene In-game cinematic or in-game movie plural. 13

Game Design Document Highly descriptive dynamic design document of the design for a video game plural. 13

joystick Input device, consisting of a stick that pivots on a base, that reports its angle or direction to the device it is controlling plural. 28

Likert Scale Scale commonly involved in research that employs questionnaires, most widely used to scale responses in survey research. When responding to a Likert item, respondents specify their level of agreement or disagreement on a symmetric agree-disagree scale for a series of statements. 37

phishing Attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. 15

pop-up Graphical control element subordinate to an application's main window plural. 15

ransomware Type of malicious software that threatens to publish the data of the victim or perpetually block access to it unless a ransom is paid. 11

storyboard Graphic organizer in the form of illustrations or images displayed in sequence for the purpose of pre-visualizing a motion picture, animation, motion graphic or interactive media sequence plural. 3

Chapter 1

Introduction

The first chapter of this document briefly presents the subject of the project, its scope and motivation, in section 1.1, in section 1.2 its objectives and the methodology used and the expected product of this project, in section 1.3. Lastly, section 1.4 contains a brief discussion of the structure of the report.

1.1 Scope and Motivation

Nowadays, technologies are increasingly becoming a part of the daily lives of younger generations of our society. Since a young age, children have contact with devices such as smartphones or tablets and the virtual world, namely the Internet. When they reach adolescence, these young people have an active virtual life through their computers and mobile phones, and this is often not accompanied by their parents (sometimes because many of them do not keep up with technological advances). As such, these teens are exposed to various computer threats through their devices. To educate the young and create awareness of the risks of smartphones and the Internet, there are several organizations and projects that focus on cyber-security and create awareness between parents and educators. Together against Cybercrime International (TaC) [5] is an example of one of these cyber-crime fighting organizations. In the context of the collaboration protocol between TaC and the Universidade da Beira Interior (UBI) and to support the pedagogical actions on cyber-security taken by this type of organizations or by educators, there was the intention to design and develop a smartphone video game addressing young people that discourses computer threats to which teenagers are exposed and to encourage a better online behavior.

1.2 Objectives

The project main goal is the design and development of a video game prototype that reinforces the cyber-security culture among young people and make them more aware of the risks and responsibilities online, eventually by turning them into active actors in the process. This prototype will serve as support for a complete game that will allow youngsters to take responsible actions on the Internet autonomously. This game must be developed for different mobile platforms and must be developed in two or three languages. A secondary goal is to define and apply a testing protocol to evaluate and fine-tune the game during field trials and to write a conference paper for dissemination.

1.3 Methodology and Expected Product

For the project to reach its proposed objectives in its due time, it was necessary to have a plan organizing the tasks to be executed. The proposed work plan was:

1. Get to know the project subject, identify the necessary tools and establish the project environment basis;
2. Research and description of the state-of-art and related works;
3. Game conceptualization and preliminary design;
4. Game prototyping and initial usability tests;
5. Game prototype improvement based on the tests and feedback from the audience;
6. Report writing.

According to the aforementioned plan, This project aims to deliver a video game prototype and a report on the project.

1.4 Report Structure

The main body of this report has six chapters, whose contents can be described in the following way:

- The first chapter, **Introduction**, starts with a brief introduction about the project, presents its scope and motivation, explains the methodology and product expected of this project and describes the report structure;
- The second chapter, **Related Work**, discusses the related works of the project, presents the innovation proposed by this project and analyses the target audience;
- The third chapter, **Game Design**, specifies the cyber-security subjects to be addressed in the project, illustrates the game main concept and defines the main and prototype game designs;
- The fourth chapter, the **Prototype Development**, describes and clarifies all the components of the prototype of the project;
- The fifth chapter, **Tests**, analyses the results of Usability Experience tests applied to the target audience and evaluates the educational component of the game;

- The sixth chapter, **Conclusions and Future Work**, ends this report, drawing some conclusions about the project, what can be done and improved in the future and what can derive from it;
- The **Appendix A** contains storyboards representing the preliminary game design of the project;
- The **Appendix B** contains a storyboard illustrating the plot of the prototype;
- The **Appendix C** contains lists of images of the possible notifications that the player can come across with in the *Social Network Analysis* Mini Game;
- The **Appendix D** contains lists of images of the possible screens that the player can come across with in the *Phishing Detector* Mini Game;
- The **Appendix E** contains lists of elements that the passwords of the mini game *Password Decoder* might contain;
- The **Appendix F** illustrates the Knowledge Quiz taken by students in order to test their knowledge about cyber-security;
- The **Appendix G** illustrates the questionnaire answered by students in order to evaluate the prototype.

Chapter 2

Related Work

2.1 Introduction

Nowadays there is a considerable amount of video games on the cyber-security subject. However, most of these games have a completely academic nature (for example, quizzes) and, from those that are not like that, there are several games that use cyber-security as the theme but do not provide any kind of knowledge as collateral, being merely playful. In addition to these points, there is also the fact that most of these games target young children. The target audience of the current project is teenagers. Therefore, the way that the topics are addressed in some of these games is childish and demotivates older players. This chapter deals with the related work of this project, in section 2.2, where some positive and negative aspects of already existing works that are relevant to the context of the project are discussed and where is presented the innovation proposed by this project, in section 2.3. Subsequently, in section 2.4, there will be a brief analysis of the target audience.

2.2 Related Games

Of the existing games about the theme, there are several that can be taken as examples in the evolution of the project. For example, there are three that stand out from the others. They are analyzed in the subsections below.

2.2.1 Digital Compass

Digital Compass [1] is a digital citizenship game addressed for children from 9 to 12 years old. This game allows players to impersonate young characters with computer problems. The player can guide each character through a story related to a theme of digital citizenship, making decisions that will influence the outcome of the story (illustrated in figure 2.1). At the end of each story there are mini games related to each theme. This game, although it is not addressed to the target audience of this project, should be considered as it allows the player to educate itself about digital citizenship through a real application of the theme and gives the player the possibility of taking its own safety choices digitally.



Figure 2.1: Screen of an interactive moment of one of the Digital Compass game stories.

2.2.2 Digizen

Digizen [2] is a game focused on cyberbullying, and unlike the game presented above, it targets teenagers. The player impersonates a character who attends a school where it is taught notions about online safety. In addition to some quizzes about the digital world (illustrated in figure 2.2), made to the player in the classroom, the main narrative of the game involves the friend of the main character, who suffers from cyberbullying. It is up to the player to make decisions in the game narrative, considering the problem of its friend. This game, as mentioned above, should be considered as it introduces good practices in proximity of a cyberbullying case through an interactive narrative, where the player learns from its actions.

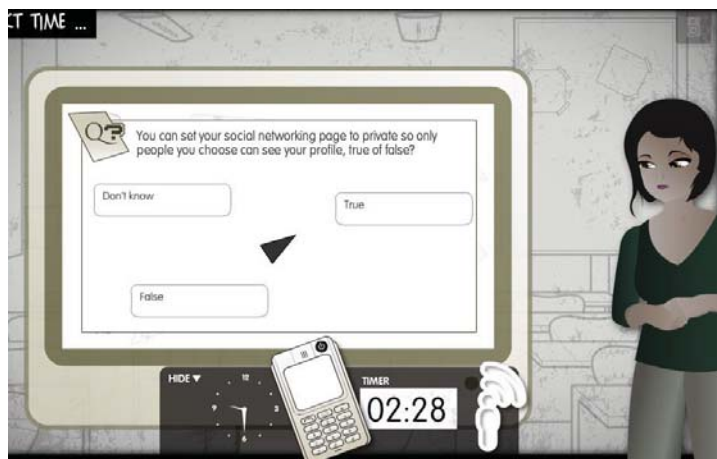


Figure 2.2: Digizen game screen - interaction via quiz.

2.2.3 Cybersecurity Lab

Cybersecurity [3] Lab is a game whose goal is to educate teenagers on the cyber-security issue, giving the player the possibility to assume the role of a newly created social network worker, supervising its security. From the games presented in this section, this is the game that best

combines the theoretical part with the playful part of the game and that is more suitable for a teen audience, therefore it is important to analyze this game. It consists of 4 mini games, which are:

- **Server Protection against Cyber Attack Game** - when an attack of a certain type occurs, the player must protect the network of the company using the coins earned in other mini games (illustrated in figure 2.3). Each coin protects one of the 6 network ports. Each attack strikes the network in 3 aspects, each of them has two respective ports. The player must choose, using cyber-security knowledge, the ports that he must protect to lose the minimum number of users. This game aims to test the knowledge of the player regarding cyber-security flaws in computer networks;

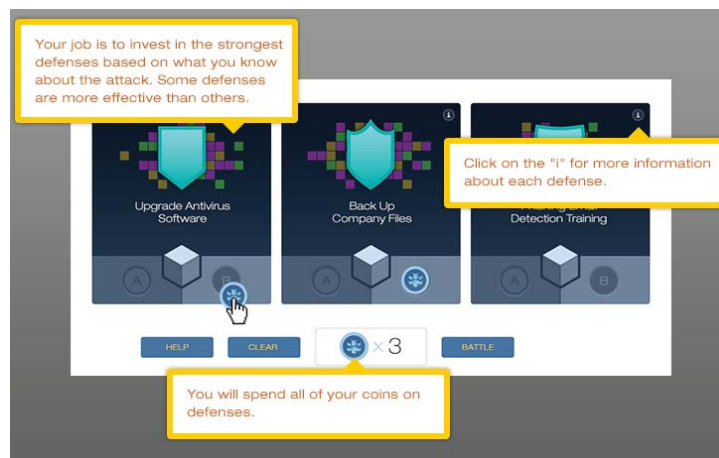


Figure 2.3: CyberLab game screen for the server protection against cyber attack game, showing a tutorial for a virus attack.

- **Programming Challenge:** With the help of code blocks, the player must create a program that allows a figure to cross a map (illustrated in figure 2.4). This game aims to introduce programming logic in the player;

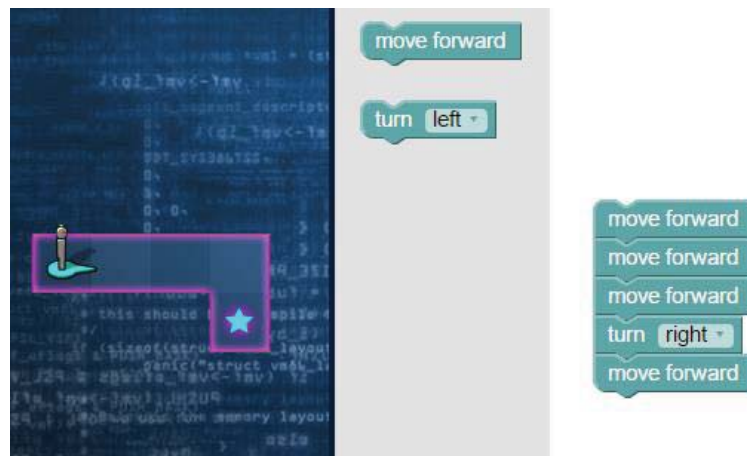


Figure 2.4: CyberLab Game Screen of the programming challenge.

- **Decipher Passwords Challenge** - the player is challenged by a spy from within the company to a password battle, in each chooses a password and then tries to unravel the password of the opponent (illustrated in figure 2.5), following certain methods used by hackers (for example, using the list of the 10 most used passwords to try to compromise the password). This game instills in the player better practices in choosing a safe keyword;

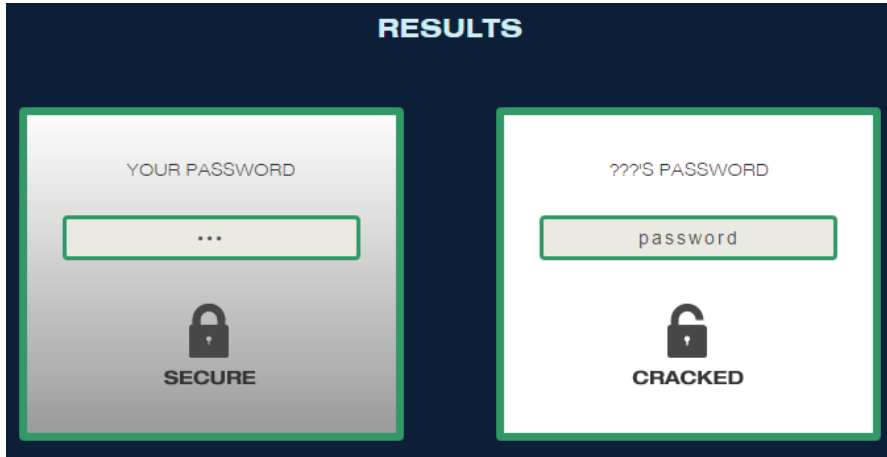


Figure 2.5: CyberLab game screen: presentation of results for the decipher passwords challenge.

- **Social Engineering Challenge:** In a game similar to a *discover the differences* one, the player must find the differences between e-mails, websites, etc. and phishing attempts (illustrated in figure 2.6). This game educates the player regarding phishing signals that may be found in suspicious e-mails, websites, etc.

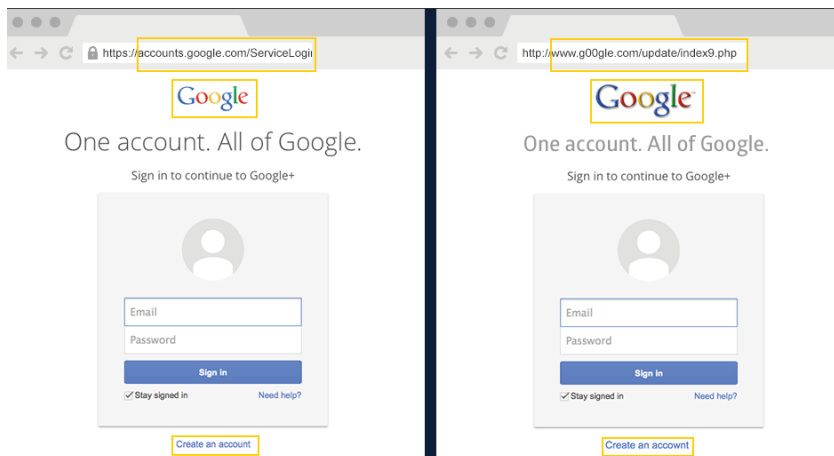


Figure 2.6: CyberLab game screen for the social engineering challenge, namely for distinguishing the website of Google from a phishing attempt.

This game should be taken as a reference for the project because, by placing the player in an active position of the cyber-security department of a company, he tests his knowledge and learns about the subject. As mentioned before, it has a good playful component that takes this educational game to an exciting level for the player.

2.3 Innovation of Project

The game produced for this project aims to innovate in the cyber-security area as it will not merely be an educational game that focuses on testing the knowledge of the player through questions, like most games on the subject. It is envisioned the development of a game that, with an immersive narrative, makes the player an active character in decisions on the cyber-security reality, using previously acquired knowledge and learning new things with the outcome caused by its decisions in the game. The game is committed to address the issue of cyber-security applying it to real examples, so that the player can see itself in the situations and thus know the best practices to have. The game also wants to demonstrate to the young player that cyber-crime is punished and that it is possible to punish cyber-criminals.

2.4 Target Audience Analysis

The main audience of this project are teenagers, particularly young between the ages of 14 and 17. Considering this audience, the top games on platforms like PlayStore, Steam and Twitch were analyzed, as well as the paper *Os jogos mais jogados pelos alunos do Ensino Básico ao Ensino Superior (Students from Basic to Higher Education Most Played Games*, in the English language) [6], to understand the gaming habits of the audience age group. Based on the results presented by the paper referred, it is possible to conclude that over 80% of surveyed secondary school students (ages 14 to 17 years old) would like to use games in school activities. It is also possible to analyze values from a survey about the preferred type of games for teaching subjects content. It was concluded that the favored three types of game that youngsters in this age group would most like to see in an educational game would be Strategy, Action and Adventure.

2.5 Conclusions

In this chapter, related works on cyber-security games were analyzed. With the breakdown of some existing related games, it was possible to establish guidelines for the continuation of this project and to define where it should stand out. By investigating the target audience and its gaming habits, it was easier to pick the right direction to follow regarding the game type.

Chapter 3

Game Design

3.1 Introduction

This chapter specifies, in section 3.2, the cyber-security subjects that fit with the goals and audience of the project. The game main concept, in section 3.3, and the first design drafts, in section 3.4, are also discussed. Finally, the game design for the main game and for the prototype to be developed is also established, in sections 3.5 and 3.6.

3.2 Themes Selection

Since the cyber-security theme is so vast, it was necessary to select the most significant subjects to be addressed in the planned game, considering the target audience and the relevance of the subjects in the daily life of teenagers. Together with Prof. Doutor Pedro Inácio and the Executive Director of TaC [5], Ms. Yuliya Morenets, a list with some of the most relevant topics of cyber-security for teenagers was established. This list is presented below:

1. Talking with Strangers in Social Networks;
2. Sharing Information in Social Networks;
3. Understanding the Dimension of Personal Data in Smartphones;
4. Passwords Management;
5. Dangers related with the webcam and microphone;
6. Ransomware (and Malware in general);
7. Online Piracy;
8. Privacy and the Internet;
9. Using Internet in Public Places;
10. Cyberbullying.

Due to the capacity of relating some themes listed above, such as numbers **1,2 and 10** (Social

Network Issues), 3 (Personal Data Importance), 4 (Passwords Management) and 6 (Ransomware) it was possible to draw a coherent storyline approaching these topics for the prototype of the project, clarified in the following sections.

3.3 Concept

Bearing in mind the conclusions drawn from section 2.4 about the preferred game types of adolescents for educational games, the three game types (Strategy, Action and Adventure) were combined, conceiving the idea for an investigation game, that would well fit in the cyber-security theme. This investigation game will connect some cyber-security issues and present them as a cyber-crime. The player then assumes the role of a cyber-detective and, to help the victim of the crime, should solve the case, winning some mini games related to some cyber-security themes mentioned in section 3.2. This strategy is proposed by Barbosa et al., 2014 in their paper entitled *A New Methodology of Design and Development of Serious Games* [7]. The full version of the game should contain numerous levels, in which each one represents a case. The full game should approach the totality of the topics listed in section 3.2. The prototype created in the scope of this project will probably be one level of this complete game and should serve as a model for the development of other levels.

3.4 Game Design Overview

"If we want to increase the appeal of our games, it is necessary to understand what makes an experience entertaining, and how such an experience can be created. The discipline that tries to answer these questions is called game design." Jurie, 2007 [8].

The main objective for this game design of the project was to offer the player an exciting experience while learning didactic content.

3.4.1 Initial Draft and Evolution

With the detective game concept mentioned in the previous section in mind, it was **initially** drawn the following list of stages for the unfolding of each case:

1. Introduction - introduction of the case where the victim can be observed taking the steps leading to it getting caught in a cyber-crime; the player is only observer at this moment;
2. Case Acceptance - in the role of the detective, the player accepts the case presented in the introduction and receives some data related to it;
3. Clues Search - the player investigates the devices of the victim to find clues about the crime;

4. Clues Analysis - In the cyber-security department, it is possible to access a cyber-laboratory where there are specific rooms to analyze each type of evidence; in these rooms the player must win some mini games related to the theme of the room to complete the analysis;
5. Case Conclusion - with all clues analyzed, the player assembles the information and discovers the criminal behind the cyber-crime, punishing him;
6. Side Game (Throughout the Game) - the player has an artificial intelligence assistant that can provide tips to help with case resolution; this assistant needs maintenance (for example, the player must run the antivirus in the software of the assistant) and the better its state, the better tips given.

A group of preliminary storyboards were created to exemplify a possible game use. These can be seen in the appendix A, made with help of Storyboard That, explained in the subsection 4.2.1. The cases game design was refined during the prototype development. The **final design** of the game stages is described as follows:

1. Introduction - animated cutscene illustrating the actions that led to a cyber-crime;
2. Case Acceptance - in the cyber-security department, the player, in the role of detective, accepts the case and objectives to accomplish (mini games);
3. Case Solving (mini games) - the player must solve some mini games to progress in the case solving;
4. Case Conclusion - Once all the objectives of the game are completed, a cutscene is presented, illustrating the resolution of the case.

As it can be seen, the points *Clues Search* and *Clues Analysis* from the initial design have been combined into the *Case Solving* point in the current design, the essential stage of this game because it is where all the action takes place. It is also important to mention that Case Conclusion purpose changed: at first, the case ended with the detection and arrest of the criminal, which in reality is not always possible. The new *happy ending* of the case portrays the damage repair caused by the cyber-crime attack. Due to the complexity of the Artificial Intelligence Assistant Side Game idea and the short time for the prototype development, the design of this side quest was left in stand-by. For a better perception of the game, some questions frequently contained in Game Design Documents are answered below.

3.4.2 *What is the game?*

This is an investigation/detective game that aims to educate teenagers about cyber-security.

3.4.3 *Where does the game take place?*

The game takes place at a police station, specifically in the cyber-security department. This department contains a waiting room, a common office, the office of the cyber-detective and a laboratory with some research rooms.

3.4.4 *What does the player control?*

The player controls the cyber-detective character of the department and her actions throughout the investigation.

3.4.5 *What is the main focus?*

The game purpose is to solve cyber-crimes resorting to cyber-security themed mini games, present in the laboratory rooms. To successfully solve the mini games, the player must use its knowledge about the themes.

3.5 **Prototype Storyline**

For the developed prototype, ransomware was the main theme chosen as the cyber-crime (as pointed in section 3.2). A storyline was then created up to connect crime with the stages of its resolution, then producing a story with logic. The plot is divided in two parts: the crime occurrence, at the house of the victim (a teenager), and its resolution, at the cyber-security department. It was decided that the victim of the crime should be a teenager, so that the audience target of the game (defined in section 2.4) could relate to the character. The plot corresponds to a full case. An illustrative storyboard can be seen in the appendix B, made with help of Storyboard That, explained in the subsection 4.2.1. The storyline is can be explained as follows:

First Part: The Crime Occurrence (House of the Victim):

1. A teenager boy surfs his social networks on his smartphone;
2. In the social network feed, he finds an ad for a website claiming to sell branded shoes at an incredibly low price;
3. The adolescent decides to check the website and then decides to buy a pair of sneakers;
4. Before letting the young advance with the purchase, the website proposes the download of an application in exchange of a 10% discount on the purchase;
5. Without suspecting, the teen continues with the download and installation of the application;
6. The teenager is surprised with a ransomware message;

7. The ransomware message claims to have encrypted all the device files and demands a large amount payment in exchange of the decryption password;
8. Frightened, the teenager decides to seek police help.

Second Part: The Resolution of the Crime (cyber-security Department):

1. The teen explains the situation to the cyber-detective and asks for help; the detective accepts;
2. The detective decides to analyze the social network of the adolescent to find the ad that led him to the malicious website; to achieve this, the player must complete the Social Network mini game;
3. The detective then decides to investigate the suspicious website and its phishing signs to find out who might have created it; for that, the player must solve Phishing Detector mini game;
4. With the suspect website creators and their info, the detective tries to discover the decryption passwords of the files; to achieve this, the player must complete the Password Decoder mini game;
5. After solving the three mini games, the detective manages to clear the ransomware off the device and decrypt the files; the smartphone is returned to the teen.

3.6 Mini Games

With the plot established, it was possible to choose the mini games themes that best fit the storyline. Each mini game design is elucidated below.

3.6.1 Social Network Mini Game

With the Social Network main theme in mind, it was intended to approach topics like Talking with Strangers, Sharing in Social Networks and Cyberbullying (Social Network issues mentioned at section 3.2). To allow the player to test its knowledge about the subjects, the idea created for the game was to enable the player, in the role of the detective, scroll through the social network feed of the teen searching for the website while making good decisions regarding incoming pop-ups, like Friend Requests, Messages and Scheduled Posts.

3.6.2 Phishing Detector Mini Game

Using Phishing as the main theme to approach the Personal Data Importance mentioned in section 3.2, this mini game has the main objective to test the capacity of the player to spot phishing

or scamming signs, whether is it in websites or e-mails. Some screens will be presented to the player and it must find the phishing signs.

3.6.3 Password Decoder Mini Game

To approach the Passwords Management theme mentioned in section 3.2, the idea created is based on showing the player a simplified bit of what hackers do to crack passwords. With this idea, it is intended to show the player how simple passwords are easily hacked. The player will have access to a list with the suspect website creators and some of their info, as well as lists with the Top 10 Most Common Passwords and the Top 10 Words from the Dictionary Most Used in Passwords. With this information, the player should combine elements to find 3 passwords. It is intended to show the player that using common words or personal information in passwords is unsafe.

3.7 Conclusions

With the main game and the mini games design defined, it was possible to proceed to the development part of the project. During that stage, the game design may suffer further adaptations to complement the development.

Chapter 4

Prototype Development

4.1 Introduction

This chapter contains information about all the components of the developed prototype. It presents the tools used for the project in section 4.2, enumerates the game features and its mini games in section, describing the game world and its key locations in section 4.3, presenting the game characters in section 4.4, clarifying the Game User Interface (UI) in section 4.5, defining the Game Cutsscenes plots in section 4.6 and lastly explaining the gameplay of the prototype in section 4.7.

4.2 Development Tools

It was necessary to use several tools to support the development and creation of the necessary elements of the game. The usage of these tools made it possible to successfully develop the desired game prototype.

4.2.1 *Storyboard That*

Storyboard That [9] is an online platform for storyboard creation, both for cinematics or applications. This tool allowed to visually design and clarify, in a preliminary stage, the prototype and the animated cut scene plot sequences.

4.2.2 *Unity*

Unity [10] is a multi-platform game engine mostly used to develop games and simulations for computers, video game consoles and mobile devices. Unity is praised for providing the developer the ability to produce a single project that works for multiple platforms (currently targeting 27 platforms). This gaming engine supports, amongst many features, 2D and 3D graphics and scripting through C#. Unity was used in the project for all the gaming prototype creation and development.

4.2.3 *Blender*

Blender [11] is a 3D computer graphics software used for 3D modeling, creating animated films, visual effects, art, texturing, composition, rendering, video editing and creation of interactive 3D applications, such as video games, through its integrated game engine Blender Game Engine. This software was used to model the 3D graphic elements of the prototype, as well as the

creation of 3D animations for the animated cutscenes.

4.2.4 *Vegas Pro 13*

Vegas Pro [12] is a video editing software for non-linear editing that features real-time multi-track video and audio editing on unlimited tracks. This software was used to compose the game animated cutscenes.

4.2.5 *Microsoft PowerPoint*

PowerPoint [13] is a software for creating, editing and displaying graphic presentations. It was used as a support for creating game design storyboards, textures for the 3D graphic elements of the game and creating all the 2D graphics (for example, the UI of the game).

4.3 Game World

The world of the prototype consists in a cyber-security Department Floor at a Police Station, in a 3D ambient. This floor has some rooms, each one with its purpose, and some locked doors (to be unlocked for future levels of the main game). The player may explore the entire department. All the unlocked doors have a name plaque so the respective rooms can be identified. The rooms have cyber-security tips in cork and chalk boards.

To complement the plot, two additional physical locations were created and demonstrated in the introduction cutscene.

All the world was created using Blender (mentioned at the subsection 4.2.3), from the rooms modeling to the objects texturing. Some texture images were web sourced, while others were created using Microsoft PowerPoint (mentioned at subsection 4.2.5).

4.3.1 Key Location 1: Cyber Detective Office

The Cyber Detective Office is the office of the main character. It serves as background for the animated level introduction and conclusion cutscenes and it is the starting location of the controllable character. This room was created following a typical detective office setting, with objects like a computer desk, a framed police badge and an evidence board. The final office model can be observed in the figures 4.1a, 4.1b, 4.1c and 4.1d. The door in the room leads to the Department Common Room (see subsection 4.3.2).

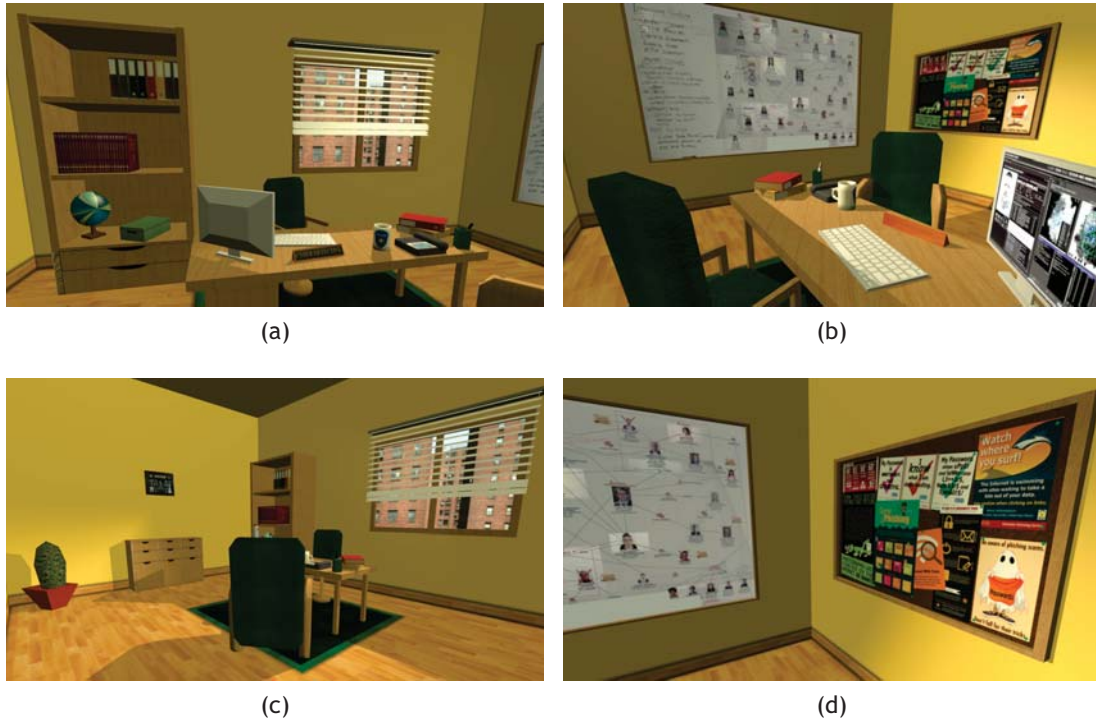


Figure 4.1: Rendered images of the model of the Cyber Detective Office.

4.3.2 Key Location 2: Cyber-security Department Common Room

The cyber-security Department Common Room is the main room of the department and where the majority of the department officers work. This room was created based on the interiors of American police stations (examples of these police stations can be seen in Figures 4.2a and 4.2b). The police department is divided in two areas: a waiting room with a counter (illustrated in Figures 4.3a and 4.3b), for receiving common citizens, and an open office room for the department staff to work in (illustrated in Figures 4.3c, 4.3d and 4.2e). The open office room was created with a vast number of computer desks. This room provides access to the Cyber Detective Office (subsection 4.3.1) and to the Cyber Lab (subsection 4.3.3, short for Cyber Laboratory).



Figure 4.2: Examples of American police station interiors which the department was based on.

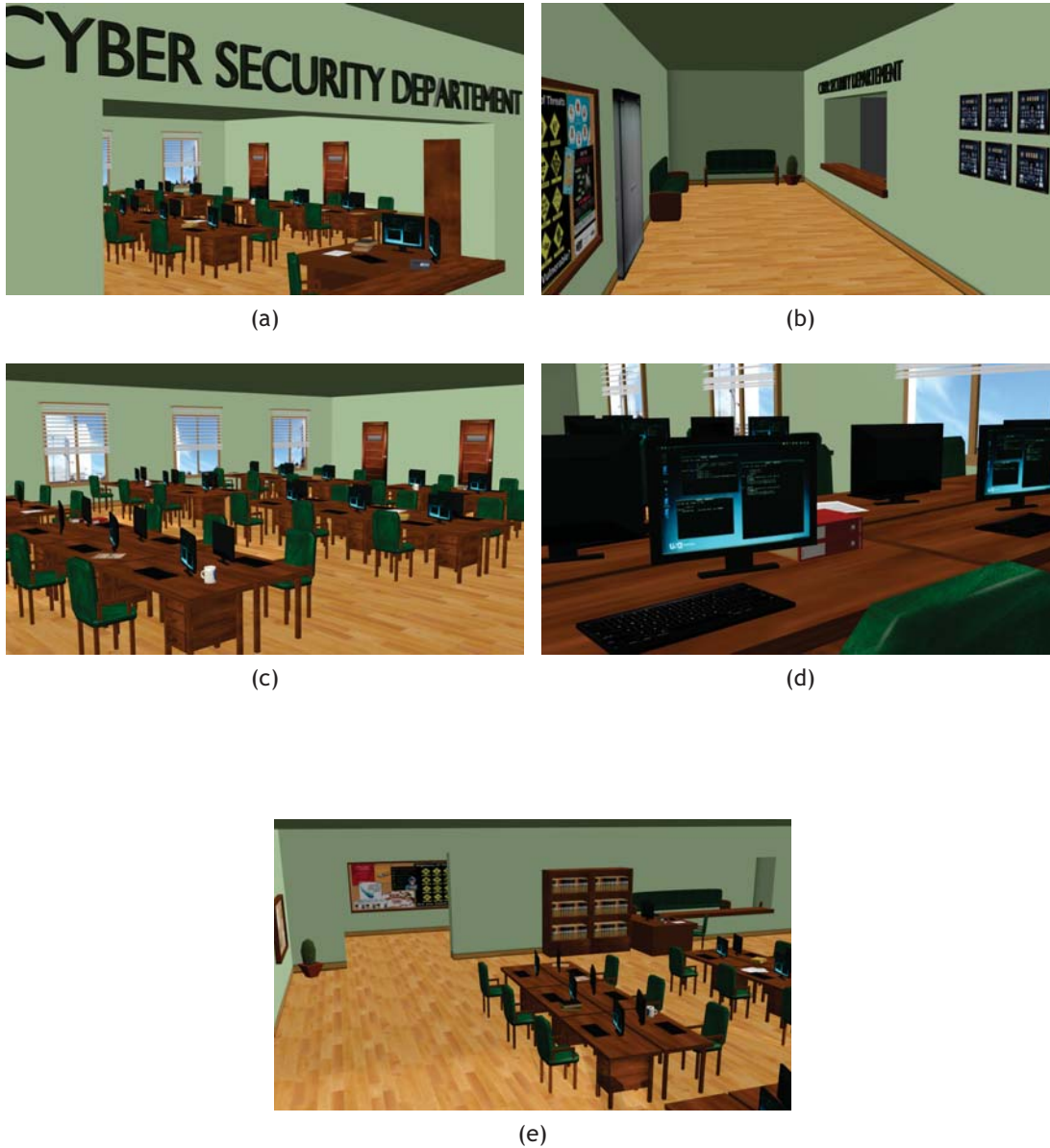


Figure 4.3: Rendered images of the model of the Cyber-security Department Common Room.

4.3.3 Key Location 3: Cyber Laboratory

The Cyber Laboratory is the place where the case solving happens. This lab has a sci-fi/futuristic ambiance, related with the cybernetic theme of the game. Figures like 4.4a and 4.4b served as guidelines for the appearance of the laboratory. The cyber lab contains numerous computer screens and an electronic evidence table and can be seen in the Figures 4.5b, 4.5c and 4.5d. The player can enter the Lab from the Department Common Room (mentioned in section 4.3.2). The laboratory contains a corridor with access to some themed rooms (illustrated in the Figure 4.5a and 4.5e), each one specific to a certain cyber-security issue. In these rooms, the cyber detective can pursue with the investigation. Some of these rooms are clarified in the subsections below.



(a)



(b)

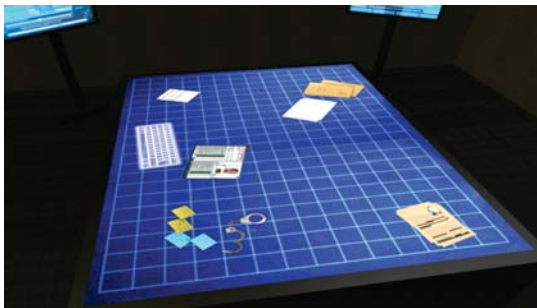
Figure 4.4: Examples of sci-fi/Futuristic laboratories of which the cyber laboratory was based on.



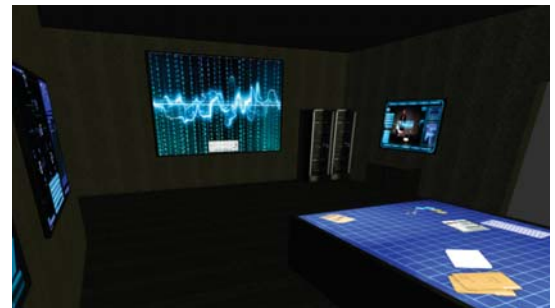
(a)



(b)



(c)



(d)



(e)

Figure 4.5: Rendered images of the model of the Cyber Laboratory.

4.3.4 Key Location 4: Password Room

The Password Room is one themed room located at the Cyber Lab (mentioned in section 4.3.3) and, as its name implies, has a password security theme. The walls and the main computer screen follow the style of the famous *Matrix Raining Code* imagery (which example can be seen in Figure 4.6) and there is a chalkboard with tips for creating safer passwords (illustrated in the Figure 4.7a). These tips may be helpful for the 3rd mini game, the *Password Decoder* (described in the subsection 3.6.3), that may be found in this room. The room can be observed in the Figures 4.7b, 4.6c, 4.6d and 4.5e.



Figure 4.6: Image of the *matrix raining code*, from which the walls from the Password Room were based of.



(a)



(b)



(c)



(d)



(e)

Figure 4.7: Rendered images of the model of the Phishing Room.

4.3.5 Key Location 5: Social Networks Room

The Social Networks Room is another themed room that can be accessed through the Cyber Lab (4.3.3). This aspect of the room resembles an office. The most important detail in this room is the amount of tips about Social Network Usage, Personal Data Sharing and Webcam Dangers contained in posters pinned to corkboards (illustrated in Figures 4.8a and 4.8b). The information of these posters can help the player to solve the 1st mini game, the *Social Network Analysis* (described in the subsection 3.6.1), that may be found in this room. This room can be observed in the Figures 4.8c and 4.8d.



(a)



(b)



(c)



(d)

Figure 4.8: Rendered images of the model of the Social Networks Room.

4.3.6 Key Location 6: Phishing Room

The Cyber Lab (mentioned in section 4.3.3) has an entry to the Phishing Room, a phishing themed room. This room can be observed in the Figures 4.9a, 4.9b, 4.9c and 4.9d. There is a corkboard and a whiteboard full of tips on how to spot phishing scam attempts (illustrated in the Figures 4.9e and 4.9f). These tips might be helpful for the 2nd mini game of the prototype that can be found in this room, the *Phishing Detector* (described in the subsection 3.6.2).



(a)



(b)



(c)



(d)



(e)



(f)

Figure 4.9: Rendered images of the model of the Phishing Room.

4.3.7 Cutsцене Location 1: Teen Room

To illustrate the Crime Occurrence as it was planned in the plot (section 3.5), the room of the teen was created to serve as background to an animated cutscene. It has a typical teen room aspect, with a bed, a computer desk and teen posters on the walls. The final model can be seen in the Figures 4.10a, 4.10b, 4.10c and 4.10d.

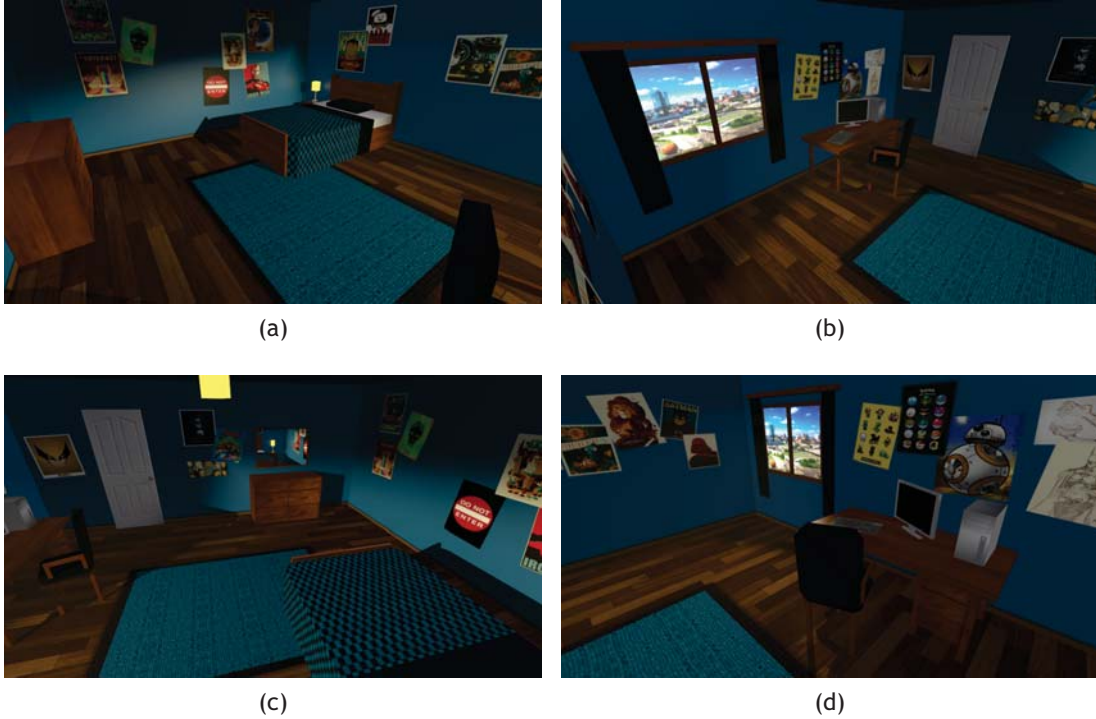


Figure 4.10: Rendered images of the model of the Room of the Teen.

4.3.8 Cutsценe Location 2: Police Station Outdoor

During the animated cutscene creation, it was realized that there was a need for a transition scene that illustrated the location changing from the room of the teen to the Cyber Detective Office (section 3.5). For that purpose, it was created a physical location of the exterior of the Police Station that holds the cyber-security Department. The Police Station was based on the building illustrated on the Figure 4.11a. The final Police Station Outdoor Model can be seen in the Figure 4.11b.



(a) Example of a police station of which the police station model was based on.



(b) Final Model of the Police Station Outdoor - Rendered Image

Figure 4.11: Police station images.

4.4 Game Characters

According to the established plot (section 3.5), at least two characters were needed, a teenager and a detective. For the prototype, it was decided to use characters from a character pack with no copyright [4] created by the user VMComix and shared at *Blender Swap* [14], a website where Blender (mentioned in the subsection 4.2.3) 3D Artists can share, exchange, collaborate and learn from other artists in the community. This pack contains 3 characters, Porl, Elaine and Ed (illustrated in the Figure 4.12). The cartoon aspect of the characters was the main reason of the choice of this pack, for the style blends with the game world created.

The characters were animated with Blender.



Figure 4.12: Elaine, Porl and Ed, from left to right, the characters from the Cartoon Character Pack 1 [4].

4.4.1 The Teenager

The cyber-crime victim (3.5) of this plot is a teenager. To illustrate the crime occurrence in an animated cutscene, the character Porl from the character pack used [4] was used. This character was chosen for its young appearance. The original 3D model was not modified and this character was merely animated for the animated cutscene. The teen is illustrated in the Figure 4.13a.

4.4.2 The Cyber-security Detective

The cyber-security Detective is the game character controlled by the player. It both appears in-game and in the animated cutscenes. The character from the character pack [4] chosen for this role was Elaine. The original 3D model colors of Elaine were changed to give her a more adult appearance. This character was animated for the animated cutscene and has two in-game animations, Idle and Walking. The default game animation of the character is Idle. The game animation changes from Idle to Walking when the player interacts with the Walking Joystick (described in the following section) and from Walking to Idle when the player stops that interaction. The cyber detective is illustrated in the Figure 4.13b.



(a) The teenager.



(b) The detective.

Figure 4.13: Rendered images of the game characters.

4.5 User Interface

The UI allows the player to interact with the game and can give some feedback on what is happening on the game. The UI is a key element to captivate players. At the beginning of the game, the player is presented with a Starting Menu, where it can choose to start a new game or to continue progressed one. In the actual game, since it involves controlling a character, the interface should provide the player a way to do so. For that purpose, two virtual joysticks were created - a Walking and a Rotation Joystick. These joysticks were created following the guidelines from the free Unity project *Mobile Touch Floating Joysticks with Options* [15], available at Asset Store of Unity, a library of free and commercial assets created both by Unity Technologies and also members of the community. To provide the player a way to view its game progress, a Missions Window was created. It enumerates the missions of the game and the progress of the player in each one of them. This window also provides the player the option to return to the Starting Menu, saving its game progress. To progress in the plot of the game, the player should complete mini games and, for that, the player needs a way to access these games. For that purpose, the Mission Markers were created. The concept of these markers is clarified in a subsection below. Lastly, each of these mini games has its own UI, also respectfully described in subsections below.

4.5.1 Camera of the Game

To show the cyber detective controllable character to the player, the virtual camera of the game uses a third-person perspective with a tracking camera system, as seen on image 4.14. This system gives the player a perspective from a fixed distance behind and slightly above the character, while tracking its motion.



Figure 4.14: Illustrative image of the camera perspective of the game.

4.5.2 User Interface Detail 1: Starting Menu

The Starting Menu interface was designed to resemble an open police/detective case file folder, since the prototype represents a police case. Inside this file folder there is a sheet with the name of the case, *Ransomware*, with two interactive buttons, *Start* and *Continue*. The latter only appears when there is a saved game. The Start Button presents the initial animated cutscene and starts a new game. The *Continue Button* starts the game where the progress was saved. The Starting Menu can be observed in Figure 4.15.



Figure 4.15: Screenshot showing the interface of the starting menu.

4.5.3 User Interface Detail 2: Walking Joystick

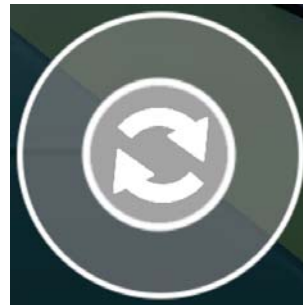
The Walking Joystick is a virtual joystick that consists of two circles, the pivot (inner circle) and the base (outer circle). As the name implies, this joystick interacts with the controllable character walking. To make the cyber detective walk, the player must interact with the joystick, sliding the pivot along the base. Moving the pivot to the top of the base will make the detective walk forward, while moving it to the bottom of the base will make her walk backwards. Moving the pivot to the left or right of the base will make the detective walk in the respective direction. To stop the movement of the character, the player simply needs to release the pivot. The Walking Joystick is illustrated in Figure 4.16a.

4.5.4 User Interface Detail 3: Rotation Joystick

The Rotation Joystick is a virtual joystick with a pivot and a base, with a similar system to the Walking Joystick. As its name implies, the Rotation Joystick allows the player to rotate the character. The camera of the game (described in the section 4.5.1) perspective follows the rotation of the character. Moving the pivot to the left or right of the base will make the detective turn to the respective direction. Moving the pivot to the top or bottom of the base will tilt the perspective of the camera down or up, respectively. Like the previous joystick, to stop the rotation the player must simply release the pivot. The Rotation Joystick is illustrated in Figure 4.16b.



(a) The walking joystick.



(b) The rotation joystick.

Figure 4.16: Close-ups of the game joysticks.

4.5.5 User Interface Detail 4: Missions Window

To allow the player to keep up with its progress in the game plot, the Missions Window was created. Clicking the Missions Button (illustrated in the Figure 4.17a) in the main interface will open this Window (illustrated in the Figure 4.17b). It provides information about the missions completed by the player and the respective scores, the current mission that the player should finish and the following missions. The Missions Window has a *Back to Menu* button, that allows the player to quit the current game and return to the Starting Menu. Interacting with this button will open a Quit Dialog Box with Affirmative and Negative buttons (as seen in Figure 4.18a), to assure if the player wants to quit the current game. Clicking the Negative button will close the window and clicking the Affirmative button will open a Save Dialog Box also with Affirmative and Negative buttons (as seen in Figure 4.18b). In that dialog, the players can chose to save the current progress or not, clicking the Affirmative or Negative button, respectively. Consequently, the player is led to the Starting Menu. The Missions Window can be exited by clicking an existing X Button.



(a) The Missions button.

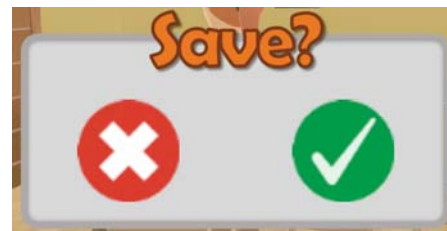


(b) The Missions window.

Figure 4.17: Screenshots of the Missions button and window.



(a) The Quit Dialog box.

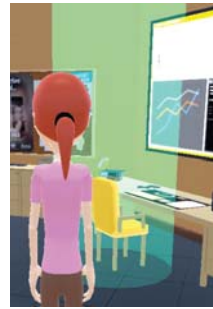


(b) The Save Dialog box.

Figure 4.18: The Back to Menu Dialog boxes.

4.5.6 User Interface Detail 5: Mission Markers

To make progress in the plot of the game and finish the level of the prototype, the player must complete three mini games (as it is defined in the section 3.6). To accomplish that, the player should lead the detective to the themed rooms from the Cyber Lab (Password Room, Social Networks Room and Phishing Room) in order to access the respective games and complete them. The mission markers are circular beams of light placed in the themed rooms, and they allow the player to enter the respective mini game of the room by walking the detective character into this beam. New mission markers are blue while completed mission markers are white (illustrated in Figure 4.19). The player may improve his mini game scores if it wants to, entering the white markers. The mission markers appear in each room following the order of the plot (as explained in section 3.5), first the *Social Network Analysis* game, then the *Phishing Detector* game and lastly the *Password Decoder* game. Therefore, the game will start only with the *Social Network Analysis* mark active and the player must complete the mini games to unlock the others.



(a) Illustration of the new mission marker.



(b) Illustration of the completed mission marker.

Figure 4.19: Screenshots showing the different mission markers.

4.5.7 Mini game User Interfaces: *Social Network Analysis*

The interface of the *Social Network Analysis* mini game resembles, intentionally, the social network *Facebook* feed interface. In this mini game, the user must scroll the feed of the social network to advance in the game, using the scroll button. At every scroll, a notification pop-up will appear in the right corner of the screen. According to the content of the notification, the player should decide to accept or decline the notification in the respective buttons. The main interface of this mini game is illustrated in the Figure 4.20.

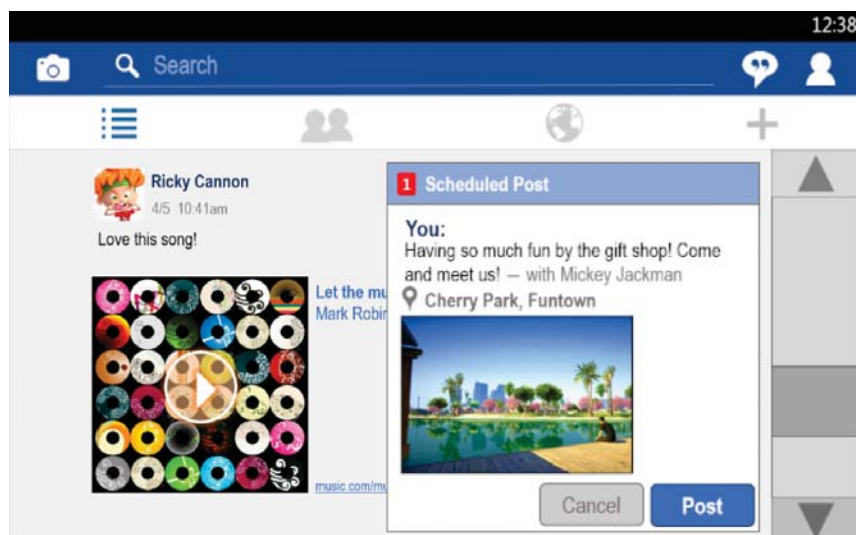


Figure 4.20: The *Social Network Analysis* mini game main interface.

In the example of the Figure 4.20, it can be observed a notification pop-up of a scheduled post. The game consists on the player clicking the *Cancel* or *Post* button according to what it thinks it would be the safest action to take. At the end of this mini game, and according to the chosen options, the player receives feedback about the correct options for each notification.

4.5.8 Mini game User Interfaces: *Phishing Detector*

In the *Phishing Detector* mini game, the player must find and click the phishing attempt signs (or flags) existent in the presented screen. In the right side bar, the player can see how many flags are in the screen, how many it has found and how many clicks left it has to find them. Every time the player clicks in a phishing flag, the flag turns red and the Flags Found counter increases. Clicking on the screen where there are no flags will decrease the Clicks Left counter. The main interface of this mini game is illustrated in the Figure 4.21.

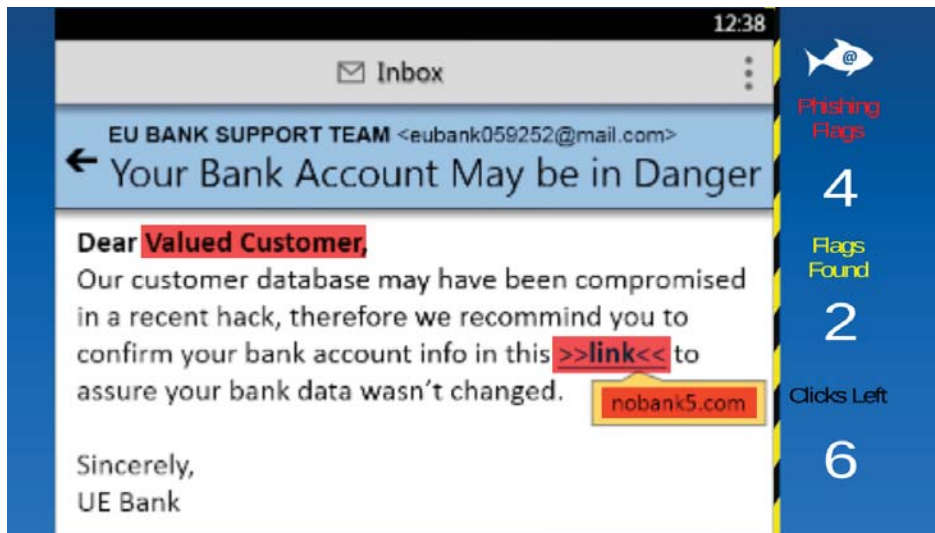


Figure 4.21: The *Phishing Detector* mini game main interface.

In the example of the Figure 4.21, it can be observed an e-mail screen. With a limited number of clicks, the player must identify the phishing signs clicking on them.

4.5.9 Mini game User Interfaces: *Password Decoder*

The *Password Decoder* mini game, the player must guess passwords using the given clues. The main element of this interface is the password guess input box. Clicking this input box will open the keyboard of the smartphone. There is a text in the interface with a tip for what the password might be. The player has access to three information windows through the buttons *Suspects Info*, *Top 10 Words Dictionary* and *Top 10 Passwords*. With the given tip and using the information elements from the previously mentioned windows, the player must guess the password. The information elements in the windows can be added automatically to the password guess input box by clicking on the intended word. The player has a number of attempts to guess the correct password. To verify if the password guess is the correct answer, the player should hit the button *Submit*. If the guess is correct, the level is complete, if the guess is wrong, the Attempts number will decrease. The main interface of this mini game is illustrated in the Figure 4.22.



Figure 4.22: The *Password Decoder* mini game main interface.

In the example of the Figure 4.22, it can be observed the main interface of the mini game. A word from the *Suspects Info* was added to the password guess input box and the player should click submit to verify if its guess is the correct answer.

4.6 Animated Cutscenes

For a better understanding of the plot by the player, it was necessary to create animated cutscenes: an introductory animation to illustrate the crime occurrence leading to the requirement of the help of the detective and an ending animation to illustrate the conclusion of the crime. The cutscenes are composed of numerous animation sequences created with Blender (mentioned at the subsection 4.2.3), all assembled, edited and subtitled with Vegas Pro (mentioned at the subsection 4.2.4).

4.6.1 Initial Cutscene

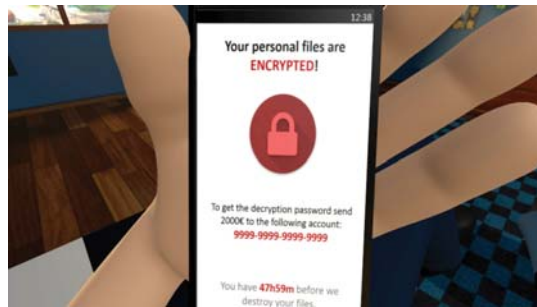
The initial animated cutscene illustrates the crime occurrence described at the Prototype Plot, section 3.5. This sequence has 3 acts, The Crime Occurrence, The Location Transition and The Request of the Help to the Detective. These acts are illustrated in Figure 4.23 and are described as follows:

- **The Crime Occurrence:** In its room, the teen surfs its social network and sees an advertising to a website claiming to sell sneakers at an incredibly low price. Trying to make a purchase, the teen is offered a 10% discount in exchange of a download. The teens downloads it and accidentally installs a ransomware;
- **The Location Transition:** This scene shows the camera closing-up of the Police station building, implying the transition of location to the Cyber Detective Office;
- **The Request of the Help to the Detective:** In the Cyber Detective Office the teen and

cyber-security detective are talking. The teen explains the ransomware situation to the detective, and she accepts to help.



(a) Teen surfing its social network.



(b) Appearance of the Ransomware message.



(c) The location transition with the closing-up of the Police station building.



(d) Teen asking the Detective for help.

Figure 4.23: Illustrative frames of the initial cutscene.

4.6.2 Ending Cutscene

The ending animated cutscene creation was needed to conclude the game plot of the prototype. It illustrates the resolution of the crime, where the detective manages to clear the ransomware off the device. This sequence has one act, illustrated in Figure 4.24 and described as follows:

- **The Conclusion of the Crime:** At the Cyber Detective Office, the teen and cyber-security detective are talking. The detective has managed to clear the ransomware off the device and decrypt the files and returns the smartphone to the teen, which thanks the detective.



(a)



(b)

Figure 4.24: Illustrative frames of the ending cutscene.

4.7 Gameplay

As any game, this prototype and its mini games have challenges and a pattern of rules to overcome them.

4.7.1 Main Victory Conditions

To follow up the defined prototype plot guidelines defined in section 3.5, the following missions were established:

1. Mission 1 - Go to the Cyber Lab: The player should lead the detective character to the Cyber Lab;
2. Mission 2 - Find the malicious website on the Social Network of the teen: The player should lead the detective character to the Social Networks Rooms and complete the *Social Network Analysis* mini game;
3. Mission 3 - Analyze the potential Phishing signs of the website: The player should lead the detective character to the Phishing Room and complete the *Phishing Detector* mini game;
4. Mission 4 - Find the Password to decrypt the files of the teen: The player should lead the detective character to the Passwords Room and complete the *Password Decoder* mini game.

Completing all the missions will present the final animated cutscene to the player.

4.7.2 Victory Conditions: *Social Network Analysis*

The *Social Network Analysis* mini game goal is to find the phishing website post on the Social Network of the teen while making safe decisions regarding oncoming notifications. The player will come across with four (4) different notifications and may answer positively or negatively to them. These notifications may come in the form of Friend Requests, Messages or Scheduled Posts. To see all the possible notification pop-ups, see appendix C.

Victory Minimum Score Condition: The player must answer correctly to at least **3 out of 4** notifications correctly.

4.7.3 Victory Conditions: *Phishing Detector*

The *Phishing Detector* mini game goal is to find phishing signs in (3) different screens. These screens may represent e-mails, websites or shopping scams. The last screen always represents the website where the teen downloaded the ransomware. To see all the possible screens, see appendix D.

Victory Condition: The player must find **ALL** the phishing flags of the three screens.

4.7.4 Victory Conditions: *Password Decoder*

The *Password Decoder* mini game goal is to use common elements used in weak passwords to guess three (3) different passwords. The player has access to a list of three Hacker Suspects and respective names, birthyears and country codes, a list of the Top 10 Dictionary Words Used in Passwords and a list of the Top 10 Most Common Passwords. From the Hacker Suspects list, only one of the three suspects is used for all the mini game passwords. The 1st password is one element of the information of the suspect (name, birthyear or country code). The 2nd password is the combination of two elements of the information of the suspect. Lastly, the 3rd password is the combination of one element of the information of the suspect with either one of the Top 10 Dictionary Words Used in Passwords or one of the Top 10 Most Common Passwords. If the password contains one of the Top 10 Dictionary Words Used in Passwords, the player receives a clue to this length of the word. If the password contains one of the Top 10 Most Common Passwords, the player receives a hint to a random character of that password. To see all the possible Hacker Suspects Information, the Top 10 Dictionary Words Used in Passwords list and the Top 10 Most Common Passwords list, see appendix E.

Victory Condition: The player must guess correctly **ALL** of the three passwords.

4.8 Conclusions

This chapter described all the components of the prototype and features created and developed. Blender and Unity, approached in the subsections 4.2.3 and 4.2.2, were the key tools used for the development of this project, since the modelling of Game World and the prototyping of the game were the main steps of the project. The world creation and character choice were made intending to give the game a realistic appearance, yet with cartoon-like features. The biggest difficulty of the project was harmonizing the creation of the game elements with the developing of the game itself, time wise. With the game prototype finished, it was possible to implement tests near the target audience.

Chapter 5

Tests

5.1 Introduction

To evaluate the quality of the prototype, some tests were implemented with the target audience of the game. In this chapter, the results of these tests are analyzed, in particular the user experience described in section 5.2, and the efficiency of the game in teaching new contents about cyber-security to the target audience, described in section 5.3.

The tests were applied in Escola Secundária do Fundão [16], to a 9th grade class, with 14 students with ages between 14 and 17 years old (the target age of the project). The students were submitted to a knowledge quiz twice: once before playing the produced game and once after playing it. This quiz (written in Portuguese) was included in appendix F. The students were observed while playing the game, making some comments about their experience. After playing, the students answered a questionnaire to evaluate the game and their usability experience. With the notes from these tests, it was possible to analyze the quality of the user experience, presented in section 5.2. The questionnaire answered by the students (written in Portuguese) was included in appendix G. With the results from the knowledge quizzes, it was possible to analyze the improvement made by the students after playing the prototype. These results are presented in section 5.3.

5.2 Usability Tests

The questionnaire answered by the students approached four different subjects: the flow of the game, the thematic of the game, graphics and mini games and didactic. The teenagers evaluated the game on these topics answering questions based on the Likert Scale.

Analyzing the evaluations made to the Flow of the Game, as seen in Table 5.1, it is noted that the students had some difficulties in understanding which were the correct actions to complete the tasks. This may have happened due to the language of the prototype, because not all the students were comfortable with the English Language.

Table 5.1: Flow of the Game Evaluation - Results

| Flow of the Game | Strongly Disagree | Disagree | I do not agree or disagree | Agree | Strongly Agree |
|---|-------------------|----------|----------------------------|-------|----------------|
| I always understood what was the task. | 0 | 0 | 5 | 7 | 2 |
| I have always found the right action to take, effortlessly. | 1 | 2 | 6 | 3 | 2 |
| I always realized that performing certain action would complete the corresponding task. | 0 | 1 | 5 | 5 | 3 |
| I was always aware of the progress made when completing tasks. | 0 | 0 | 3 | 8 | 3 |

Analyzing the evaluations made to the Thematic of the Game, as seen in Table 5.2, it can be concluded that almost a third of the students seems to have no awareness of all the dangers they face online everyday, since they stated that they did not deal with the themes of the game on their daily life, although the answers to the questions *I use a smartphone/the Internet/social networks everyday* were so positive. The results also show that the students are concerned about cyber-security and the dangers of the Internet. With these results, it can be concluded that, even with lack of knowledge, this age segment is worried and interested about cyber-security, making it the perfect audience target for the current project.

Table 5.2: Thematic of the Game Evaluation - Results

| Thematic of the Game | Strongly Disagree | Disagree | I do not agree or disagree | Agree | Strongly Agree |
|---|-------------------|----------|----------------------------|-------|----------------|
| I use a smartphone every day. | 0 | 0 | 1 | 7 | 6 |
| I use the Internet every day. | 0 | 0 | 1 | 6 | 7 |
| I use social networks every day. | 0 | 0 | 2 | 6 | 6 |
| I understood the themes of the game. | 0 | 1 | 2 | 7 | 4 |
| The themes of the game are something that I deal with in my daily life. | 0 | 1 | 5 | 4 | 4 |
| cyber-security and the dangers of the Internet are something that worries me. | 0 | 0 | 2 | 6 | 6 |

Analyzing the evaluations made to the Graphics and Mini Games, as seen in Table 5.3, it is possible to observe that the students were pleased with the game graphics and mobility. The mini games evaluation results show that the mini games of the prototype were not too difficult nor too easy. With these values, it can be concluded that overall the difficulty of the mini games is well-balanced.

Table 5.3: Graphics and Mini Games Evaluation - Results

| Graphics and Mini Games | Strongly Disagree | Disagree | I do not agree or disagree | Agree | Strongly Agree |
|--|-------------------|----------|----------------------------|-------|----------------|
| The game graphics were adequate. | 0 | 1 | 1 | 7 | 5 |
| I understood the plot of the game. | 0 | 1 | 2 | 6 | 5 |
| The mobility in the game was good. | 0 | 2 | 3 | 6 | 3 |
| The social networks mini game was difficult. | 1 | 4 | 7 | 1 | 1 |
| The phishing mini game was difficult. | 1 | 4 | 8 | 0 | 1 |
| The passwords mini game was difficult. | 1 | 2 | 6 | 3 | 2 |

Analyzing the evaluations made to the Didactic of the Game, as seen in Table 5.4, it is possible to conclude that overall the students learned about cyber-security with the game and would willingly play a full version of the game conceptualized in this document. It is also possible to observe that the students think that learning about cyber-security with a video game is appealing, comparing to the typical teaching methods.

Table 5.4: Didactic Evaluation - Results

| Didactic | Strongly Disagree | Disagree | I do not agree or disagree | Agree | Strongly Agree |
|--|-------------------|----------|----------------------------|-------|----------------|
| This game taught me about the topics approached in the game. | 0 | 0 | 3 | 7 | 4 |
| I think this type of game suits the theme. | 0 | 0 | 1 | 8 | 5 |
| I would like to play a full version of this game to learn more about cyber-security. | 0 | 0 | 2 | 4 | 8 |
| I would rather learn about cyber-security with a video game than with lectures/videos/classes. | 0 | 0 | 2 | 5 | 7 |

5.3 Education Efficiency

Since the game of this project is an educational game, it was imperative to evaluate the efficiency of its educational component. The students answered a knowledge quiz with questions about ransomware, phishing signs, passwords and social network security (themes approached by the game). To evaluate the growth of the knowledge of the students, the students were asked to take this quiz twice, once before playing the game and once after playing, and the results of both quizzes were compared. Regarding the comparison of the results for each question, as seen on Table 5.5, the two questions that got the worst results in the second take of the quiz were a question to evaluate if a screen was a phishing attempt and a question asking if it was safe to post a picture of a football player in a social network. In the question to evaluate if a

screen was a phishing attempt, the screen presented was NOT a phishing attempt, just a simple bank account e-mail. Although that, the students were more hesitant regarding this question in the second take of the quiz. The question asking if it was safe to post a picture of a football player in a social network had a positive answer, it IS SAFE to post a simple picture of a football player. In spite of that answer, in the second take of the quiz, the students seemed more unsure of the safety of the post.

Opposing the results of the phishing question above, the question that had the better improvement rate was a similar phishing question, in which the screen presented is an e-mail with a phishing attempt. The combination of the results of these two questions conclude that the students were more aware of phishing attempts through e-mails after playing the prototype and were overly cautious about them.

The second question with better improvement asked the student to pick the safest password of a list. The improvement of the score of this question shows that the students improved their capacity of identifying a safe password.

Table 5.5: Quiz Scores Improvement per Question

| | Quiz Questions | | | | | | | | | | | | | | | |
|----------------|----------------|-----|------|-----|------|-----|------|------|-----|-----|------|-----|------|------|-----|-----|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| First Results | 21% | 50% | 100% | 64% | 100% | 64% | 100% | 100% | 50% | 64% | 86% | 50% | 100% | 79% | 28% | 11% |
| Second Results | 36% | 71% | 100% | 79% | 100% | 79% | 100% | 100% | 64% | 64% | 71% | 93% | 100% | 57% | 33% | 32% |
| Improvement | 15% | 21% | 0% | 15% | 0% | 15% | 0% | 0% | 14% | 0% | -15% | 43% | 0% | -22% | 5% | 21% |

Overall, it was possible to verify an improvement of the quiz scores, as seen in Table 5.6. The scores of the quiz improved on average nearly 7%. With these results it is possible to conclude that the education component is efficient, since the students improved their knowledge on the subject. Each row of the table 5.6 represents a student of the class.

Table 5.6: Ordered Quiz Scores Improvement

| First Take of the Quiz | Second Take of the Quiz | Improvement (Ordered from low to high) |
|------------------------|-------------------------|--|
| 68,8% | 67,7% | -1,0% |
| 83,3% | 83,3% | 0,0% |
| 58,3% | 58,3% | 0,0% |
| 58,3% | 59,4% | 1,0% |
| 78,1% | 80,2% | 2,1% |
| 77,1% | 83,3% | 6,2% |
| 71,9% | 78,1% | 6,3% |
| 51,6% | 58,2% | 6,6% |
| 68,8% | 76,0% | 7,3% |
| 56,3% | 63,5% | 7,3% |
| 71,9% | 83,3 | 11,5% |
| 60,4% | 71,9 | 11,5% |
| 52,1% | 70,8 | 18,8% |
| 78,1% | 96,9 | 18,8% |
| 66,8% | 73,7% | 6,9% |
| Average | | |

5.4 Conclusions

With the results from the tests implemented with the target audience and analyzed in this chapter, it was possible to conclude that teenagers are sometimes unaware of the cybernetic dangers that they might encounter in their daily life. However, these young students showed interest in learning about the subject to be safer, supporting the purpose of this project. In this chapter it was also possible to verify an improvement of cyber-security knowledge on the teenagers after playing the created game, confirming that the game of this project can be used not only as a game, but also as a learning tool.

Chapter 6

Conclusions and Future Work

This chapter presents the most important conclusions of this project in section 6.1 and points out some lines for future work, as well as other possible outcomes from the project, in section 6.2.

6.1 Main Conclusions

With this project it was possible to **conceptualize the idea for a cyber-security detective game for teenagers** and to **develop a prototype** of a level of that game, in the English language. The prototype was developed in Unity 4.2.2 to be available for different platforms. The prototype was tested with a group of teenagers (representing the target audience) and was proven to improve the cyber-security knowledge of teens, making it a suitable base for a full game of the conceptualized idea.

This project had various components of video game creation created using the learning acquired from the Game Design and Development Masters classes, such as **Design of Digital Games I** (game design), **Screenwriting and Planning Laboratory** (creation of the prototype plot), **Computer Animation** (3D modelling and animation), **Prototyping in Digital Games** (prototype development), **Programming in Digital Games** (prototype scripting), **Game Balance** (balancing of the mini games of the prototype) and **User Experience** (tests near the target audience).

Personally, this project was an important opportunity to explore all the video game creation steps and to follow closely the many stages of video game design and development.

Summing up, it was possible to develop a game prototype that teaches concepts of cyber-security to teenagers in a fun way by using the technology daily used by these young, making the learning process more appealing.

6.2 Future Work

Although the main goal of the project was achieved, the developing of a prototype, there are some improvements that can be applied to the prototype. Following are some proposed improvements for the prototype:

- Addition of sound and music to the cutscenes and game;
- Better flow of the game for the understanding of the player;

- Improvement of some colors and interactions in mini games interfaces;
- Development of the Artificial Intelligence Assistant Side Game (described in the subsection 3.4.1);
- Addition of multiple languages.

To accomplish all the proposed goals of this project, it is also proposed the writing of a conference paper for dissemination of the result of the project.

The **main future goal** of this project is the development of the conceptualized full game, creating more levels to approach the numerous important themes about cyber-security.

Bibliography

- [1] C. S. Education, "Digital compass," 2015, Last Checked: 6/1/2017. [Online]. Available: <https://www.brainpop.com/games/digitalcompass/> vi, 5
- [2] C. International, "Are you a responsible digital citizen?" 2016, Last Checked: 6/1/2017. [Online]. Available: <http://www.digizen.org/resources/cyberbullying/interactive/> vi, 6
- [3] W. E. Foundation, "Cyber lab," 2014, Last Checked: 6/1/2017. [Online]. Available: <http://www.pbs.org/wgbh/nova/labs/lab/cyber/research#/newuser> vi, 6
- [4] VMComix, "Cartoon character pack 1," 2011, Last Checked: 9/9/2017. [Online]. Available: <https://www.blendswap.com/blends/view/14445> xix, 26
- [5] TaC, "Tac together against cybercrime international," 2016, Last Checked: 14/1/2017. [Online]. Available: <https://againstcybercrime.org/> 1, 11
- [6] Ana Amélia Carvalho, Inês Cardoso Araújo, Nelson Zagalo, Tiago Gomes, Cândida Barros and Sónia Cruz, "Os jogos mais jogados pelos alunos do ensino básico ao ensino superior," 2014, Last Checked: 14/1/2017. [Online]. Available: http://jml.fpce.uc.pt/pub/2014_Os_jogos_mais_jogados_2CEB_ES_ejml.pdf 9
- [7] André F. S. Barbosa, Pedro N. M. Pereira, João A. F. F. Dias, and Frutuoso G. M. Silva, "A new methodology of design and development of serious games," *International Journal of Computer Games Technology*, vol. 2014, Article ID 817167, 8 pages, 2014, Last Checked: 24/9/2017. [Online]. Available: <http://www.hindawi.com/journals/ijcgt/2014/817167/> 12
- [8] Jurie, "Why game design is important." [Online]. Available: <http://www.intelligent-artifice.com/2007/10/why-game-design-is-important.html> 12
- [9] Clever Prototypes, "Storyboard that: The world's best free online storyboard creator," 2017, Last Checked: 25/9/2017. [Online]. Available: <http://www.storyboardthat.com/> 17
- [10] Unity Technologies, "Unity - game engine," 2017, Last Checked: 25/9/2017. [Online]. Available: <https://unity3d.com/> 17
- [11] blender.org, "blender.org - home of the blender project - free and open 3d creation software," 2017, Last Checked: 25/9/2017. [Online]. Available: <https://www.blender.org/>

//www.blender.org/ 17

- [12] MAGIX Software GmbH, “Video editing software for film enthusiasts vegas pro,” 2017, Last Checked: 25/9/2017. [Online]. Available: <http://www.vegascreativesoftware.com/us/vegas-pro/> 18
- [13] Microsoft, “Microsoft powerpoint 2016 slide presentation software, ppt,” 2017, Last Checked: 25/9/2017. [Online]. Available: <https://products.office.com/en-us/powerpoint> 18
- [14] Blend Swap, “Blend swap dashboard,” 2017, Last Checked: 9/9/2017. [Online]. Available: <https://www.blendswap.com/> 26
- [15] Kevin Blake, “Mobile touch floating joysticks with options,” 2017, Last Checked: 26/9/2017. [Online]. Available: <https://www.assetstore.unity3d.com/en/#!/content/58759> 27
- [16] Agrupamento de Escolas do Fundão, “Agrupamento de escolas do fundão,” 2017, Last Checked: 26/9/2017. [Online]. Available: <http://www.esfundao.pt/> 37

Appendix A

Preliminary Storyboard

The preliminary game concept was based in a combination of two games - an Interactive Narrative, which is illustrated by the storyboard in the Figure A.1, and a Detective Game, illustrated by the storyboard in the Figure A.2. The Interactive Narrative was later converted to the Introduction of the Game.

A.1 Interactive Narrative



(a)



(b)



(c)



(d)



(e)



(f)



(g)



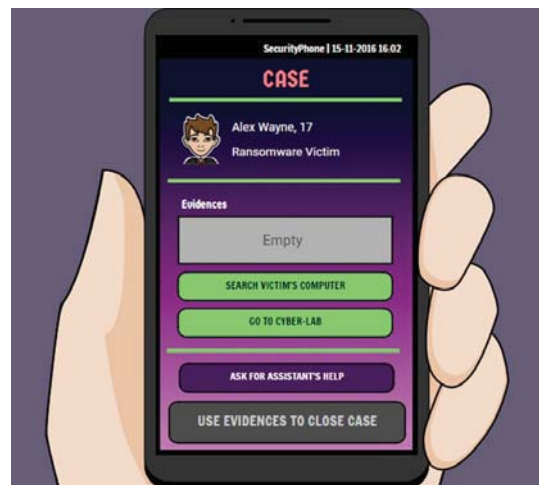
(h)

Figure A.1: Storyboard images illustrating the interactive narrative idea.

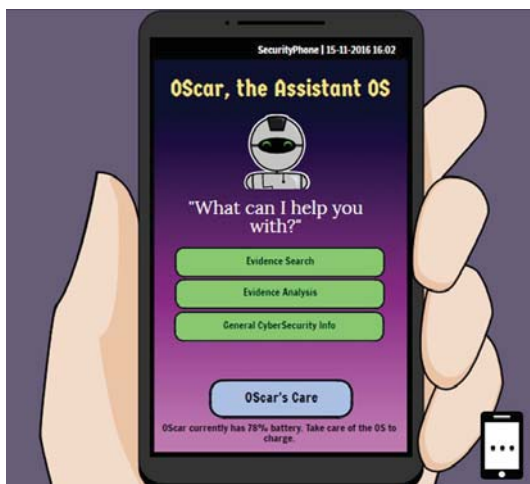
A.2 Detective Game



(a)



(b)



(c)



(d)



(e)



(f)



(g)



(h)



(i)



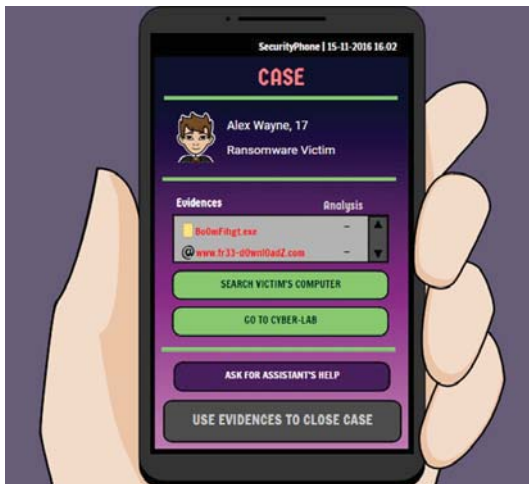
(j)



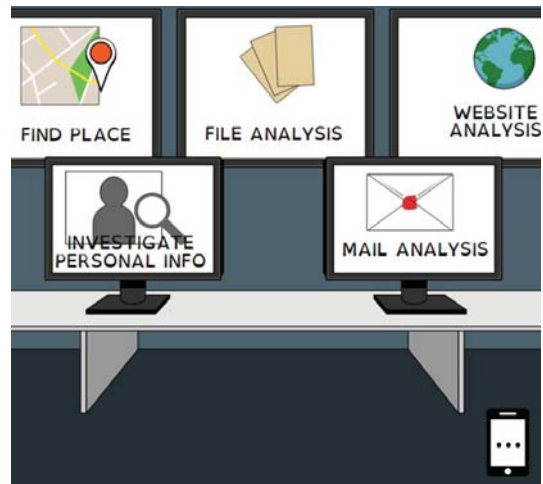
(k)



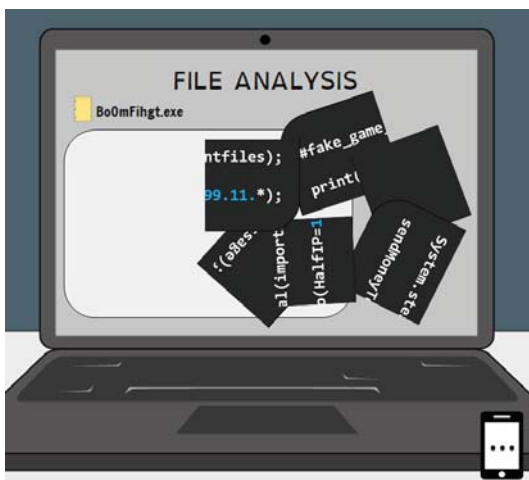
(l)



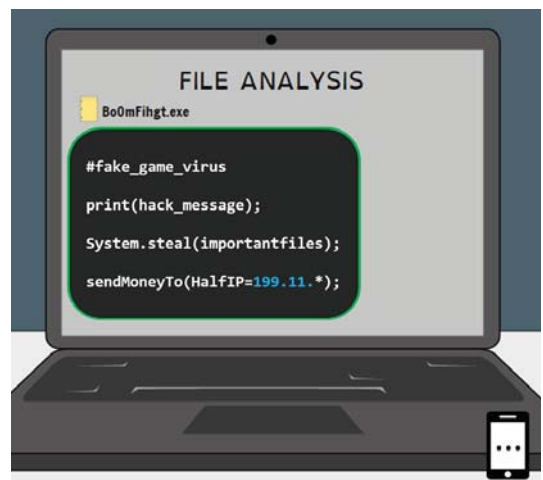
(m)



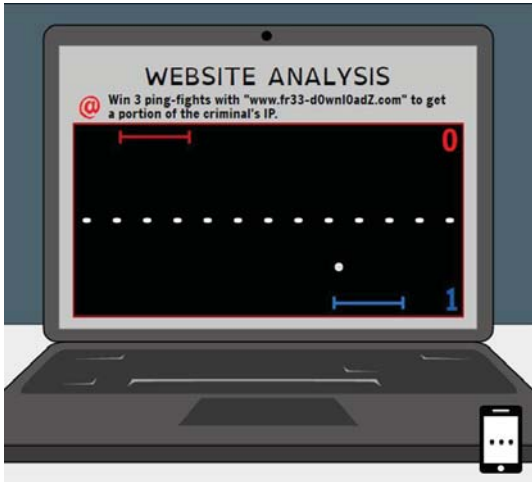
(n)



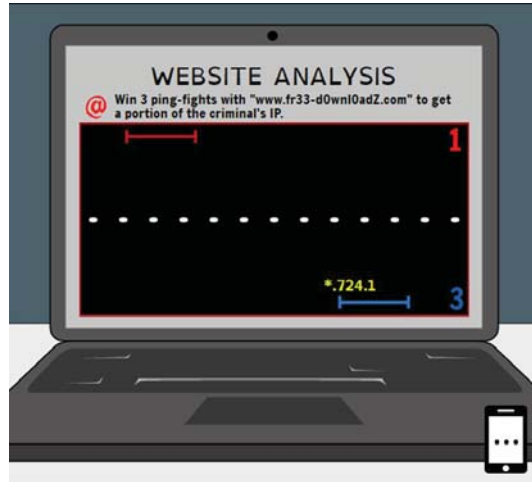
(o)



(p)



(q)



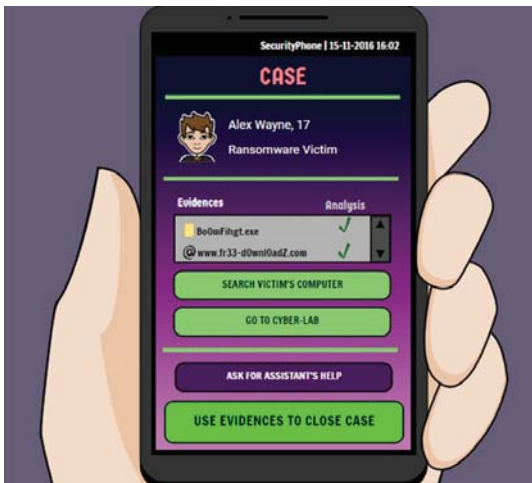
(r)



(s)



(t)



(u)



(v)

Figure A.2: Storyboard images illustrating the Detective Game idea.

Appendix B

Plot Storyboard

This appendix presents the storyboard of the story of the prototype, illustrated in the Figure B.1. The "File Search" mini game mentioned in the Figure B.1q was later changed to the Social Network mini game.



Introduction

Teen is in his room, checking his FB.

(a)



Suddenly, an ad for cheap brand sneakers appears on his feed.

(b)



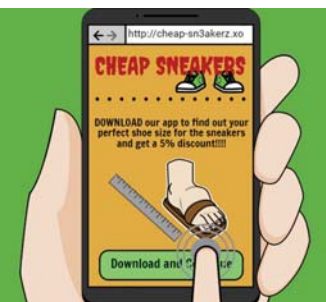
Since he's been craving some brand sneakers but had no money for them, he decides to check the site out.

(c)



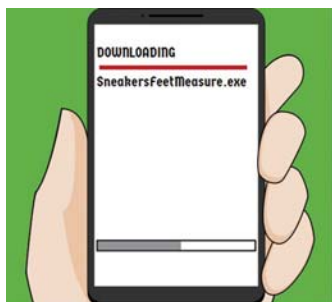
The website only lets the teen continue for the purchase page if he downloads an app that claims to measure his feet size.

(d)



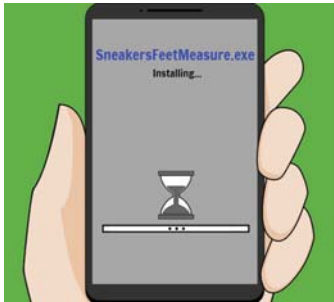
The teen proceeds to download the app.

(e)



He downloads it.

(f)



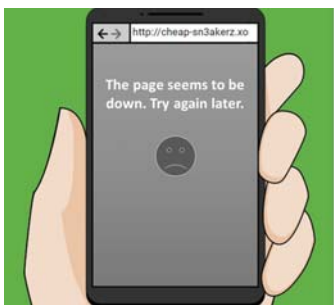
And install it.

(g)



After the installation, there seems to be no new app on the phone.

(h)



The website also seems to be down.

(i)



Oh well! Since it didn't work, the teenager forgets about the sneakers.

(j)



The teen then decides to go get a snack.

(k)



When the teen comes back, there seems to be something wrong with his phone.

(l)



There is a ransomware message blocking the device! Someone took over the teen files. The teen decides to get help from his parents, but they don't know what to do. 2000€ seems a lot of money, but the teen has important files on his phone. The family then decides to contact a cyber-detective.

(m)



Investigation Part

The teen goes to the cyber-police station and asks the detective for help. The detective takes over the case and promises the teen she'll try her best to recover his files.

(n)



(interactive part starts)
The player takes over the detective role and can roam in the station to get to the cyber-lab.

(o)



In the cyber-lab, there will be many lab-rooms, each one with a theme. (for example to analyze passwords, the player should go to the Password Room)

The player should follow a path to recover the files:

- Find which files are infected;
- Investigate the suspicious website and app;
- Use a tool similar to Kaspersky to decode the encrypted files.

To follow that path, the game can provide the player goals, that will help the player chose the room.

(p)



1st Goal: Find which files are infected
The player will then play a mini-game to discover which files are infected.
A good idea for the game is one that teaches the importance of backups of important files and the danger of explicit files (for example, semi-nude photos).

- The files infected found might be:
- An important school work (History.docx)
 - An embarrassing video (DancingInTheShowers.avi)

(q)



2nd Goal: Investigate the website and app
The player will then play a mini-game to analyze the suspicious website and app.
A good idea for the game is one that teaches how to find signs of suspicious websites and apps.

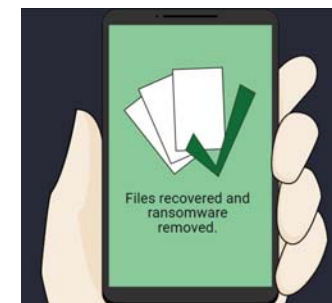
Analyzing the content, the detective finds that the ransomware code used by the hackers is on the Top 10 of the most common ransomware codes. This code encrypts the files with a cypher existent in a tool owned by the police, therefore the files can be recovered without paying the ransom.

(r)



3rd Goal: Decode the files
The player will then play a mini-game to decode the files and remove the ransomware.
A good idea for the game is one that teaches password security.

(s)



Finally, the files are recovered and the ransomware is removed.

(t)



The detective returns the device to the teen. He is very happy that he recovered his important files without paying 2000€ and promises he'll be more careful browsing suspicious webpages and downloading mysterious apps.

(u)

Figure B.1: Storyboard images illustrating the prototype plot.

Appendix C

Social Network Notifications List

This appendix contains the possible notification pop-ups that a player can encounter in the *Social Network Analysis* Mini Game, illustrated in the Figures C.1, C.2 and C.3.

C.1 Friend Requests



(a) Friend Request 1



(b) Friend Request 2



(c) Friend Request 3



(d) Friend Request 4



(e) Friend Request 5



(f) Friend Request 6



(g) Friend Request 7



(h) Friend Request 8



(i) Friend Request 9

Figure C.1: Possible friend request notifications.

C.2 Messages



(a) Message 1



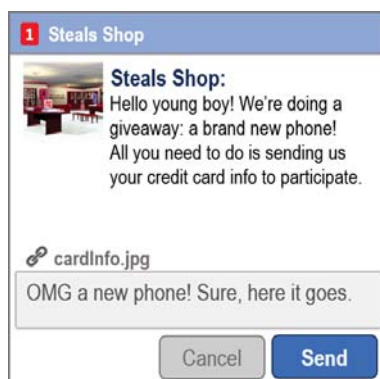
(b) Message 2



(c) Message 3



(d) Message 4



(e) Message 5



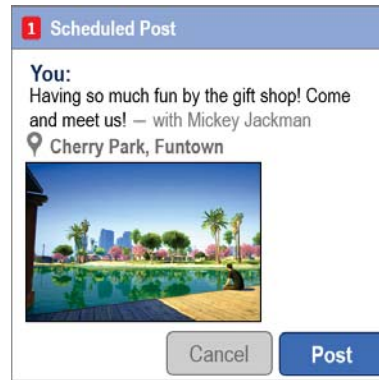
(f) Message 6

Figure C.2: Possible message notifications.

C.3 Scheduled Posts



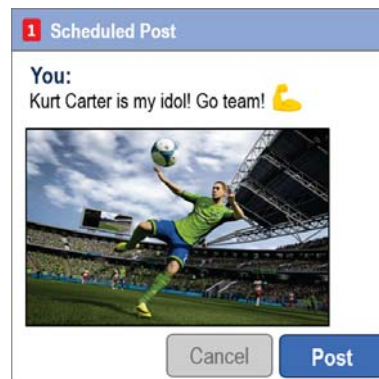
(a) Scheduled Post 1



(b) Scheduled Post 2



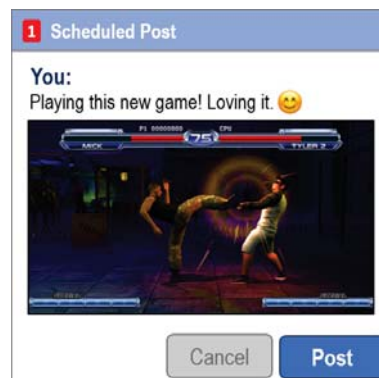
(c) Scheduled Post 3



(d) Scheduled Post 4



(e) Scheduled Post 5



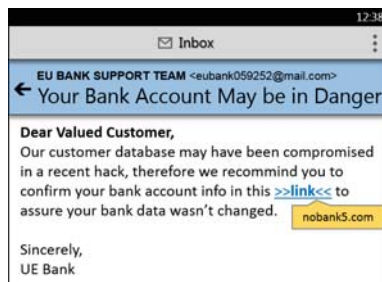
(f) Scheduled Post 6

Figure C.3: Possible scheduled post notifications.

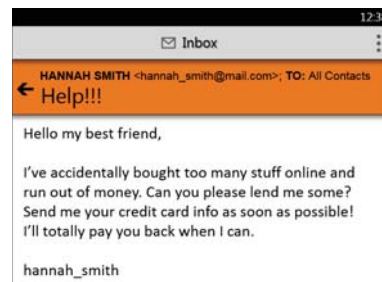
Appendix D

Phishing Detector Screens List

This appendix contains the possible phishing screens that the player can encounter in the *Phishing Detector* Mini Game. These screens are illustrated in the Figure D.1.



(a) Screen 1



(b) Scheduled Post 2



(c) Screen 3



(d) Screen 4



(e) Screen 5



(f) Screen 6

Figure D.1: Possible Phishing screens.

Appendix E

Password Decoder - Password Elements Lists

This appendix contains the possible elements contained in the passwords of the levels of the *Password Decoder Mini Game*.

E.1 Suspects

Name, Birthyear and Country Code of the suspect.

- Henry, 1978, AUS
- Pierre, 1991, FRA
- Nicolai, 1987, RUS
- Filippo, 1993, ITA
- Tao, 1989, CHN
- Ewald, 1975, DEU
- Ekber, 1984, TUR
- Ramon, 1990, ESP
- Adriano, 1986, PRT
- Ramsey, 1974, GBR
- Marshall, 1997, USA
- Berit, 1992, SWE
- Feliks, 1985, POL
- Stamatis, 1995, GRC
- Matheus, 1994, BRA
- Keiko, 1998, JPN
- Pascual, 1988, COL
- Ansgar, 1983, NOR

E.2 Top 10 Most Common Used Passwords

- 123456
- password
- 12345
- 12345678
- football
- qwerty
- 1234567890
- 1234567
- princess
- 1234

E.3 Top 10 Dictionary Words Most Used in Passwords

- football
- baseball
- dragon
- monkey
- mustang
- access
- shadow
- master
- superman
- batman

Appendix F

Knowledge Quiz

The Knowledge Quiz done by the students in the scope of the Tests described in chapter 5 is illustrated in the following pages. The quiz is written in portuguese.

NOME

IDADE

Seguidamente ser-te-ão colocadas perguntas para testar alguns dos teus conhecimentos acerca de temáticas da ciber-segurança.

Escolhe a opção que consideres correcta.

1. O QUE ENTENDES POR RANSOMWARE?

- É um *software* malicioso (*malware*) que se infiltra em sistemas de computador de forma ilícita.
- É um *software* malicioso que restringe o acesso a um sistema infetado e exige pagamento pela recuperação do mesmo.
- É um programa de computador que recolhe informações sobre o utilizador e sobre os seus hábitos na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do mesmo.
- É o mesmo que um antivírus.

2. O QUE ENTENDES POR PHISHING?


- É o ato de alegar falsamente ser uma entidade credível, como uma empresa ou organização, numa tentativa de fazer a vítima entregar informações pessoais que serão utilizadas para fins indesejáveis.
- É um videojogo de simulação de pesca.
- É o ato de usar ferramentas tecnológicas com o objetivo de perseguir ou assediar uma pessoa.
- É um programa de computador que recolhe informações sobre o utilizador e sobre os seus hábitos na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do mesmo.

3. NAS PRÓXIMAS IMAGENS SÃO REPRESENTADOS PEDIDOS DE AMIZADE DA REDE SOCIAL FACEBOOK. PARA CADA IMAGEM, INDICA A OPÇÃO QUE CONSIDERES SEGURA.



- Posso aceitar o pedido porque tenho 3 amigos em comum com a pessoa, apesar de não a conhecer.
- Não é seguro aceitar o pedido pois não conheço a pessoa.

1 Pedido de Amizade




Carlos Silva
81 Amigos em Comum
"Olá, conhecemo-nos ontem na festa de anos da Patrícia!"

Ignorar Aceitar

- Posso aceitar o pedido porque para além de conhecer pessoalmente a pessoa, tenho bastantes amigos em comum.
- Não é seguro aceitar o pedido porque não conheço bem a pessoa.

1 Pedido de Amizade




Tiago Roque
78 Amigos em Comum
"Da próxima vez que te vir a olhar para a minha namorada *prepara-te para lebares porrada em frente à turma toda.*"

Ignorar Aceitar

- Posso aceitar o pedido pois é um colega da minha turma e tenho 78 amigos em comum com a pessoa em questão.
- Não é seguro aceitar o pedido porque a pessoa em questão me está a ameaçar.

4. NAS PRÓXIMAS IMAGENS SÃO REPRESENTADAS MENSAGENS DA REDE SOCIAL FACEBOOK. PARA CADA IMAGEM, INDICA A OPÇÃO QUE CONSIDERES SEGURA.

1 Melhor Amigo (Marco Salvado)



Marco Salvado:
Olá, mandas-me então o teu CC como tínhamos combinado para inscrever a nossa equipa de futebol no torneio? Abraço!

[cc.pdf](#)

Claro! Aqui vai!

Cancelar Enviar

- Posso enviar a mensagem porque confio na pessoa.
- Posso enviar a mensagem, porém prefiro passar o documento por uma *pen* ao meu colega para não circular o meu cartão de cidadão na internet.
- Não é seguro enviar um documento pessoal pela internet.

1 Loja Baratinho



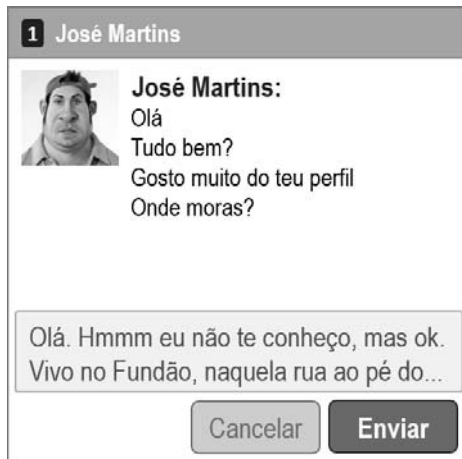
Loja Baratinho:
Olá. Estamos a fazer um sorteio do novo iPhone e foste escolhido para participar! Para te inscreveres só precisas de nos enviar uma fotografia do teu cartão de crédito, apenas como garantia!

[infoCartao.jpg](#)

OMG um iPhone! Claro, aqui vai!

Cancelar Enviar

- Posso enviar a mensagem.
- Não é seguro enviar um documento pessoal pela internet.



- Posso enviar a mensagem.
- Não é seguro revelar informação pessoal na internet, principalmente com desconhecidos.

5. NAS PRÓXIMAS IMAGENS SÃO REPRESENTADAS PUBLICAÇÕES DA REDE SOCIAL FACEBOOK. PARA CADA IMAGEM, INDICA A OPÇÃO QUE CONSIDERES SEGURA.



- Posso publicar a fotografia sem problemas.
- Posso publicar a fotografia, mas sem identificações e sem localização.
- Posso publicar a fotografia, mas apenas depois abandonar o local.
- Não é seguro publicar a fotografia.

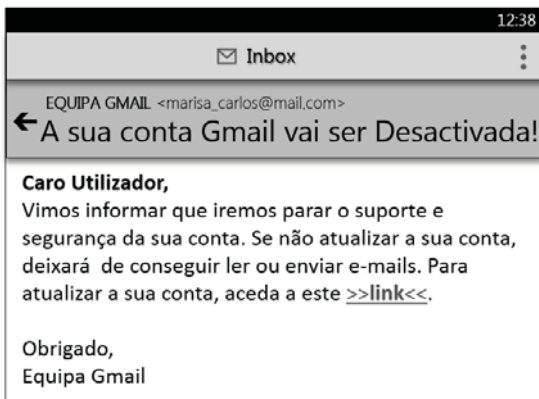


- Posso publicar o vídeo da minha colega sem problemas.
- Posso publicar o vídeo, se a minha colega der autorização.
- Não é seguro publicar o vídeo porque a minha colega está numa situação embaraçosa.

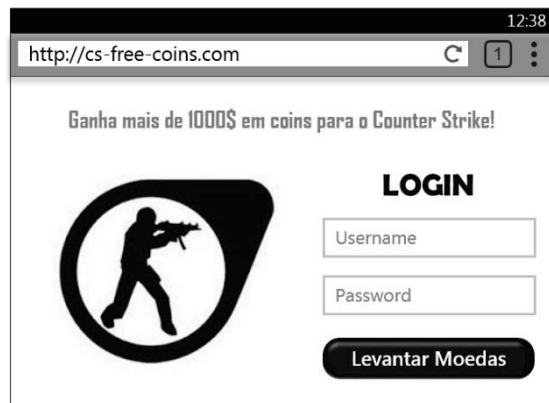


- Posso publicar a fotografia do meu jogador de futebol preferido.
- Não é seguro publicar a fotografia.

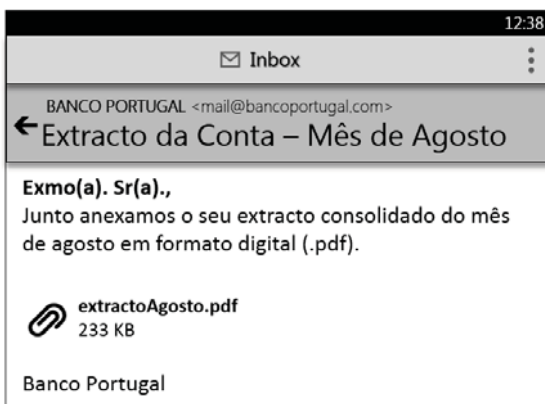
6. NAS PRÓXIMAS IMAGENS ESTÃO REPRESENTADOS E-MAILS E PÁGINAS DA INTERNET. PARA CADA IMAGEM, INDICA SE DESCOBRISTE ALGO SUSPEITO OU NÃO NOS E-MAILS OU PÁGINAS.



- O e-mail é uma tentativa de burla.
- O e-mail **não** é uma tentativa de burla.



- A página é uma tentativa de burla.
- A página **não** é uma tentativa de burla.



- O e-mail é uma tentativa de burla.
- O e-mail **não** é uma tentativa de burla.

7. QUAIS SÃO OS ELEMENTOS QUE CONSIDERAS NECESSÁRIOS PARA CONSTRUIR UMA PASSWORD FORTE?

8. DAS SEGUINTESS PASSWORDS, QUAL CONSIDERAS A MAIS SEGURA?

- | | |
|---|---|
| <input type="checkbox"/> MarianaPatriciaMartins | <input type="checkbox"/> olaamigostudobem? |
| <input type="checkbox"/> dzrt4ever | <input type="checkbox"/> asdfghjkl |
| <input type="checkbox"/> q\$audadesdoV3rao | <input type="checkbox"/> Tenho2gatinhos |
| <input type="checkbox"/> tiaguinhoSLB | <input type="checkbox"/> #YOLO |
| <input type="checkbox"/> snoopdog2001 | <input type="checkbox"/> 123Qwerty987654321 |
| <input type="checkbox"/> password | <input type="checkbox"/> ilovesara |

Appendix G

Questionnaire

The questionnaire completed by the students to evaluate the game in the scope of the Tests described in chapter 5 is illustrated in the following pages. The questionnaire is written in portuguese.

NOME

IDADE

Seguidamente ser-te-ão feitas algumas perguntas acerca do jogo que jogaste.

PARTE 2 - AVALIAÇÃO DO JOGO

PREENCHE AS SEGUINTEs TABELAS SEGUNDO A ESCALA APRESENTADA.

| Fluxo do jogo | Discordo totalmente | Discordo | Não concordo nem discordo | Concordo | Concordo totalmente |
|--|---------------------|----------|---------------------------|----------|---------------------|
| Percebi sempre qual era a tarefa a cumprir. | | | | | |
| Encontrei sempre a ação correta a tomar sem esforço. | | | | | |
| Percebi sempre que ao executar certa ação completaria a correspondente tarefa. | | | | | |
| Apercebi-me sempre do progresso feito ao cumprir tarefas. | | | | | |

| Temáticas do jogo | Discordo totalmente | Discordo | Não concordo nem discordo | Concordo | Concordo totalmente |
|--|---------------------|----------|---------------------------|----------|---------------------|
| Utilizo um <i>smartphone</i> todos os dias. | | | | | |
| Utilizo a internet todos os dias. | | | | | |
| Utilizo redes sociais todos os dias. | | | | | |
| Percebi as temáticas do jogo. | | | | | |
| As temáticas do jogo são algo com que lido no dia-a-dia. | | | | | |
| A ciber-segurança e os perigos da internet são algo que me preocupa. | | | | | |

| Gráficos e mini-jogos | Discordo totalmente | Discordo | Não concordo nem discordo | Concordo | Concordo totalmente |
|--|---------------------|----------|---------------------------|----------|---------------------|
| Os gráficos do jogo eram adequados. | | | | | |
| Compreendi a história do jogo. | | | | | |
| A mobilidade no jogo era boa. | | | | | |
| O minijogo das redes sociais era difícil. | | | | | |
| O minijogo do <i>phishing</i> era difícil. | | | | | |
| O minijogo das passwords era difícil. | | | | | |

| Didática | Discordo totalmente | Discordo | Não concordo nem discordo | Concordo | Concordo totalmente |
|--|---------------------|----------|---------------------------|----------|---------------------|
| Este jogo ensinou-me acerca das temáticas tratadas. | | | | | |
| Acho que o tipo de jogo se adequa à temática. | | | | | |
| Gostava de utilizar uma versão completa deste jogo para aprender mais sobre ciber-segurança. | | | | | |
| Preferia aprender sobre ciber-segurança com um videojogo do que com palestras/vídeos/aulas. | | | | | |

ENCONTRASTE ALGUM PROBLEMA NO JOGO? QUAL?

QUE MELHORIAS PROPUNHAS PARA O JOGO?

OBRIGADA POR PARTICIPARES NOS TESTES, FOSTE UMA GRANDE AJUDA!