UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

VICTOR WOHLERS CARDOSO

Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo *Phishing*

RIO DE JANEIRO
2024

VICTOR WOHLERS CARDOSO

Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo *Phishing*

Trabalho de conclusão de curso de graduação apresentado ao Instituto de Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientadores: Prof. Claudio Miceli,
Prof. Evandro Macedo,
Profa. Silvana Rossetto

RIO DE JANEIRO
2024

CIP - Catalogação na Publicação

C645s

Cardoso, Victor Wohlers
Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo phishing / Victor Wohlers Cardoso. -- Rio de Janeiro, 2024.
62 f.

Orientador: Evandro Luiz Cardoso Macedo.
Coorientador: Claudio Miceli de Farias.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Instituto de Computação, Bacharel em Ciência da Computação, 2024.

1. Engenharia Social. 2. Phishing. 3. Gamificação. 4. Cibersegurança. 5. Conscientização. I. Cardoso Macedo, Evandro Luiz, orient. II. de Farias, Claudio Miceli, coorient. III. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

VICTOR WOHLERS CARDOSO

Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo *Phishing*

Trabalho de conclusão de curso de graduação apresentado ao Instituto de Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em 6 de agosto de 2024

BANCA EXAMINADORA:

Documento assinado digitalmente
gov.br
EVANDRO LUIZ CARDOSO MACEDO
Data: 19/08/2024 18:55:10-0300
Verifique em https://validar.iti.gov.br

Evandro Luiz Macedo
D.Sc. (UFRJ)

Documento assinado digitalmente
gov.br
CLAUDIO MICELI DE FARIAS
Data: 20/08/2024 17:52:13-0300
Verifique em https://validar.iti.gov.br

Claudio Miceli de Farias
D.Sc. (UFRJ)

Documento assinado digitalmente
gov.br
SILVANA ROSSETTO
Data: 20/08/2024 22:00:41-0300
Verifique em https://validar.iti.gov.br

Silvana Rossetto
D.Sc. (UFRJ)

Documento assinado digitalmente
gov.br
DANIEL SADOC MENASCHE
Data: 20/08/2024 20:32:24-0300
Verifique em https://validar.iti.gov.br

Daniel Sadoc Menasché
Ph.D. (UFRJ)

Documento assinado digitalmente
gov.br
DIEGO LEONEL CADETTE DUTRA
Data: 20/08/2024 19:19:41-0300
Verifique em https://validar.iti.gov.br

Diego Lionel Cadette Dutra
D.Sc. (UFRJ)

Gostaria de primeiramente dedicar este trabalho ao meu avô Homero, que me apoia, me incentiva, e é meu exemplo de vida que o trabalho duro e a determinação sempre compensam.

Aos meus pais, Renato e Maria Helena, que me apoiam, me incentivam a alcançar meus sonhos e torcem pelo meu sucesso em todas as fases da minha vida.

A minha noiva Gabriele, com quem divido todos os momentos da minha vida. Obrigado por me apoiar e acreditar em mim mesmo quando eu mesmo não acreditava. Você é a minha luz e estar ao seu lado é meu maior presente.

Por fim, aos meus amigos do Clube das *Winx* e Amigoslol, que acompanharam minha jornada pela UFRJ e seu companheirismo tornou os momentos mais tranquilos e descontraídos.

AGRADECIMENTOS

Gostaria de expressar meus sinceros agradecimentos os meus orientadores, Silvana Rosseto, Claudio Miceli, que me apoiaram e acolheram minhas ideias, desempenhando um papel exemplar, mesmo com mudanças nos planos e especialmente ao Evandro Macedo, que me acolheu no Laboratório Ravel, em um momento transitório da minha vida.

Agradeço também ao Professor Luís Felipe que, ao me aceitar como parte do laboratório Ravel, me deu a oportunidade de aprender e praticar meus conhecimentos sobre segurança da informação.

Por fim, agradeço a todos os participantes do formulário de pesquisa, pois suas respostas foram cruciais para finalização desta monografia.

"The human. Now you know all about your target."

Kevin Mitnick

RESUMO

Com o aumento das ameaças de engenharia social, especialmente por meio de ataques de *phishing*, há uma necessidade crescente de soluções que envolvam os usuários de maneira proativa na defesa contra essas ameaças. Este trabalho propõe uma abordagem focada no fator humano, em vez de depender exclusivamente de soluções automatizadas baseadas em aprendizado de máquina e inteligência artificial, investigando a viabilidade do uso de um aplicativo móvel gamificado como ferramenta complementar no combate ao *phishing*. Uma revisão do estado da arte foi conduzida, examinando a literatura sobre treinamentos de cibersegurança e o uso de elementos de jogos para engajar os usuários. O aplicativo desenvolvido foi projetado para desafiar os usuários a reconhecer e responder a ataques de *phishing* através de simulações e desafios interativos. A avaliação do aplicativo foi realizada por meio de um formulário no qual os participantes foram questionados sobre os aspectos lúdico e educativo do aplicativo, bem como forneceram sugestões para melhorias. Os resultados indicaram uma receptividade positiva ao aplicativo, sugerindo um engajamento e interesse crescente à medida que os usuários respondiam os desafios de *phishing* e adquiriam pontos. Este trabalho contribui para a compreensão do papel da gamificação na educação e treinamento sobre cibersegurança e fornece reflexões para o desenvolvimento de ferramentas educacionais para campanhas de conscientização contra ataques baseados em engenharia social.

Palavras-chave: engenharia social; *phishing*; gamificação; cibersegurança; conscientização; aplicativo móvel.

ABSTRACT

With the increase of social engineering threats, especially through attacks of *phishing*, there is a growing need for solutions that involve users in a proactive way in the defense against these threats. This study proposes an approach focused on the human factor, instead of relying exclusively on automated solutions based on machine learning and artificial intelligence, investigating the feasibility of using a gamified mobile application as a complementary tool in the fight against *phishing*. A review of the state of the art was conducted, examining the literature on cybersecurity training and the use of game elements to engage users. The developed application was designed to challenge users to recognize and respond to attacks of *phishing* through simulations and interactive challenges. The evaluation of the application was carried out through forms in which the participants were questioned about the playful and educational aspects of the application, as well as provided suggestions for improvements. The results indicated a positive receptivity to the application, suggesting growing engagement and interest as users faced *phishing* challenges and collected points. This work contributes to the understanding of the role of gamification in education and training on cybersecurity and provides reflections for the development of educational tools for awareness campaigns against social engineering.

Keywords: social engineering; *phishing*; gamification; cibersecurity; awareness; mobile application

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

SVM	*Support Vector Machine*
ELM	*Extreme Learning Machines*
LR	*Linear Regression* (Regressão Linear)
PWA	*Progressive Web App*
URL	*Uniform Resource Locator*
HTML	*HyperText Markup Language* (Linguagem de Marcação de HiperTexto)
MVP	*Minimum Viable Product* (Produto Mínimo Viável)
LABRAVEL	Laboratório de Redes de Alta Velocidade
SSL	*Secure Socket Layer*

SUMÁRIO

1 INTRODUÇÃO

No contexto de segurança cibernética, engenharia social é um tipo de ataque no qual um agente malicioso explora vulnerabilidades humanas através de interações sociais para violar a segurança cibernética de um indíviduo, ou organização, utilizando, ou não, de meios tecnológicos (WANG; SUN; ZHU, 2020). Por se tratar de um ataque que o vetor principal é o elo mais fraco de um sistema seguro, isto é, os humanos, os criminosos que utilizam desta técnica se aproveitam de sentimentos e falhas dos seres humanos como ganância, empatia, conformidade e ignorância para roubar informações pessoais e valiosas. Por isso, o meio pelo qual o ataque pode ser reproduzido é bastante diverso, variando de *emails*, mensagens de texto, *web sites* e *softwares*. No mundo digital, ataques que utilizam da engenharia social estão cada vez mais comuns e são considerados um dos ataques cibernéticos mais poderosos contra sistemas atualmente (SALAHDINE; KAABOUCH, 2019).

1.1 MOTIVAÇÃO

Dentre as diversas técnicas que utilizam engenharia social, é necessário destacar o *phishing*. Esse ataque influencia uma vítima, através de engenharia social, para revelar informações pessoais, como endereço de email, nome de usuário, senha ou informações financeiras (ALABDAN, 2020). Um relatório feito pelo time de Inteligência de Ameaças da IBM constatou que em 2022, 42% dos ataques que resultaram em incidentes de segurança tiveram seu início com uma tentativa de *phishing* através de email, (X-FORCE, 2023), evidenciando importância da educação e treinamento dos usuários dos sistemas, principalmente sobre os riscos envolvidos em ataques do tipo phishing.

1.2 PROBLEMA

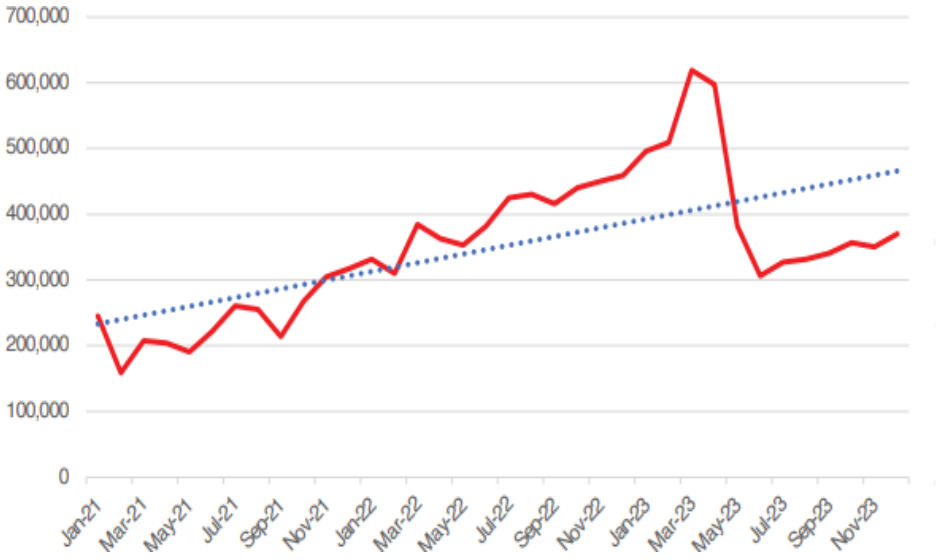
De acordo com um *survey*[1] global feito com profissionais de TI, conduzido em países como Estados Unidos, Canada e Alemanha, os ataques de engenharia social são experienciados por empresas de todos os tamanhos, sendo que 32% das empresas participantes do *survey* experienciaram pelo menos 25 ataques deste tipo. Além disso, segundo o relatório feito pela *Anti-Phishing Working Group*[2], houve um crescimento substancial no número de ataques de *phishing* entre os anos de 2021 e 2023, como é ilustrado na Figura 1. Apesar de ser possível ver uma expressiva queda na quantidade de ataques à partir de Janeiro de 2023, devido a um fechamento de uma grande empresa de registro de DNS, segundo a

[1] Disponível em: https://www.pressetext.com/nfs/166/633/pdf/2.pdf. Acesso em: 13 jul. 2024

[2] Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf. Acesso em: 13 jul. 2024

APWG, o ano de 2023 foi decretado como o pior ano para *phishing* chegando a 5 milhões de ataques.

Figura 1 – Ataques de Phishing 2021 – 2023



Fonte: APWG Report, 2024

Portanto, por conta da constante ameaça que os ataques de engenharia social apresentam aos sistemas e aplicações, se faz necessário desenvolver técnicas eficazes que tenham foco nos usuários do sistema, visto que são o alvo principal dos ataques de engenharia social, para impedir o sucesso dos agentes maliciosos. Com o foco nos humanos, é fundamental educar as pessoas para entenderem como podem se proteger de eventuais tentativas de roubo de dados e informações pessoais e treiná-las com casos reais, sendo estes *phishing* ou não, para identificar possíveis padrões que possam ajudá-los a distinguir potenciais ataques que possam sofrer.

1.3 PROPOSTA

Esta monografia apresenta um aplicativo desenvolvido para dispositivos móveis que tem como objetivo facilitar a aprendizagem sobre a prevenção de incidentes e golpes cibernéticos, por meio de tópicos de estudo de curta duração e simplificados. O aplicativo permite que os usuários adquiram conhecimento através de uma leitura leve sobre conceitos relacionados à engenharia social e por meio de desafios interativos, os quais também validam a eficiência do aprendizado. Por fim, o aplicativo contará com elementos de gamificação, como pontos e sistemas de ranqueamento dos integrantes da plataforma, tornando a experiência de treinamento mais engajada e proveitosa (SCHÖBEL et al., 2021). Dessa forma, através de experiências de aprendizado *hands-on*, estes usuários terão maiores chances de reter informações e aplicar a situações do mundo real (JIA; BAO; YU, 2023).

1.4 INSPIRAÇÃO

Para a concepção da aplicação, algumas plataformas de treinamentos em segurança da informação e cibersegurança, além de aplicativos de telefone gamificados, foram utilizados de inspiração.

1.4.1 Duolingo

Duolingo é um aplicativo de telefone e *website* com o objetivo de ensinar línguas utilizando elementos gamificados como *rankings* dos usuários da plataforma, número máximo de respostas erradas, pontuação por lição feita, distintivos de conquistas, entre outros. Possui como público-alvo usuários das mais variadas faixas etárias e do mundo todo. Na Figura 2, é possível conferir um dos exemplos utilizados para gamificação, o ranqueamento de usuários e seus respectivos pontos. É por meio desses elementos de gamificação que este software garante que os estudantes de línguas continuem usando e dedicando seu tempo a aplicação, permitindo-lhes absorver o novo conhecimento de maneira bem-sucedida (FREEMAN et al., 2023).

Figura 2 – *Ranking* do Duolingo

Fonte: Positivo em Foco, 2021

1.4.2 Hacker Rangers

A plataforma de treinamento de usuários Hacker Rangers promove cultura de cibersegurança através da gamificação. Assim como o aplicativo discutido anteriormente, essa ferramenta corporativa oferece uma série de funcionalidades gamificadas, podendo citar algums exemplos como questionários, medalhas, simulações de *phishing*, *ranking* (Figura 3) e vídeos animados.

Além disso, são oferecidas aulas sobre engenharia social, onde o aluno aprende as mais recentes técnicas e ferramentas usadas por cibercriminosos e como usá-las ao seu favor para se proteger contra fraudes digitais (RANGERS, 2024).

Figura 3 – *Ranking* do Hacker Rangers

Fonte: Positivo em Foco, 2021

1.4.3 LetsDefend, Hackthebox e TryHackMe

LetsDefend, Hackthebox e TryHackMe são três plataformas gamificadas de ensino de segurança da informação que oferecem aos usuários uma experiência de aprendizagem através de simulações de condições reais de ataques ou exploração de vulnerabilidades

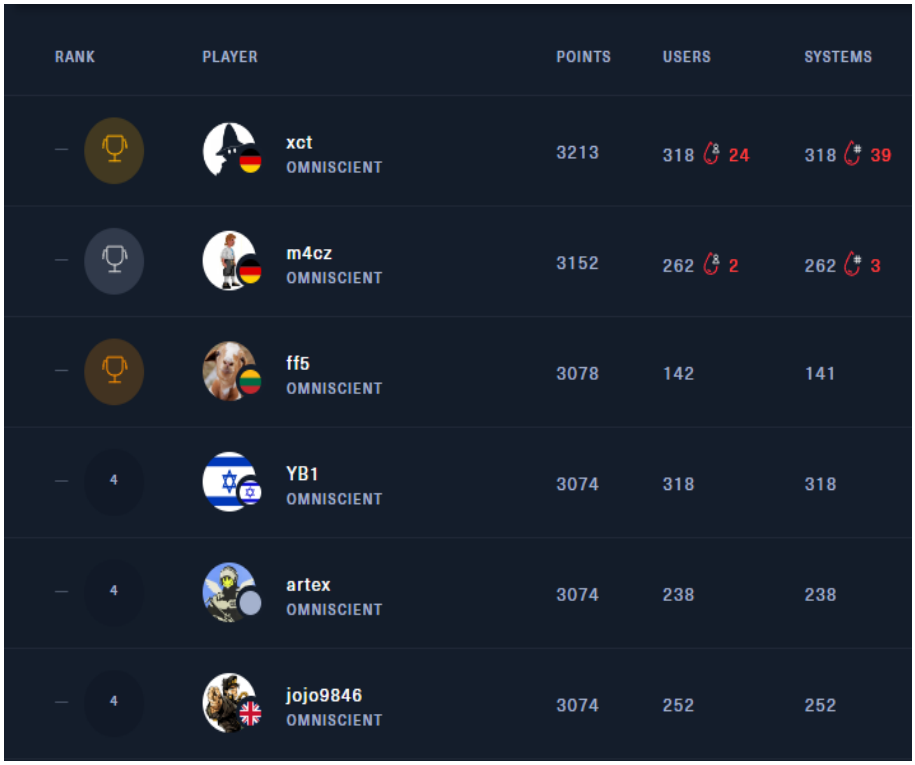
por meio de ambientes *sandbox*, onde o indivíduo pode interagir com máquinas virtuais e aplicar os conhecimentos adquiridos em aulas oferecidas pelas plataformas.

Como os demais programas citados anteriormente, os três oferecem funcionalidades gamificadas aos partificipantes, como *ranking* de usuários e medalhas, como pode ser ilustrado nas Figuras 4, 5 e 6.

Figura 4 – *Ranking* do LetsDefend

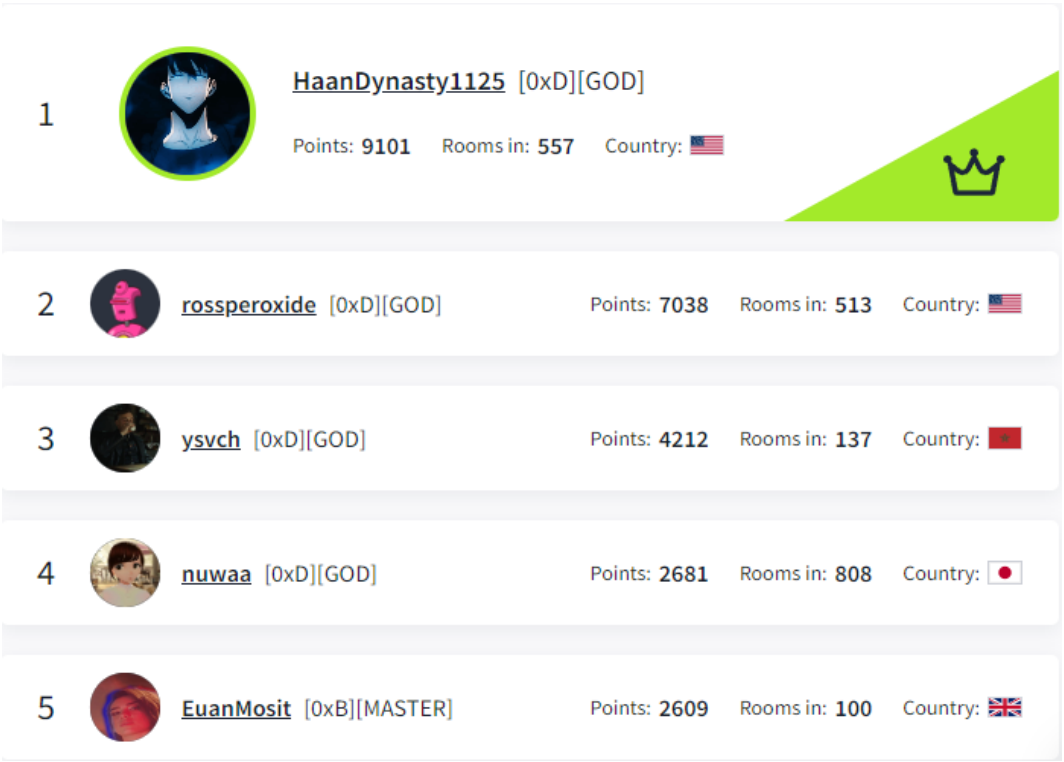
Fonte: LetsDefend, 2024

Figura 5 – *Ranking* do HackTheBox



Fonte: HackTheBox, 2024

Figura 6 – *Ranking* do TryHackMe



Fonte: TryHackMe, 2024

1.5 ESTRUTURA

O resto da monografia é organizado da seguinte forma. No Capítulo 2, serão contextualizados os vetores de ataque, os meios pelos quais as técnicas são executadas e as categorias da engenharia social, bem como a ideia por trás da gamificação do estudo e treinamento. No Capítulo 3, serão discutidos os trabalhos relacionados, avaliando o estado da arte das pesquisas por trás de técnicas de engenharia social, mais especificamente sobre *phishing* e as formas de se defender desses ataques, comparando propostas anteriores com esta que é desenvolvida nesta monografia. No Capítulo 4, é apresentada a proposta de aplicação para combater os problemas da utilização de engenharia social por criminosos através de um software de telefone de educação e treinamento gamificado, onde usuários podem aprender sobre como se defender através de tópicos informativos e concisos e desafios interativos. No Capítulo 5, a proposta é testada através de um formulário qualitativo para averiguar a eficácia do método proposto. Finalmente, no Capítulo 6, a monografia é concluída e trabalhos futuros são propostos.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são definidos alguns conceitos importantes para o entendimento completo da monografia. Além disso, a taxonomia existente na literatura, usada como base deste trabalho, é revisada.

2.1 CONCEITOS

2.1.1 Phishing

Como vista na Seção 1.1, *phishing* é uma das técnicas de engenharia social que tem como objetivo influenciar o alvo do ataque a revelar informações pessoais, através de vários métodos. Esse termo se originou da palavra *fishing*, que significa pescar. A lógica por trás dessa terminologia é que um ataque utiliza de uma isca para atrair potenciais vítimas (ALABDAN, 2020).

É possível encontrar na literatura conceitos que se aproveitaram da base teórica da palavra *phishing* para serem formados. Este é o caso de *smshing*, um ataque de engenharia social voltado para mensagens de texto e *vishing* que pertence a mesma família, porém utiliza chamadas de telefone para conduzir o ataque (YEBOAH-BOATENG; AMANOR, 2014).

2.1.1.1 Indicador de Phishing

São o conjunto de atributos que um email, uma mensagem de texto ou um *site* possuem que podem ser utilizados para ajudar a distinguir um ataque de *phishing*.

- Email: Os indicadores de *phishing* do email são o nome do remetente, o endereço de email do remetente, o título da mensagem e o corpo da mensagem.
- Mensagem de texto (SMS): Os indicadores de mensagem de texto são o número do remetente e o corpo da mensagem.
- URL: Já os indicadores de URL são a URL do site e a página *web* hospedada no site.

2.1.2 Gamificação

Gamificação, de acordo com (KAPP, 2012), envolve a adição de elementos de jogos e mecânicas para o conteúdo de aprendizado. Seu objetivo é transformar um conteúdo que é tipicamente apresentado como uma aula ou curso online e adicionar elementos baseados em jogos, como desafios e recompensas. Desta forma, cria-se uma oportunidade de

aprendizado gamificado em forma de aprendizado educacional ou experiência engajadora onde o aluno participa de desafios para aprender o conteúdo apresentado.

2.1.3 *Serious Game*

Serious Game é um termo usado para designar jogos que possuem o propósito específico relacionado a treinamentos, não apenas para diversão. Possui diversos elementos lúdicos, parecidos com jogos, porém eles têm um objetivo a ser atingido que já foi predeterminado (KIRYAKOVA; ANGELOVA; YORDANOVA, 2014), como aprender sobre *phishing*.

2.2 TAXONOMIA

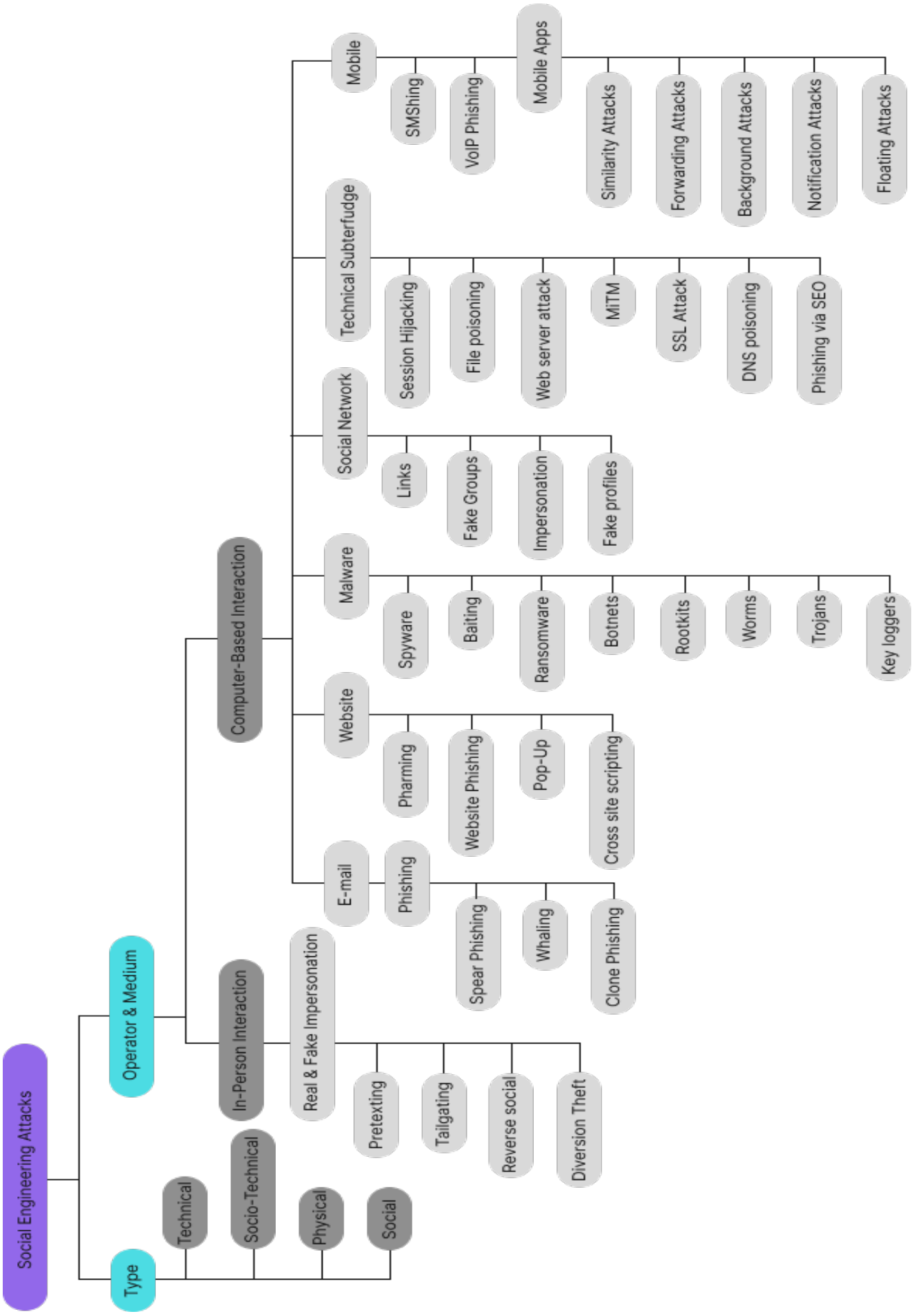
O presente trabalho utilizou a taxonomia desenvolvida por (ALDAWOOD; SKINNER, 2020) como base teórica para o desenvolvimento da proposta. Essa taxonomia diferencia os ataques de engenharia social por tipos e "meio/operador". Na categoria de tipo, é possível dividir em quatro seções, sendo elas (i) técnico, (ii) socio-técnico (ataques que utilizam de ferramentas técnicas e de persuasão e manipulação), (iii) físico e (iv) social. Por meio dessa divisão, é possível distinguir de maneira mais precisa quais ataques são de fato realizados usando ferramentas técnicas (do tipo técnico), uso de manipulação e persuasão (do tipo social), e a presença do atacante onde a vítima está localizada (do tipo físico).

Além disso, os autores definiram a diferença entre ataques que se baseam na interação pessoal ou na interação com computadores. Para a interação com pessoas, o artigo exemplificou alguns ataques que se aproveitam desse meio, como *pretexting*, *tailgating*, *quid pro quo* e *diversion theft*. Já nas interações com computadores, os autores do artigo decidiram dividir por qual meio de comunicação o ataque foi desenvolvido: Email, *Website*, *Malware*, Mídias Sociais, Telefone e Subterfúgio Técnico. Dentre alguns dos ataques que se encaixam em cada meio de comunicação, é possível citar o *phishing* de email, o *phishing* de *website* e o *smishing*.

Utilizando os conceitos definidos e as classificações utilizadas no trabalho desenvolvido por (ALDAWOOD; SKINNER, 2020), se tornou possível definir quais foram os conceitos abordados na presente monografia, como diferenciá-los e priorizar quais assuntos deveriam seria estudados para a elaboração do projeto proposto.

A Figura 7 exemplifica o diagrama criado para representar a taxonomia escolhida.

Figura 7 – Taxonomia da Engenharia Social



Fonte: (ALDAWOOD; SKINNER, 2020)

3 REVISÃO BIBLIOGRÁFICA

3.1 ENGENHARIA SOCIAL

A engenharia social sempre foi um problema relevante para a sociedade. Quando aplicada para fins maliciosos, ela pode ocasionar em roubo de informações e até perda de bens. A literatura vem tentando identificar as técnicas e ataques utilizados por criminosos e sugerir formas de mitigá-los.

Entre eles, o autor de (SALAHDINE; KAABOUCH, 2019) realizou uma revisão do estado da arte dos métodos que utilizam engenharia social, suas classificações e possíveis estratégias de detecção e prevenção. Entre as formas de detecção, o artigo menciona algoritmos de aprendizado de máquina e de inteligência artificial e como são eficientes na minimização do impacto desses ataques.

Entretanto, ele também enfatiza o quanto os ataques estão ficando cada vez mais sofisticados e o quão importante é também investir no lado não-técnico da prevenção, seja por meio de treinamento ou conscientização de usuários.

Além disso, artigos como (WANG; SUN; ZHU, 2020) tentam não só apontar os possíveis ataques, mas também definir o que é engenharia social no contexto da segurança cibernética, de forma a eliminar inconsistências e ambiguidades no uso do termo e propor uma definição precisa. Os autores revisaram o uso do termo ao longo das épocas em que a cibersegurança evoluiu e, através do método clássico da teoria da categorização, propuseram uma nova definição para o termo "engenharia social". Dessa forma, se torna possível eliminar a confusão gerada ao usar esse termo de forma equivocada e evitar generalização. Esse trabalho não só beneficia especialistas da área, mas pessoas que desconhecem do assunto e tem intenção de aprender para se proteger.

3.2 PHISHING COMO ATAQUE DE ENGENHARIA SOCIAL

Apesar de amplamente estudado na literatura especializada, o *phishing*, um método de ataque baseado em engenharia social, ainda é extremamente prejudicial para a Internet. Este ataque pode resultar em sérias consequências financeiras e de segurança, tanto para indivíduos quanto para organizações, causando perdas monetárias, roubo de identidade e comprometimentos de segurança em larga escala.

A crescente sofisticação dos ataques de *phishing* e a sua capacidade de se adaptar às novas tecnologias e comportamentos dos usuários tornam este um problema persistente e desafiador. Os atacantes frequentemente utilizam técnicas avançadas, como o uso de domínios quase idênticos aos legítimos e a personalização de mensagens para aumentar a taxa de sucesso dos ataques. Entre os métodos estudados para defender o usuário

final, temos as técnicas para detecção de *phishing* utilizando aprendizado de máquina e inteligência artificial que atualmente são apontadas como as mais eficazes. Em (BASIT et al., 2021), os autores fazem uma revisão bibliográfica dos melhores algoritmos para detecção de *websites* maliciosos. Entre eles, é possível destacar o trabalho de (CHEN; CHEN, 2019) que através da combinação de métodos de classificação como *Suport Vector Machine* (SVM), *Extreme Learning Machines* (ELM) e *Linear Regression* (LR), e métodos de seleção de *features* como o *Analysis of Variance* (ANOVA), os autores conseguiram chegar em uma acurácia de 99,2%. Porém, apesar de resultados altamente positivos, os autores reconhecem que a defesa mais eficaz contra ataques de *phishing* é um usuário educado sobre os perigos da Internet e bem informado sobre como se defender deles.

De contraste, os autores de (SARKER et al., 2024) investigaram, dentre artigos acadêmicos e *grey literature*, os desafios existentes na educação e conscientização de *phihsing*, bem como os pontos que levaram ao seu sucesso. Segundo o artigo, os usuários finais constituem a última linha de defesa contra esses ataques. Dentre os trabalhos estudados pelos autores, foi possível indicar que os estudos relacionados ao treinamento e a conscientização são mais numerosos que os de educação, evidenciando a importância de incorporar não só métodos para treinar os usuários como também formas de educar e fazê-los reter o conhecimento nos trabalhos relacionados a *phishing*.

Além disso, na pesquisa realizada pelo grupo, eles conseguiram coletar dados relevantes às principais dificuldades na implementação de métodos para educação e treinamento *anti-phishing*. Entre os desafios mencionados, é essencial citar a dificuldade de cativar a atenção das pessoas treinadas e a falta de engajamento, além do fato que soluções de jogos educacionais estudadas possuem interface complexa e de difícil uso por usuários não-experientes. Por outro lado, através de sua pesquisa, os autores conseguiram encontrar que o uso de elementos de gamificação e de treinamento interativos foi um fator de sucesso nos estudos relacionados à prevenção de *phishing*.

Foram esses desafios e sucessos apontados em (SARKER et al., 2024) que ajudaram a modelar e projetar a proposta desta monografia de aplicação gamificada e com elementos de interface de email conhecidos que ajudem a criar um paralelo com ações do cotidiano realizada pelos usuários do sistema.

3.3 GAMIFICAÇÃO NO ENSINO E TREINAMENTO DE PHISHING

Através da definição do foco na gamificação de soluções voltadas para a prevenção de *phishing*, foi possível identificar outros trabalhos que se propuseram a utilizar de artifícios gamificados para proporcionar aos indivíduos uma experiência engajadora e interessante. Aqui, são detalhados os artigos que foram estudados para a elaboração do aplicativo gamificado, bem como a comparação deles com a proposta desta monografia.

A literatura voltada para o estudo da gamificação aplicada ao ensino de alguma compe-

tência é bem diversa e os trabalhos desenvolvidos utilizam diversas técnicas para engajar os alunos e métodos para facilitar a compreensão de conceitos que, utilizando abordagens tradicionais, seriam mais custosos aprender. E quando são discutidos assuntos como *phishing*, é essencial utilizar de artifícios práticos para educar o usuário.

Autores como (CJ et al., 2018) exploraram a criação de uma aplicação que pudesse atender aos requisitos mencionados anteriormente. Através de um *Serious Game* desenvolvido para dispositivos *web*, procuraram contribuir para o treinamento de *phishing* para empresas, ajudando os colaboradores a reconhecer endereços URL mal intencionados. Entretanto, comparado a proposta apresentada nesta monografia, (CJ et al., 2018) não desenvolveu uma proposta que trouxesse uma simulação do mundo real, onde os participantes pudessem relacionar os ataques com os desafios apresentados a eles nas aplicações.

Isso se repete em trabalhos como (WEANQUOI; JOHNSON; ZHANG, 2018), (NIJLAND, 2022) e (LE et al., 2023) que propuseram soluções utilizando artifícios gamificados e, através de aplicações para celulares, criaram projetos voltados para o conhecimentos de técnicas de *phishing*, porém não implementaram elementos que fizessem o paralelo entre experiências reais e simuladas. Entretanto, diferente da proposta desenvolvida na presente monografia, que tirou amostras de um dataset público (PEIXOTO, 2024), os trabalhos citados anteriormente, principalmente (NIJLAND, 2022) e (LE et al., 2023) não utilizaram amostras reais para o treinamento dos participantes, mas perguntas criadas relacionadas aos assuntos escolhidos. Já em (WEANQUOI; JOHNSON; ZHANG, 2018), os autores não revelam qual *dataset* foi utilizado para a elaboração do treinamento.

Por outro lado, alguns artigos decidiram procurar outras abordagens para resolver esse problema. Foi o caso de (BASLYMAN; CHIASSON, 2016) que criou um jogo de tabuleiro com a temática de *phishing*. Os autores desenvolveram um sistema que pode conscientizar os participantes da partida e engajar discussões sobre o assunto enquanto tentam cumprir com o objetivo final (educação do jogador). Porém, por mais que os autores utilizassem artifícios que provoquem debates sobre o assunto e utilizassem linguagem de fácil entendimento, o recurso da simulação com situações do cotidiano e ambientes que lembrassem ataques reais não foram implementados.

Por fim, duas propostas criaram soluções que conseguiram, de maneira bem sucedida, aplicar simulação e dar *feedback* aos usuários. É o caso de (WEN et al., 2019) e (WIJAYA et al., 2022) que conseguiram criar um ambiente controlado que se aproximasse de atividades que vítimas de ataque poderiam sofrer, utilizando componentes de gamificação como pontos e *ranking* para promover engajamento entre os usuários e *feedback* para que possam aprender com seus erros. Entretanto, ambas as aplicações focaram em um público reduzido, como estudantes com experiência em TI e empresas (respectivamente), e não implementaram aplicações em dispositivos móveis que, como apontado em (LANE et al., 2016), é extremamente efetivo para treinamentos e desenvolvimento de habilidades.

Portanto, a proposta da presente monografia tem como contribuição a utilização de

tecnologias inclinadas para aplicativos móveis, voltado para o público geral, sendo estudantes, ou não e empresas interessadas em treinar seus funcionários. Além disso, é criado um ambiente que tente se aproximar de situações reais de ataques de *phishing*, utilizando amostras encontradas em *datasets* abertos. As ações relacionadas aos desafios propostos aos usuários serão identificadas e comentários serão enviados a eles com explicações sobre possíveis erros realizados nas simulações. Por fim, os modelos por trás da concepção da aplicação e os *endpoints* criados para a comunicação da interface com o servidor foram listados, capacitando futuros desenvolvedores com meios para a reprodução dos experimentos. A Tabela 1 exemplifica a comparação dos trabalhos.

Tabela 1 – Propostas de Gamificação do treinamento de Phishing

Artigo	Aplicação	Grupo	Simulação	Feedback	Amostras	Modelo
(CJ et al., 2018)	Web	Funcionários	Não	Sim	PhishTank	Sim
(WEANQUOI; JOHNSON; ZHANG, 2018)	Desktop e Mobile	Estudantes	Não	Sim	Não se aplica	Não
(NIJLAND, 2022)	Mobile	Estudantes	Não	Sim	Não se aplica	Não
(LE et al., 2023)	Mobile	Funcionários	Não	Sim	Não se aplica	Não
(BASLYMAN; CHIASSON, 2016)	Board Game	Pessoas 12+	Não	Sim	Não se aplica	Não
(WEN et al., 2019)	Desktop	Pessoas sem experiência em TI	Sim	Sim	Dataset Cornell TI	Não
(WIJAYA et al., 2022)	Protótipo	Funcionários	Sim	Sim	Não se aplica	Não
Minha proposta	Mobile/PWA	Público Geral	Sim	Sim	Phishingpot	Sim

Fonte: Elaboração própria

4 MODELAGEM E IMPLEMENTAÇÃO DA APLICAÇÃO

4.1 CONCEPÇÃO DA APLICAÇÃO

A partir da revisão dos artigos no Capítulo 3, foi possível perceber um foco na prevenção de ataques de *phishing* por meios de tecnologias como inteligência artificial e aprendizado de máquina. Entretanto, por mais sofisticadas que sejam as medidas de segurança e as ferramentas que protegem os usuários, é crucial preparar o próprio usuário para possíveis ataques que passem pelo filtro de defesa da segurança da informação.

Com essa perspectiva, o presente trabalho propõe um método de treinamento a partir de exemplos reais de emails maliciosos e emails legítimos e o participante precisa apontar, em uma quantidade de indicadores de *phishing* presentes no desafio, quais deles ajudaram a decidir se aquele era um ataque de um agente mal-intencionado ou não.

Para desenvolver a proposta de treinamento dos usuários contra os diversos tipos de *phishing*, foi idealizado um aplicativo de celular gamificado, onde o usuário possa aprender, com informações atuais e simplificadas, quais são as técnicas que ameaçam sua segurança, como identificá-las e como se defender, por meio de tópicos em formato de postagem de *blog* com ilustrações e *tags*. O texto será produzido com o objetivo de ser bastante informativo e de leitura leve, para abranger o público de idades variadas.

Além disso, através de desafios interativos oferecidos no *software*, é possível treinar a capacidade das pessoas de identificar tentativas de ataque e ajudar a entender quais são os indicadores que ela pode usar para conseguir discenir um *email*, mensagem de texto e site de *phishing*. Para tal, a interface por onde os usuários do sistema irão interagir com os desafios terá *design* semelhante à de outras interfaces de programas de *email*, mensagens de texto e navegadores *web* de forma tentar simular um evento real.

Por fim, os usuários do sistema poderão se adicionar em uma lista de amigos. Essa lista permite que eles criem grupos para poder visualizar seus ranqueamentos de pontos de forma filtrada. Essa funcionalidade tem em mente o público corporativo, para facilitar o controle dos responsáveis por trás do treinamento dos funcionários da empresa e público geral, para que possam criar comunidades entre amigos e competir.

4.2 PROCESSO DE SOFTWARE

O método utilizado para definir a prioridade das funcionalidades para a versão de *Minimum Viable Product* (MVP) foi a técnica de MoSCoW (DAVIS, 2012), de modo que cada função do aplicativo deve ser colocada dentro de quatro categorias que definem sua prioridade quanto a entrega da aplicação: *Must-Have* (deve ter), *Should-Have* (deveria ter), *Could-Have* (poderia ter) e *Won't-Have* (não terá). Dessa forma, foi identificado

que funcionalidades como cadastro e *login* de usuários no sistema, textos informativos e desafios sobre os ataques de *phishing* de email, e o ranqueamento de usuários são funcionalidades que devem ter, pois são fundamentais para a implementação da proposta. Funcionalidades que foram categorizadas como *Should-Have* foram identificadas, como uma interface similar à de serviços de email e perfil para visualização de pontos. Para *Could-Have*, funcionalidades de adição de amigos e criação de grupos foram indicadas, assim como a adição de desafios de mensagem de texto. As funcionalidades que acabaram sendo categorizadas como *Won't-Have* foram a adição de desafios personalizados com preferências do usuário e desafios de URL.

A partir desse mapeamento, foi possível criar diagramas que pudessem ajudar a ilustrar as possíveis funções listadas anteriormente, como elas interagem com os usuários do sistema, como seus componentes interagem entre si, quais são as principais ações que um ator do sistema pode realizar e qual é o fluxo principal das pessoas que utilizam o software proposto.

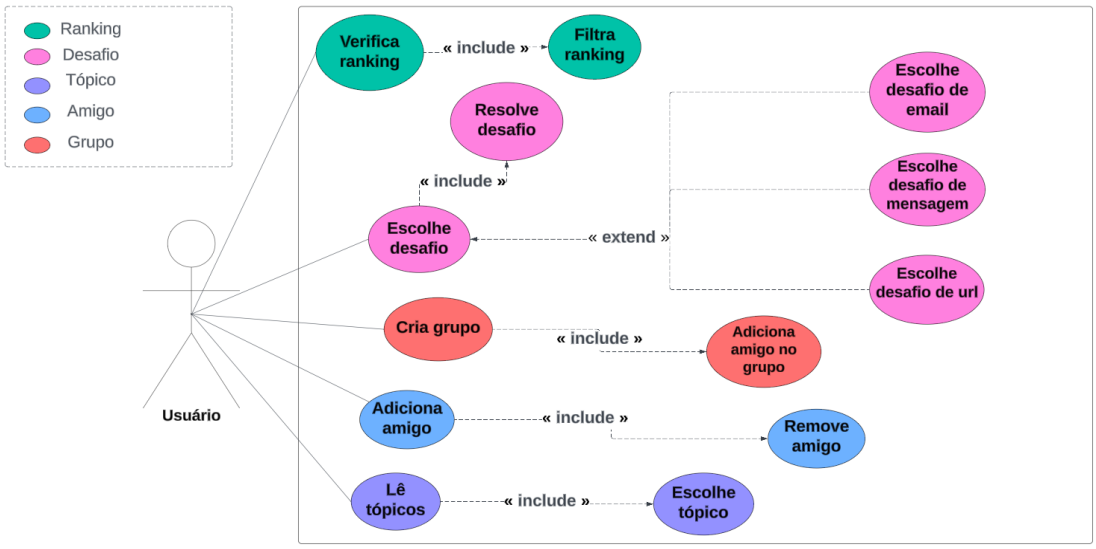
4.2.1 Diagrama de Casos de Uso

A partir do levantamento das funcionalidades essenciais através da técnica de MoSCoW, foi possível identificar apenas um ator, isto é, a pessoa que irá interagir com o sistema, o Usuário. Além do ator, foram listadas as interações dele com sistema. Entre elas estão:

- Escolher um desafio para ser resolvido (entre os de email, mensagem e URL)
- Resolver um desafio
- Adicionar usuários da lista de amigos
- Remover usuários da lista de amigos
- Criar um grupo a partir dos amigos adicionados
- Adicionar amigos no grupo criado anteriormente
- Escolher tópicos para ler
- Ler tópicos disponíveis
- Verificar ranking de pontos
- Filtrar ranking por pontuação

É possível verificar o diagrama e seus relacionamentos a partir da Figura 8. As cores agrupam as diferentes funcionalidades do sistema: *Ranking*, desafios, grupos, amigos e tópicos.

Figura 8 – Diagrama de Casos de Uso



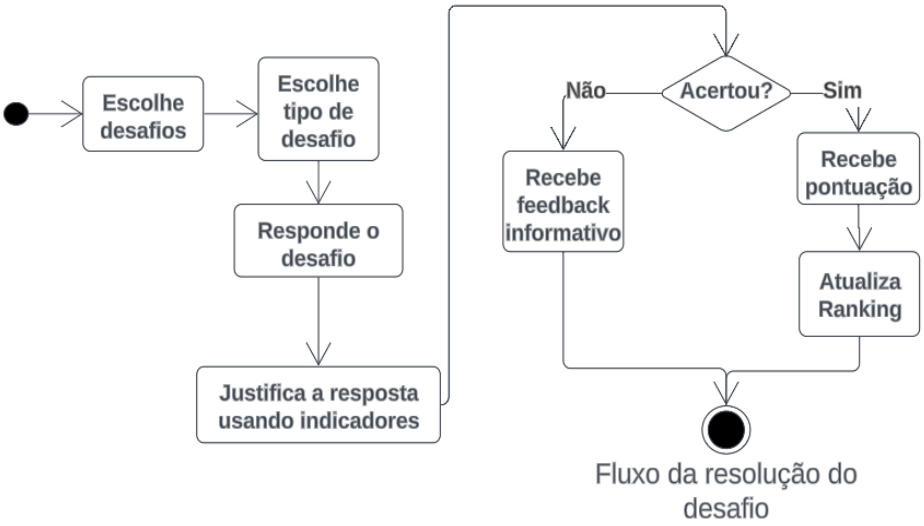
Fonte: Elaboração própria

4.2.2 Diagrama de Atividades

A idealização e concepção das possíveis atividades do usuário na aplicação permitiu visualizar e criar os diagramas que representassem o fluxo de uma pessoa nas ações principais do sistema: Resolver Desafios e Ler tópicos.

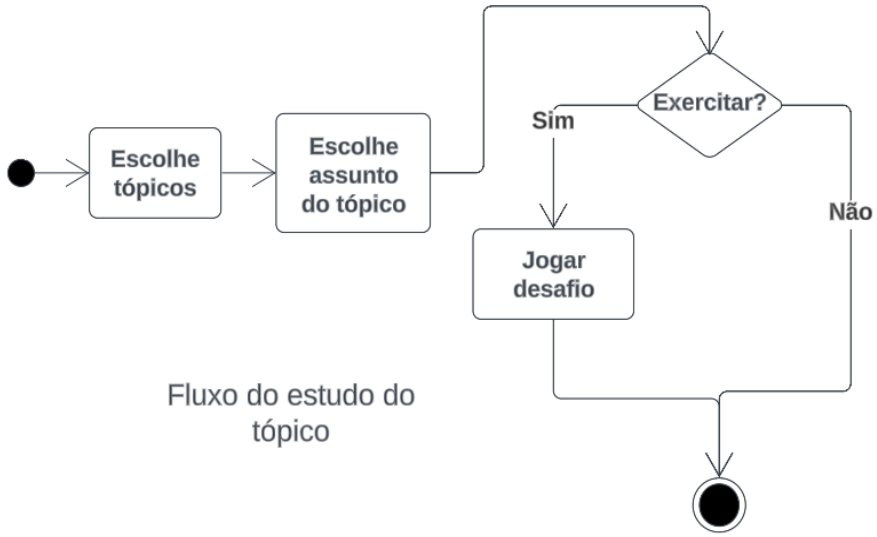
As Figuras 9 e 10 representam as interações necessárias para que o participante da aplicação realize as funcionalidades que permitem o aprendizado e o exercício dos ensinamentos adquirido nos tópicos.

Figura 9 – Diagrama de Atividades - Resolução de Desafios



Fonte: Elaboração própria

Figura 10 – Diagrama de Atividades - Ler Tópicos



Fonte: Elaboração própria

4.2.3 Diagrama de Classes

Após o mapeamento dos casos de uso e atividades no sistema, tornou-se possível listar quais a entidades desse projeto e como elas interagem entre si (Figura 11). Além do usuário (mencionado no diagrama de casos de uso), as entidades de desafio, tópico, indicador e grupo também foram identificadas:

a) Usuário: Seus atributos base são o nome de usuário, o nome da pessoa, seus pontos (que começam com 0 assim que for instanciado) e o email. Ele possui relacionamento N para N com desafio podendo ser nulo, relacionamento 1 para N e N para N com grupo (um usuário é dono de um ou mais grupos grupo e vários usuário pertencem à vários grupos).

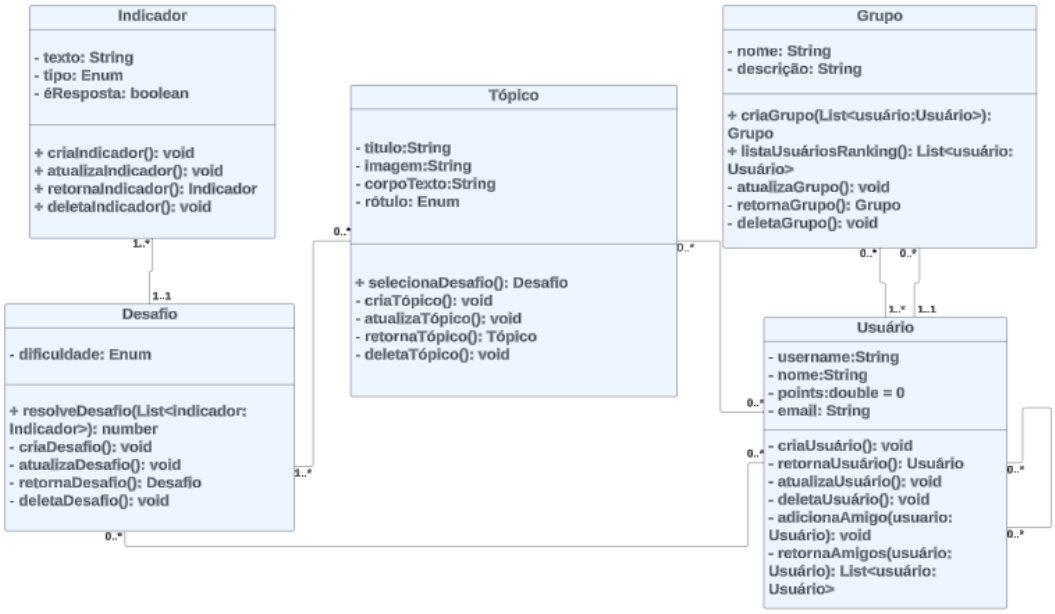
b) Tópico: Seus atributos base são o título do tópico, uma imagem, corpo do tópico e um rótulo que varia entre “EMAIL”, “SMS”, “WEB” e “SOCIAL_ENGINEERING”. Seus relacionamentos são de N para N com usuário (podendo ser nulo) e N para N com Desafio.

c) Grupo: Seus atributos base são o nome do grupo e sua descrição. Seus relacionamentos são de N para 1 e de N para N com usuário.

d) Indicador: Seus atributos base são texto, tipo do indicador (título, nome do remetente, endereço do rementente e corpo) e se ele é resposta ou não. Ele possui um único relacionamento com desafio de N para 1.

e) Desafio: Por fim, o desafio possui apenas a dificuldade de atributo. Ela pode ser “EASY”, “MEDIUM” e “DIFFICULT”. Esta entidade possui relacionamento 1 para N com indicador, N para N com tópico e N para N com usuário.

Figura 11 – Diagrama de Classes



Fonte: Elaboração própria

4.2.4 Diagrama de Sequência

Após a criação dos diagramas que ajudaram a facilitar a visualização dos casos de uso do sistema, as atividades que podem ser realizadas na aplicação e a interação das entidades e suas cardinalidades, foi possível montar um diagrama de sequência (Figura 12) que contemplasse as principais funções do aplicativo, as interações que o usuário tem com a interface, a interface com o servidor e o servidor com o banco.

4.3 GAMIFICAÇÃO

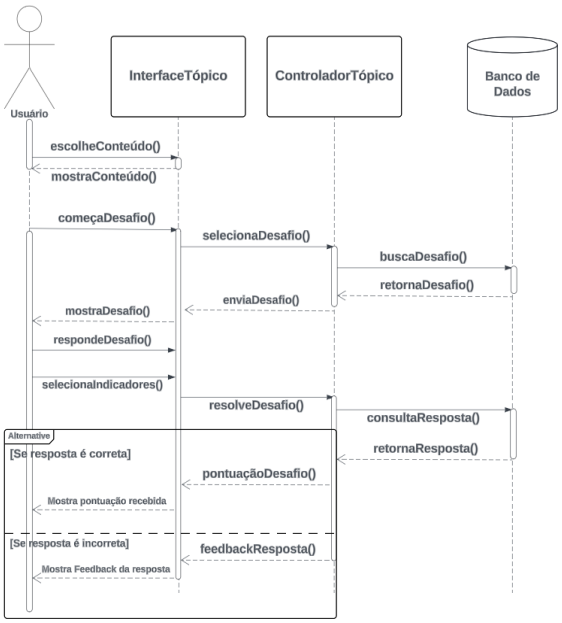
Como forma de introduzir elementos de gamificação para gerar uma experiência de treinamento e aprendizado ao usuário mais engajada e proveitosa (SCHÖBEL et al., 2021), o trabalho propõe a implementação de *Rankings* (geral e em grupo), desafios, pontos e sequência de desafios feitos, inspirados nos aplicativos e plataformas de ensino gamificada citados no Capítulo 1.

4.3.1 Pontuação

A pontuação pode ser dividida de duas formas: desafios com mensagens e URL legítimas e as de *phishing*.

No caso de desafios que são golpes, para recompensar a interação do usuário com os desafios feitos, o jogador receberá uma quantia de pontos relativa à quantidade de indicadores que ele acertou. Para cada indicador correto, o jogador receberá 50 pontos

Figura 12 – Diagrama de Sequência



Fonte: Elaboração própria

que serão usados para medir a colocação dele no *ranking*. Entretanto, como forma de bonificar a identificação de tentativas de *phishing* bem sucedida, o usuário ganhará 50 pontos adicionais se todos os indicadores forem corretamente identificados.

Por outro lado, nos desafios que são legítimos, o jogador não poderá indicar nenhum indicador como ilegítimo, ou seja, caso ele escolha qualquer indicador, ele não receberá nenhum ponto. Ele receberá pontos apenas se indicar que todos os indicadores são legítimos, ganhando o total de 250 pontos.

4.3.2 Desafios

Os desafios foram criados com o objetivo de proporcionar uma experiência engajadora aos aprendizes, podendo fazê-los exercitar os conhecimentos adquiridos nos tópicos em troca de pontos. Estes podem ser divididos em três tipos: Email, Mensagem de Texto e URL.

4.3.2.1 Email

Neste desafio, os usuários são convidados a identificar se os emails apresentados em uma interface semelhante à de um provedor de email convencional são tentativas de *phishing* ou não. Além de responder a essa pergunta, os participantes devem apontar quais indicadores de *phishing* os levaram a essa conclusão. Ao final, os usuários receberão uma pontuação conforme estabelecido na Seção Pontuação deste trabalho.

4.3.2.2 Mensagem de Texto

Para este desafio, o desafiante recebe uma amostra de uma conversa de texto e precisa responder se aquela é uma mensagem legítima ou um golpe, assim como ocorreu no desafio de *email*. Como definido no Capítulo de Fundamentação Teórica, os indicadores existentes nesse tipo de desafio são o nome da pessoa (podendo ser apenas um número de telefone ou o nome real) e o corpo da mensagem. Assim como mencionado anteriormente, a pontuação segue o formato definido na Seção de Pontuação.

4.3.2.3 URL

Por fim, o último desafio existente na plataforma é o de sites ou URL. Este desafio consiste em identificar, dado um exemplo mostrado ao usuário, se aquela URL é real ou falsa. Ademas, será apresentado o conteúdo da página carregada ao acessar a URL na tela, para ajudar o jogador na decisão. Como os demais desafios, a pontuação segue o que foi definido nas Seções anteriores.

4.3.3 Ranking

O ranqueamento dos usuários pode ser divido de duas formas: O ranqueamento global e o ranqueamento por grupo. O *Ranking* global é onde os usuários podem verificar sua pontuação e posição em relação a todos os participantes da plataforma. Já a versão de grupo é utilizada para competir entre amigos ou entre colegas de trabalho, caso estejam participando em um treinamento de segurança da informação. Essa funcionalidade pretende facilitar o controle do *ranking* dos pontos dos colaboradores por parte das empresas que estão aplicando o treinamento.

Para que o ranqueamento de grupo seja visualizado, primeiro é necessário ter adicionado um usuário na lista de amigos. Dessa forma, é possível garantir que apenas pessoas que aceitaram uma solicitação de amizade anteriormente podem ser adicionadas em grupos.

4.3.4 Sequência de Desafios Feitos

Por fim, o aplicativo terá um recurso de rastreio da quantidade de vezes que um desafio foi feito. Sempre que um usuário entrar na aplicação e resolver um desafio de maneira bem sucedida (ganhar algum ponto), o contador de sequência de desafios será incrementado. A partir dessa funcionalidade, participantes poderão acompanhar sua constância no aprendizado e treinamento de *phishing*.

4.4 IMPLEMENTAÇÃO DO SOFTWARE

Para poder materializar a solução idealizada até aqui, foi criado uma aplicação do tipo *Progressive Web App* (PWA) para a prova de conceito neste trabalho, como forma de facilitar o teste entre usuários de diferentes plataformas de celular. O software foi dividido em duas camadas: o Front-end, responsável pela experiência e interação do usuário, além da visualização da interface, e o Back-end, responsável por processar as requisições recebidas e gerenciar a parte lógica dele. Além disso, para esta primeira versão, foi escolhido o foco em tópicos e desafios de *phishing* por email, visto que ainda são usados em quase 42% dos ataques que resultaram de incidentes de segurança, segundo os estudos mencionados na Seção 1.1.

4.4.1 Amostras de Email

Um ponto-chave para que essa aplicação sirva seu propósito é utilizar amostras de *phishing* coletadas por algum *honeypot*. Entre as disponíveis atualmente, foi optado por escolher uma criada pelo usuário rf-peixoto do Github. Junto de outras pessoas, ele foi responsável por reunir mais de 1800 amostras. Para disponibilizar todos os arquivos, ele decidiu disponibilizar em seu repositório criado no Github (PEIXOTO, 2024).

4.4.2 Banco de Dados

O banco de dados utilizado para o desenvolvimento da solução proposta foi o PostgreSQL, uma base de dados que usa o paradigma relacional e é *open-source*.

4.4.3 Lógica de Negócio

A Seção lógica da aplicação foi desenvolvida utilizando a linguagem de programação Typescript, uma versão atualizada e com a implementação de tipos de variáveis do Javascript. Além disso, para realização *back-end* de forma facilitada, foi utilizado o NestJs, um *framework* progressiva de Node.Js para construir aplicações eficientes, escaláveis e confiáveis (NESTJS, 2024). Por fim, foi adicionado a biblioteca TypeORM para facilitar a interação entre o banco de dados e a parte da codificação no *back-end*.

Foram criados *endpoints* para cada entidade existente no sistema, como mapeado no diagrama de classes anteriormente. Adicionalmente, dois *endpoints* foram criados para executar as funções de *login* e registro da aplicação. Essas funcionalidades são cruciais para cadastrar e liberar o acesso a um potencial usuário ao sistema. Abaixo, são listadas as funções de cada entidade, bem como o tipo de requisição (por parâmetro ou por corpo), método utilizado (dentre os existentes no protocolo HTTP), o que é esperado que ela receba do usuário e o que ele deve retornar ao mesmo.

4.4.3.1 Autenticador

O autenticador (Quadro 1), apesar de não ser uma entidade, é uma classe controladora das funções de autenticação do sistema, entre elas o registro de uma nova conta e o *login* dessa mesma conta.

Quadro 1 – *Endpoints* de Autenticação

Endpoint	Funcionalidade	Tipo	Método	Argumentos	Retorno
register	Registra um usuário no sistema	Corpo	Post	*Username*, nome, email e senha	Objeto Usuário Criado
login	Autentica o usuário no sistema	Corpo	Post	Email e senha	Bearer Token

Fonte: Elaboração própria

4.4.3.2 Tópico

A entidade Tópico (utilizada apenas pelos gerenciadores da aplicação) controla as ações relacionadas aos tópicos de *phishing*. O Quadro 2 exemplifica suas funções.

Quadro 2 – *Endpoints* de Tópico

Endpoint	Funcionalidade	Tipo	Método	Argumentos	Retorno
topic	Cria um tópico	Corpo	Post	Token, título, texto, imagem e rótulo	Objeto Tópico
topic	Retorna todos os tópicos do sistema	N/A	Get	Bearer Token	Array de Objetos Tópico
topic/:id	Retorna tópico do sistema	Parâmetro	Get	Bearer Token e Id do tópico	Objeto Tópico
topic/:id	Atualiza informações do tópico	Parâmetro e Corpo	Put	Bearer Token e Id do grupo	N/A
topic/:id	Deleta o tópico do sistema	Parâmetro	Delete	Bearer Token e Id do tópico	N/A

Fonte: Elaboração própria

4.4.3.3 Grupo

A entidade Grupo governa as ações relacionada aos grupos, compostos por usuários. Entre as ações é possível citar a criação do grupo, adicionar novos usuários, listar todos os grupos, listar o ranking de usuários por ponto e sair de um grupo, como pode ser visto no Quadro 3.

Quadro 3 – *Endpoints* de Grupo

Endpoint	Funcionalidade	Tipo	Método	Argumentos	Retorno
group	Cria um grupo	Corpo	Post	Bearer Token, nome, descrição e lista de usuários	Objeto Grupo
group/users	Adiciona usuário ao grupo	Corpo	Post	Bearer Token, Id do grupo e lista de usuários	Objeto Grupo Atualizado
group	Retorna todos os grupos	N/A	Get	Bearer Token	Array de Objetos Grupo
group/:id	Retorna um grupo	Parâmetro	Get	Bearer Token e Id do grupo	Objeto Grupo
group/:id /ranking	Retorna o ranking de usuários do grupo	Parâmetro	Get	Bearer Token e Id do grupo	Array de Objetos Usuários organizado
group/:id	Atualiza informações do grupo	Bearer Token, Id do grupo e corpo	Put	Bearer Token, nome e descrição	N/A
group/:id/users /:userid	Remove usuários do grupo	Corpo	Delete	Bearer Token, Id do grupo e Id do usuário	N/A
group/leave/:id	Usuário se retira do grupo	Parâmetro	Delete	Token e Id do grupo	N/A
group/:id	Apaga grupo do sistema	Parâmetro	Delete	Bearer Token e Id do grupo	N/A

Fonte: Elaboração própria

4.4.3.4 Indicador

A entidade Indicador é uma entidade complementar. Ela é de utilidade para a entidade de desafio, visto que a existência de Indicadores dependem da criação de um desafio. Além disso, funções como retornar indicadores, atualizar e deletar (Quadro 4) não serão acessíveis por usuários comuns, visto que a criação de indicadores, assim como a de tópicos, é feita a partir de uma análise e coleta de amostras de *phishing* e, portanto, precisa ser verificada e minuciosamente desenvolvida pelos organizadores do sistema/aplicação.

Quadro 4 – *Endpoints* de Indicador

Endpoint	Funcionalidade	Tipo	Método	Argumentos	Retorno
indicator	Cria um Indicador	Corpo	Post	Bearer Token, título, texto, imagem e rótulo	Objeto Indicador
indicator	Retorna todos os indicadores do sistema	N/A	Get	Bearer Token	Array de Objetos Indicador
indicator/:id	Retorna indicador do sistema	Parâmetro	Get	Bearer Token e Id do indicador	Objeto Indicador
indicator/:id	Atualiza informações do indicador	Parâmetro e Corpo	Put	Bearer Token e Id do indicador	N/A
indicator/:id	Deleta o indicador do sistema	Parâmetro	Delete	Bearer Token e Id do indicador	N/A

Fonte: Elaboração própria

4.4.3.5 Desafio

Por fim, temos os endpoints da entidade de Desafio. Essa classe vai comportar todas as funções que interagem com os desafios da aplicação, entre elas, a criação de desafios, o retorno de todos os desafios ou algum em específico, a atualização dos desafios, a remoção deles e a resolução de um desafio. Assim como os tópicos e os indicadores, essas entidades são criadas pelos organizadores do sistema, visto que precisam de um acompanhamento mais específico para sua criação. No Quadro 5, é possível verificar quais são todos os endpoints e suas funcionalidades.

Quadro 5 – *Endpoints* de Desafio

Endpoint	Funcionalidade	Tipo	Método	Argumentos	Retorno
challenge	Cria um Desafio	Corpo	Post	Bearer Token, dificuldade do desafio, lista de indicadores	Objeto Desafio
challenge/solve	Resolve um desafio	Corpo	Post	Bearer Token, Id do desafio e um objeto de respostas de indicadores	Quantidade de pontos e lista de Objetos Indicador Incorretos
challenge	Retorna todos os desafios do sistema	N/A	Get	Bearer Token	Lista de Objetos Desafio
challenge /difficulty/:id	Retorna todos os desafios da dificuldade escolhida	Parâmetro	Get	Bearer Token e Número do desafio	Lista de Objetos Desafio
challenge/:id	Retorna um Desafio	Parâmetro	Get	Bearer Token e Id do desafio	Objeto Desafio
challenge/:id	Atualiza um desafio	Parâmetro e Corpo	Patch	Bearer Token e Id do desafio, dificuldade e lista de Objetos Indicador	N/A
challenge/:id	Deleta um Desafio	Parâmetro	Delete	Bearer Token e Id do desafio	N/A

Fonte: Elaboração própria

4.4.3.6 Usuário

A entidade Usuário governa todas as ações relacionadas ao usuário após se registrar e entrar na aplicação. Isso inclui adicionar e deletar uma outra pessoa a lista de amigos, procurar usuários no sistema e desafios que o usuário já fez. Os *Endpoints* podem ser visualizados no Quadro 6.

Quadro 6 – *Endpoints* de Usuários

Endpoint	Funcionalidade	Tipo	Método	Argumentos	Retorno
user/friend/:id	Adiciona um usuário a lista de amigos	Parâmetro	Post	Bearer Token e Id	N/A
user	Retorna todos os usuários do sistema	N/A	Get	N/A	Array de Objetos Usuário
user/ranking	Retorna todos os usuários do sistema em ordem descrescente de pontos	N/A	Get	N/A	Array de Objetos Usuário
user/friends	Retorna todos os amigos do usuário	N/A	Get	Bearer Token	Array de Objetos Usuário
user/challenges	Retorna todos desafios que o usuário fez	N/A	Get	Bearer Token	Array de Objetos Desafio
user/:id	Retorna um usuário do sistema	Parâmetro	Get	Bearer Token e ID de Usuário	Objeto Usuário
user/search	Retorna usuários do sistema que batem com a busca	Corpo	Post	Bearer Token, Email, nome ou nome de usuário	Array de Objetos Usuário
user/profile	Atualiza as informações do usuário	Corpo e Bearer Token	Put	Bearer Token, Id do usuário, nome de usuário, nome e email	N/A
user/friend/:id	Remove um usuário da lista de amigos	Parâmetro	Delete	Token e Id do usuário amigo	N/A
user	Apaga usuário do sistema	N/A	Delete	Token	N/A

Fonte: Elaboração própria

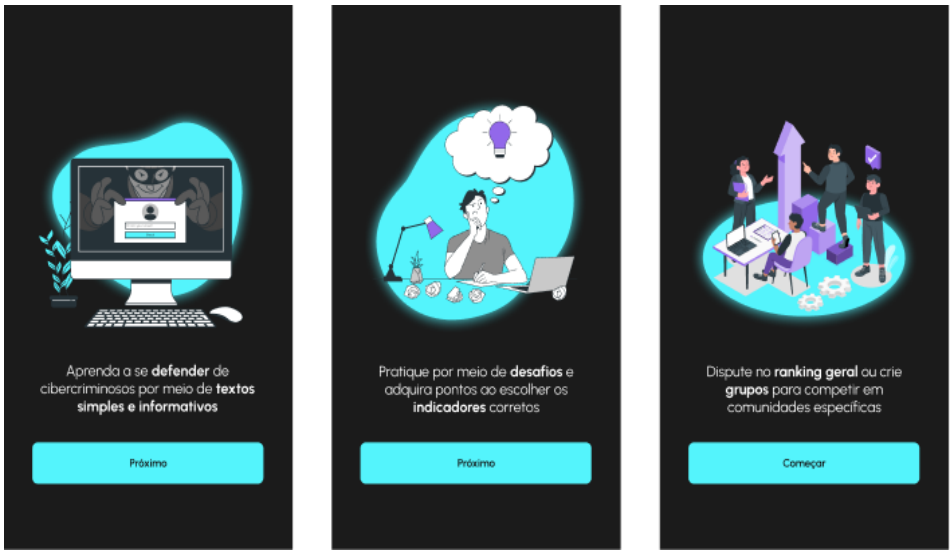
4.4.4 Interface da Aplicação

A parte visual do *software* foi desenvolvido utilizando a *framework* React para auxiliar no desenvolvimento dos componentes que fazem parte das telas do PWA. A linguagem de programação utilizada é o Typescript (assim como foi utilizado na parte lógica) e a criação da estrutura das páginas foi feita utilizando HTML e CSS, linguagens da *web* que auxiliam na customização de interfaces. É neste módulo da aplicação que ocorre a integração entre a camada lógica e camada de interação com o usuário. Nas subseções seguintes, é possível visualizar a divisão das telas e suas funcionalidades.

4.4.4.1 *Onboarding*

As telas de *Onboarding* foram criadas para poder familiarizar o usuário com as tarefas que ele irá desempenhar, além de citar algumas das funcionalidades mais importantes. Como é possível ver na Figura 13, elas foram divididas em três partes para não sobrecarregar o usuário com informação e explicar, de forma simples, como ele pode interagir com a solução.

Figura 13 – Telas de *Onboarding*



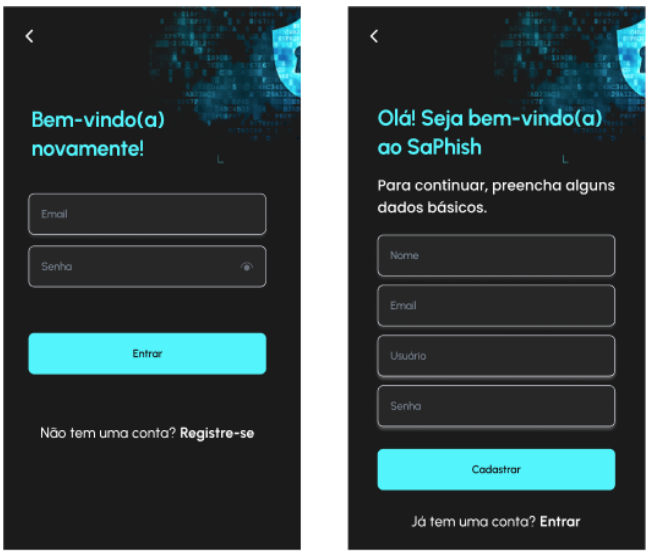
Fonte: Elaboração própria

4.4.4.2 *Login* e Cadastro

Após a introdução inicial, os participantes são convidados a criar uma conta para que possam interagir com a aplicação. São requisitados dados como nome, email, usuário e senha. Para logar, basta apenas informar email e senha. Tanto o nome como o email são importantes para a criação personalizada e imersão dos desafios. Em ambas as telas, existe a opção de ser redirecionada para a outra, caso a pessoa possua ou não a conta.

Na Figura 14 é possível visualizar as telas mencionadas.

Figura 14 – Telas de *Login* e Cadastro



Fonte: Elaboração própria

4.4.4.3 Tela Inicial, Trilha e Tópicos

Um usuário devidamente logado consegue ter acesso à tela inicial da aplicação. Nela, é possível escolher um tópico de interesse para aprender. Estes tópicos estão apresentados em formato de cartões. Na concepção da proposta desta monografia, três tópicos foram idealizados: email, mensagens de texto e *website*. Entretanto, como mencionado na Seção 4.4, apenas o tópico de email foi implementado. Ao clicar nesses cartões, o usuário é redirecionado para a tela de trilha de tópicos, possibilitando acompanhar todos os tópicos de um assunto.

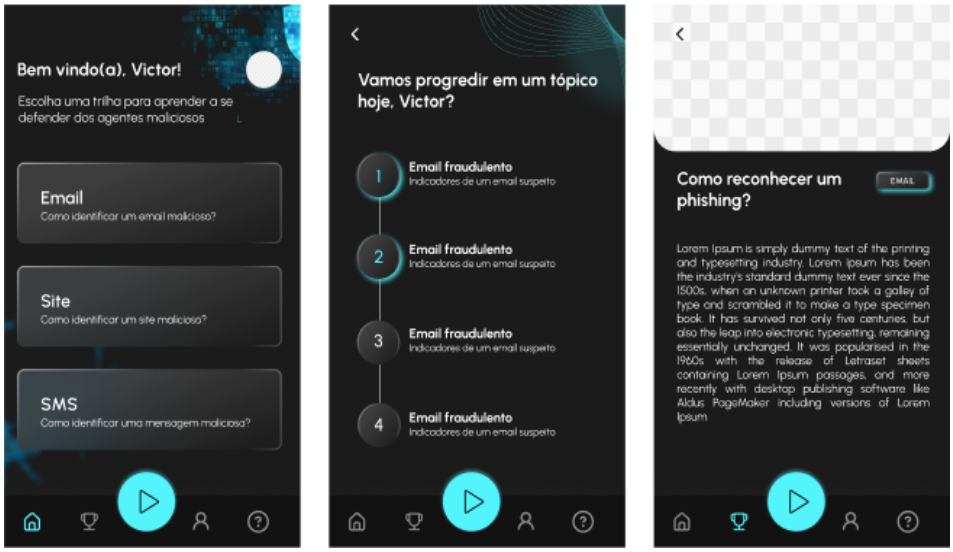
Escolhendo um dos itens da trilha, o aprendiz consegue estudar sobre o assunto de interesse, por meio de de uma interface em formato de postagem de *blog*, como apresentado na Figura 15.

4.4.4.4 Perfil

A tela de perfil (Figura 16) é utilizada para verificar algumas informações sobre o usuário logado, como pontos, grupos que a pessoa está (e caso algum deles foi criado pela mesma, a funciondalidade de deletar é apresentada), funcionalidades de adição de amigos e criação de grupos.

Além disso, no canto superior direito da tela, é possível deslogar, retornando para a página de *login*.

Figura 15 – Tela Inicial, Trilha e Tópicos



Fonte: Elaboração própria

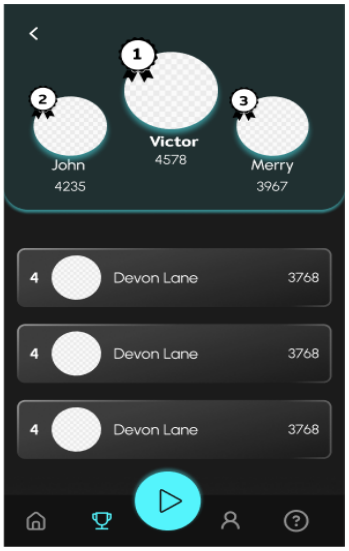
Figura 16 – Tela de Perfil

Fonte: Elaboração própria

4.4.4.5 *Ranking*

Ao clicar no ícone de troféu na barra de navegação, é possível verificar a tela de *ranking* geral dos usuários do sistema. Diferente dos *rankings* dos grupos que uma pessoa está, este representa todos os usuários cadastrados até o momento no sistema. Esta é uma maneira de adicionar mais um fator de competição ao usuário, onde ele poderá verificar sua posição geral diante de todos os outros participantes da aplicação. A Figura 17 exemplifica a interface do *ranking*.

Figura 17 – Tela de *Ranking*



Fonte: Elaboração própria

4.4.4.6 Criação e visualização de grupo

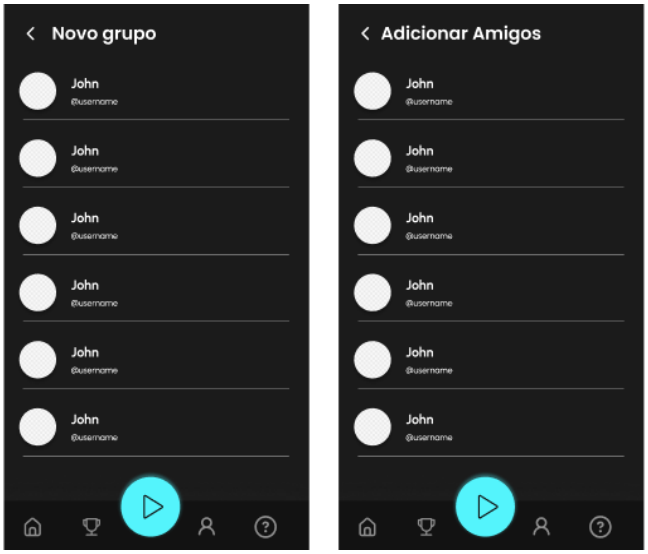
Como mencionado na Seção de Concepção da aplicação, os usuários que possuírem interesse em competir com pessoas específicas poderão adicionar outros participantes dentre uma lista com todos no sistema. Após adicionados, eles poderão criar grupos para poderem competir e comparar sua pontuação. A tela de adição de amigos e de criação de grupos (Figura 18) compartilham do mesmo *design*, mudando apenas o título da página e as etapas extras para o caso de criação do grupo.

Nessas etapas extras, um modal é apresentado ao criador do grupo, solicitando nome e descrição. Ao final da ação, uma tela avisando o usuário que o processo de geração do grupo foi bem sucedida é revelada.

Após criados, todos os grupos podem ser visualizados em formato de lista no perfil (a Figura 16, mencionada anteriormente, exemplifica este fato). Ao acessá-los, eles possuem uma interface semelhante ao ranking, porém com informações sobre o título do grupo e uma descrição.

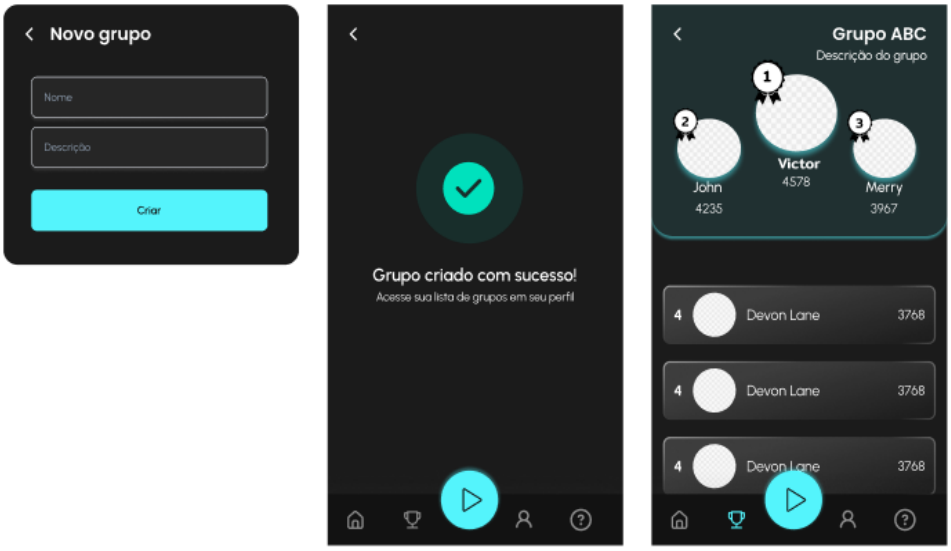
Essas interfaces, incluindo o processo de criação e visualização de grupos, podem ser verificadas na Figura 19.

Figura 18 – Tela de Adição de amigos e Criação de Grupos



Fonte: Elaboração própria

Figura 19 – Modal de criação do Grupo, Tela de resposta e do Grupo



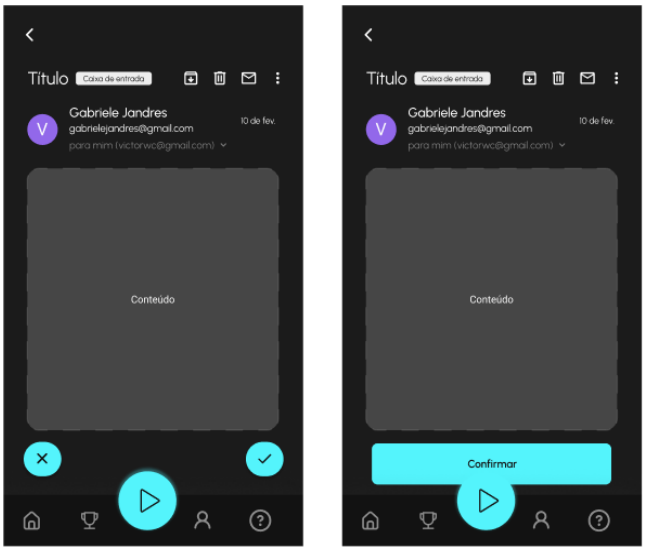
Fonte: Elaboração própria

4.4.4.7 Desafio

A última e mais importante funcionalidade deste sistema são os desafios. No meio da barra de navegação é possível visualizar um botão que faz referência à funcionalidade de *play* que está presente em aplicativos de jogos e reprodutores de vídeos. Este botão permite o usuário escolher entre os desafios de interesse. Apesar de disponibilizado três opções de desafio para escolher (*email*, mensagem de texto, e *website*), apenas o desafio de email foi implementado para o presente trabalho.

Ao clicar nesse botão, o participante da aplicação é redirecionado para uma tela que simula a de uma caixa de entrada de aplicativo de email. Todas as partes necessárias para identificar um email comum estão presentes: nome do remetente, email do remetente, o título do email e o corpo da mensagem, podendo ser uma imagem, um texto ou a junção dos dois. O usuário pode interagir com este conjunto de indicadores de um email, podendo selecioná-los ou não. A interação do jogo se baseia em analisar minuciosamente este email, selecionar aqueles indicadores que levaram a pessoa a acreditar se aquilo era um email de *phishing* ou não, e confirmar a resposta. Na Figura 20 é possível verificar os indicadores mencionados e os botões para resposta. Caso o usuário acredite que este email é um golpe, ele deve clicar no botão de "certo" (no lado direito da tela) e indicar (pressionando em cima dos indicadores de *phishing*), quais foram os fatores que levaram a responder e selecionar "Confirmar". Esse procedimento visa não só ajudar os usuários a reconhecer um email malicioso, mas também como identificar se o email é de fato malicioso. Caso ele acredite que é legítimo, basta escolher o ícone de "X" e "Confirmar".

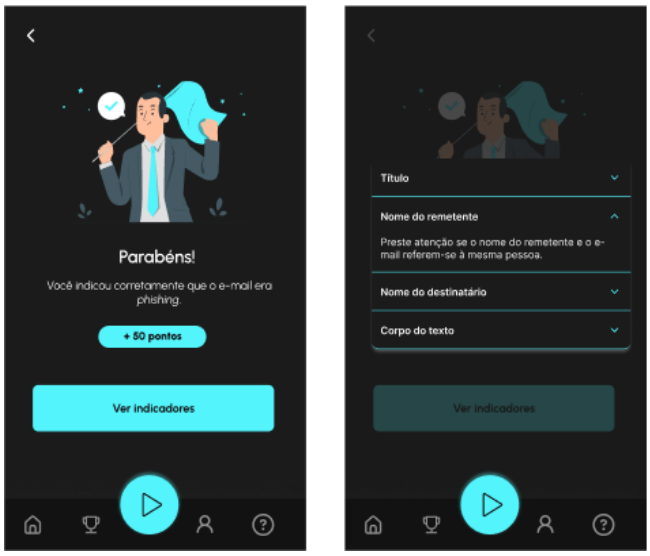
Figura 20 – Tela de Desafio



Fonte: Elaboração própria

Por fim, ao responder, o usuário recebe o *feedback* sobre seu palpite, informando se a resposta dele foi correta ou não e retornando algumas dicas para ajudar no seu aprendizado e prepar para outros desafios parecidos, assim como a informação sobre sua pontuação adquirida naquele desafio (Figura 21).

Figura 21 – Tela de *Feedback*



Fonte: Elaboração própria

5 EXPERIMENTAÇÃO E RESULTADOS

Neste capítulo, demonstraremos o método escolhido para verificar a eficácia do aplicativo servindo seu propósito, além de analisar as respostas dos usuários diante das perguntas feitas no formulário criado.

5.1 MÉTODO DE EXPERIMENTAÇÃO

A forma escolhida para avaliação da aplicação foi a utilização de um formulário online direcionado para pessoas de origens variadas, não se restringindo simplesmente à estudantes da UFRJ. Este formulário foi dividido em quatro seções.

A primeira seção verifica com o participante se ele já interagiu com a aplicação e concorda em participar da pesquisa. Na segunda seção, os participantes foram questionados sobre informações importantes para avaliar dados demográficos, como faixa etária, gênero, ocupação e área de ocupação. Esses serão levados em conta na análise dos resultados, a fim de averiguar se foram fatores que diferenciaram as respostas do formulário. Na terceira seção, foi perguntado aos usuários questões sobre conhecimentos prévios de *phishing*, como o entendimento da definição, se já foram alvos e se já usaram aplicativos similares para aprender sobre algum assunto. Por fim, na seção de "Experiência com o aplicativo SaPhish", as pessoas foram convidadas a responder sobre sua experiência com o aplicativo e seu impacto na educação e conhecimento do assunto.

Para teste do software, a aplicação foi difundida entre grupos do meio acadêmico e não-acadêmico. A aplicação foi hospedada em ambiente Docker, dividida em três *containers*: *Front-end* responsável pela hospedagem da interface, *Back-end* responsável pela hospedagem da API e banco de dados responsável pela hospedagem do banco PostgreSQL. Essa divisão tem a intenção de facilitar a administração e manutenção individual de cada componente do *software* ao acaso de eventuais correções de *bugs* e adição de novas funcionalidades. Para mais, foi utilizado o servidor *web* Nginx para redirecionar as requisições para os *containers* e adicionar a camada de segurança *Secure Socket Layer* (SSL) ao acessar o SaPhish. A máquina onde o aplicativo estava armazenado pertence ao Laboratório de Redes de Alta Velocidade (RAVEL) localizado na COPPE, e permaneceu ativa durante a execução dos testes.

O aplicativo gamificado contou com 6 tópicos sobre *phishing de email*, oferecendo dicas sobre como se defender desse tipo de ataque e familiarizar os indivíduos com o conceito de indicadores de um email de golpe. Foram adicionados 6 desafios na plataforma, sendo eles cinco de *phishing* com indicadores variados e apenas um email legítimo, criado de forma que os campos não se encaixem na descrição de um email de golpe.

5.2 MÉTRICAS UTILIZADAS

O objetivo deste presente trabalho é averiguar se o uso de elementos de gamificação para educação, conscientização e treinamento de *phishing* (como o *ranking*, os desafios e a pontuação) são diferenciais para o maior engajamento na interação com aplicativos desse gênero e se influenciaram de maneira positiva o aprendizado dos participantes.

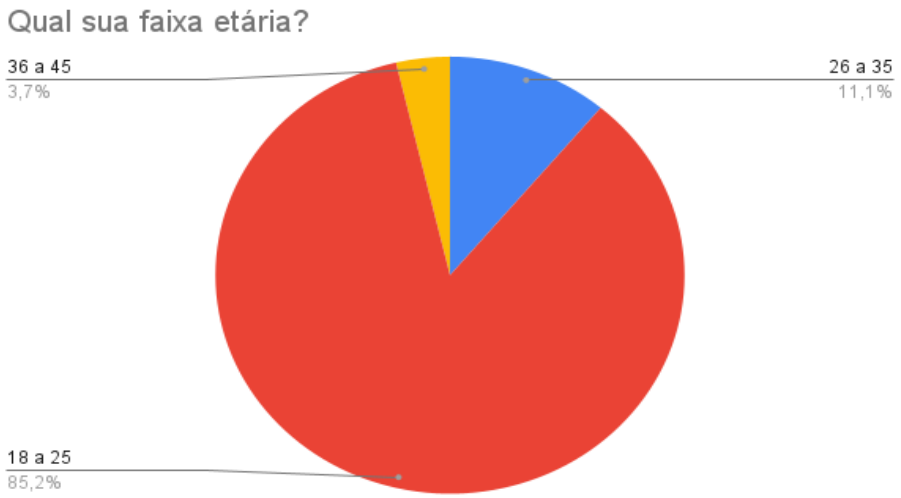
Para medir o potencial sucesso, o formulário criado explora alguns pontos considerados como fatores importantes para promover a utilização repetida da aplicação, como a facilidade no entendimento dos tópicos desenvolvidos e a pontuação final de cada usuário. Também foram feitas perguntas sobre a relação da funcionalidade de ranqueamento com a utilização da aplicação, a satisfação pela utilização de aplicativos de ensino gamificado para aprender a se proteger na Internet, se os participantes utilizariam o SaPhish no dia a dia e a plataforma que, na opinião do usuário, seria a mais benéfica para utilização desse tipo de aplicação.

5.3 DISCUSSÃO DOS RESULTADOS

5.3.1 Dados pessoais dos participantes

A pesquisa contou com a participação de 27 pessoas, as quais 85,2% delas possuem idade entre 18 a 25 anos, 11,1% pessoas entre 26 a 35, e apenas 3,7% entre 36 a 45 como mostra a Figura 22.

Figura 22 – Gráfico da faixa etária dos participantes

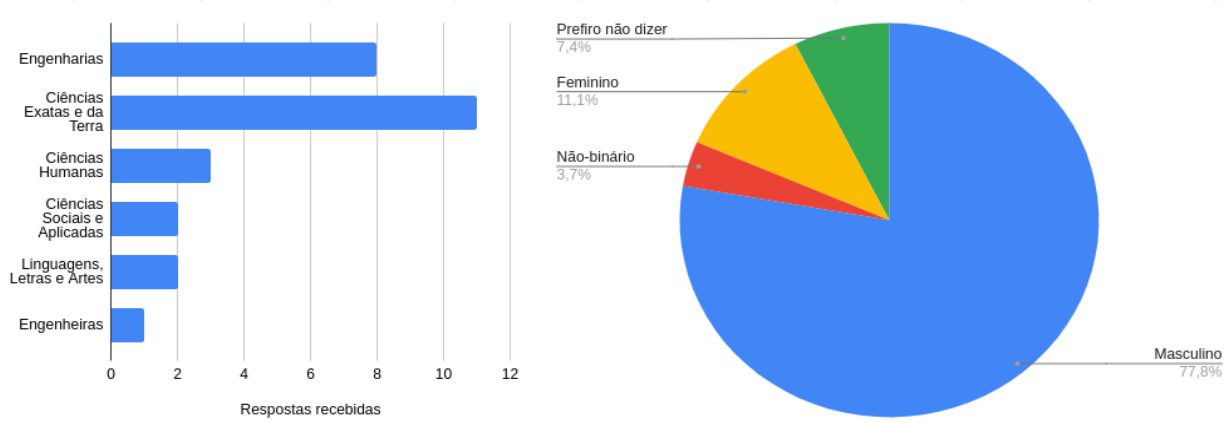


Fonte: Elaboração própria

Esses dados revelam uma limitação na variedade do público atingido, visto que a grande maioria de participantes se encontra na faixa etária de 18 a 25 anos e poucos

participantes declararam possuir mais do que 25 anos. Além disso, 77,8% dos participantes se declararam do gênero masculino, 11,1% se declararam do gênero feminino, 7,4% preferiram não dizer seu gênero e apenas 3,7% se consideram não-binário. Por conta da estratégia de difundir o formulário para ambientes acadêmicos e não-acadêmicos, foi possível obter o *feedback* de 11 pessoas que não se declararam estudantes, e uma grande diversidade de áreas de ocupação, com 12 pessoas pertencendo à área de Ciências Exatas e da Terra, 8 pessoas pertencendo a área de Engenharias, 2 de Linguísticas, Letras e Artes, 3 de Ciências Humanas e 2 de Ciências Sociais e aplicadas. A Figura 23 exemplifica ambos resultados comentados.

Figura 23 – Gráfico da ocupação e gênero dos participantes



Fonte: Elaboração própria

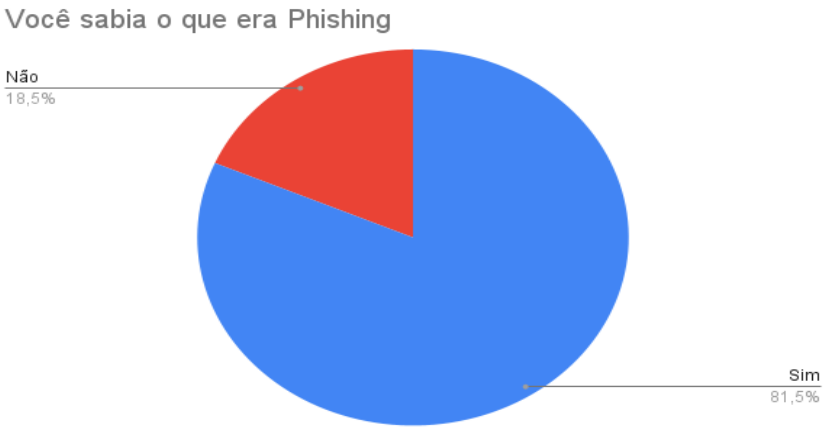
5.3.2 Conhecimento prévio sobre o tema

Ao analisar os resultados das perguntas feitas aos participantes sobre conhecimento a cerca o tema, percebeu-se que 81,5% dos envolvidos na pesquisa já possuíam conhecimento sobre o conceito de *phishing* antes de interagir com a aplicação (Figura 24) e, de todos os participantes, 77,8% deles foram alvos de *phishing*, sendo 59,3% de email e 55,6% de mensagem, como mostra a Figura 25. Essa expressiva quantidade de pessoas que já receberam alguma tentativa de ataque vinda de um cibercriminoso sugere a importância do desenvolvimento de soluções que visam ajudar os usuários vulneráveis a ataques de engenharia social. Além disso, apenas 5 pessoas das 27 totais não utilizaram nenhuma aplicação gamificada antes do SaPhish, indicando uma popularidade das aplicações de aprendizado com elementos de gamificação.

5.3.3 Experiência com a aplicação

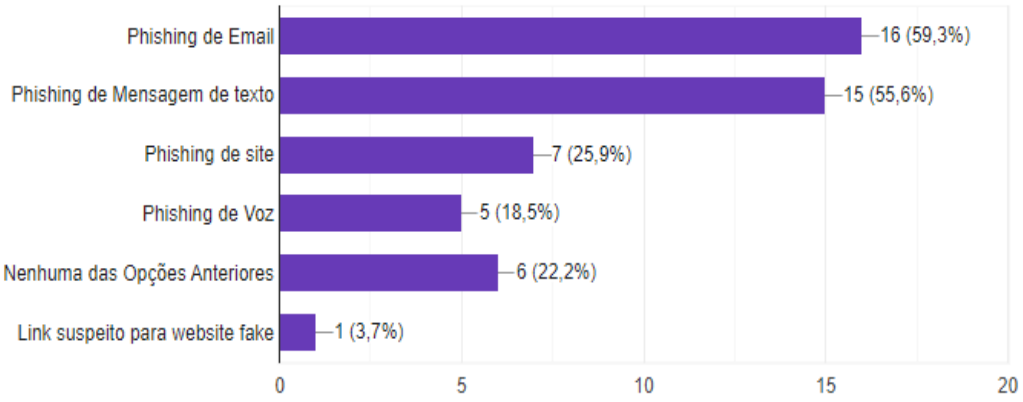
Na seção da experiência com o aplicativo SaPhish no formulário de participação, algumas informações importantes foram observadas. O total de 92,6% das respostas da

Figura 24 – Gráfico do conhecimento sobre Phishing



Fonte: Elaboração própria

Figura 25 – Tipos de Phishing recebido

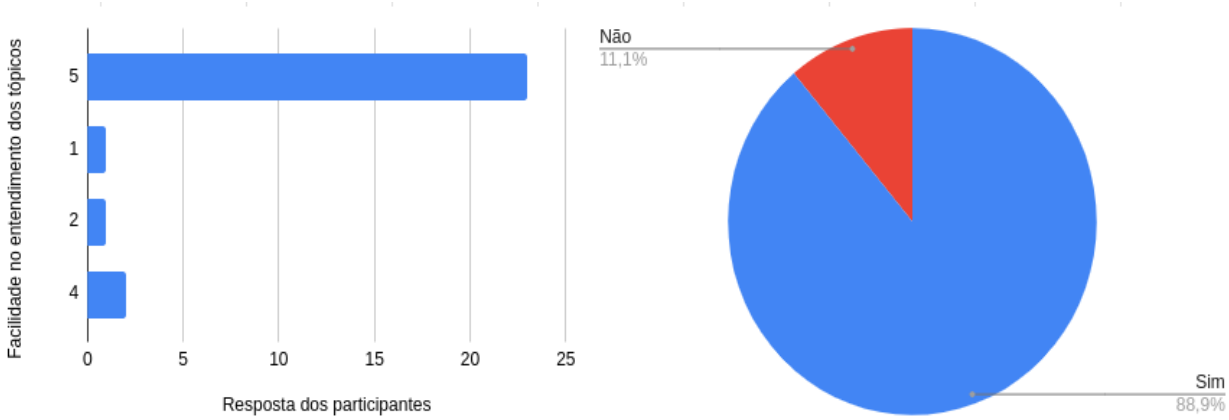


Fonte: Elaboração própria

pesquisa reveleram que o formato escolhido para falar sobre os tópicos informativos foi de fácil entendimento, onde 85,2% escolheram a opção máxima (em uma escala de um a cinco). Além disso, 100% dos participantes responderam que os tópicos ajudaram na realização dos desafios, indicando que a maneira como os tópicos foram formatados foi um fator positivo para o aprendizado dos usuários e resolução dos desafios.

Outra funcionalidade relevante na discussão dos resultados foram os desafios, os pontos e o *ranking*. De todos os participantes da pesquisa, aproximadamente 78% das pessoas que responderam adquiriram uma pontuação a cima de 1000. Além disso, a mediana de pontos adquirido pelas pessoas foi 1850 e a média encontrada foi de aproximadamente 5550 pontos. Porém, ao retirarmos alguns *outliers* que pontuaram a cima de 20000 pontos, temos a média de 2408. Essas respostas somadas ao resultado de 81,5% potencialmente indicam uma falta de refinamento na dificuldade dos desafios comparado ao conhecimento

Figura 26 – Facilidade no entendimento dos tópicos e engajamento pelo ranking



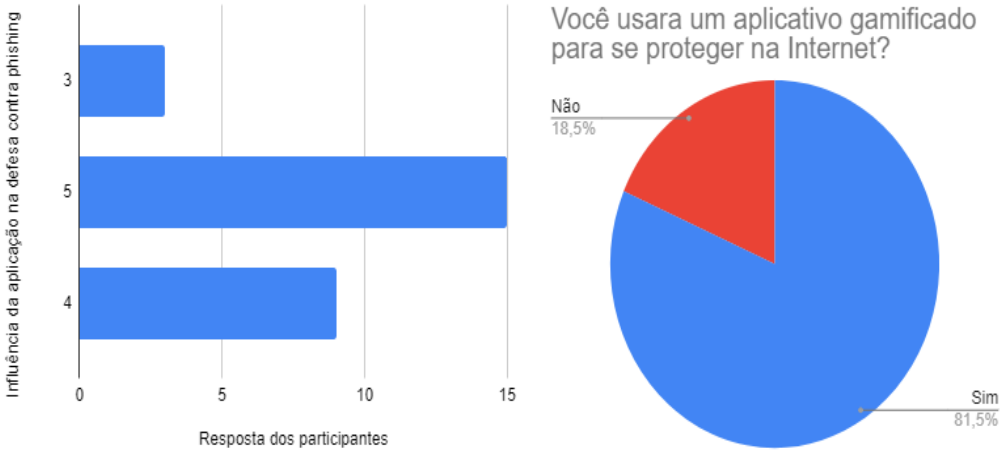
Fonte: Elaboração própria

dos participantes. Entretanto, como aproximadamente 89% das respostas indicaram que a existência do *ranking* geraram mais engajamento na aplicação, os resultados da pontuação podem indicar que o uso de elementos gamificados foi benéfico para a interação repetida do usuário com o *software*.

Algumas perguntas abordaram a experiência da interação do usuário com o sistema. Entre elas, se o aplicativo SaPhish ajudou os participantes a conhecer como se defender de *phishing* (em uma escalada de um a cinco). Das 27 respostas, 23 delas foram a cima de três, e 15 das 27 foram cinco. Além disso, não houve nenhuma resposta um e dois. Essas informações sugerem que o objetivo principal foi alcançado, isto é, conscientizar e educar os usuários sobre os perigos das técnicas de engenharia social, como o *phishing*. Ademais, 81,5% dos participantes expressaram o interesse em utilizar a proposta deste trabalho no seu dia a dia, porém, contrário as hipóteses que a utilização de aplicativo móveis é de interesse maior para aplicações gamificadas, 63% dos usuários não usariam apenas em dispositivos celulares, mas também nos computadores, em *sites* acessíveis via navegadores *web*, revelando um possível interesse do público pela diversificação de plataformas disponíveis para aprendizado. Essas informações podem ser visualizadas nas Figuiras 27 e 28.

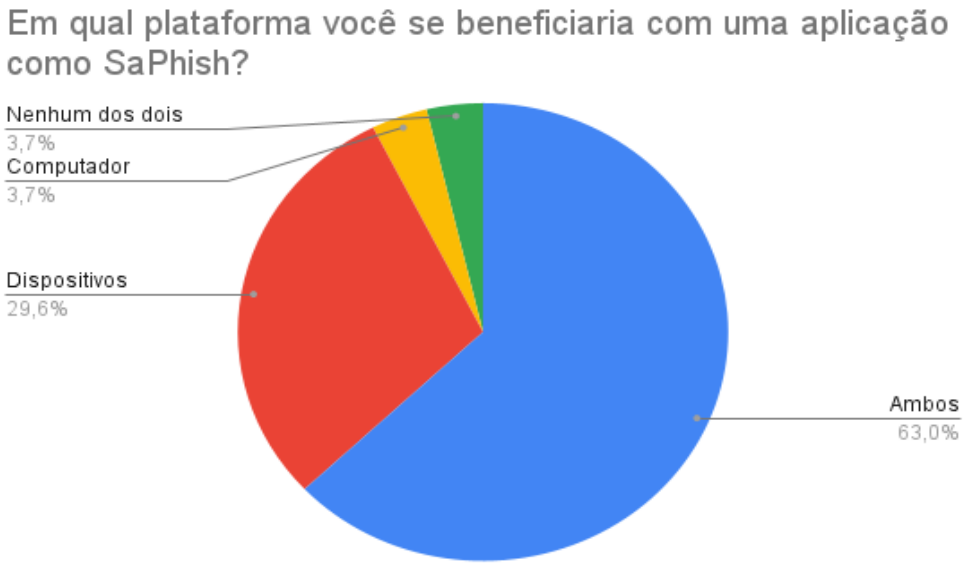
Por fim, foi perguntado aos participantes sobre dificuldades na navegação da interface e sugestões para melhorar a experiência do usuário. Entre as respostas, foram mencionados problemas de interação com a funcionalidade de desafio e trilhas. Segundo os relatos, os botões para interação com o desafio não ficaram claros ao relatar se um email é ou não legítimo. Já a funcionalidade de trilhas, criada para guiar a ordem de tópicos, não se mostrou intuitiva para alguns participantes, exigindo mais etapas para continuar a leitura de outros artigos e tópicos. Todos os *feedbacks* recebidos sobre a interface ajudarão a aperfeiçoar o SaPhish nas próximas edições.

Figura 27 – Utilização da aplicação no dia a dia



Fonte: Elaboração própria

Figura 28 – Utilização da aplicação no dia a dia



Fonte: Elaboração própria

6 CONCLUSÃO

6.1 REVISÃO

Este trabalho procurou abordar uma forma de contribuir para a defesa contra a ameaça da engenharia social, especialmente por meio de ataques de *phishing*, através de uma proposta que se concentrasse nos seres humanos ao invés de soluções automatizadas que utilizam aprendizado de máquina e inteligência artificial. Esse foco se deve pelo fato das pesquisas realizadas terem trazido dados importantes sobre o impacto de se promover iniciativas que contribuam para o aprendizado e conscientização dos usuários que são linha de defesa final dos sistemas.

Além disso, através do estudo feito nos artigos que discutem o estado da arte de soluções de treinamento sobre cibersegurança para pessoas, percebeu-se uma tendência na utilização de elementos de jogos para engajar o usuário e tornar a experiência de aprender como se defender na Internet mais proveitosa. Por conta disso, foi decidido a criação de um aplicativo que englobasse esses elementos e tentasse facilitar o aprendizado sobre *phishing* e como identificá-lo.

Essa proposta contribui com o meio acadêmico através de modelagens e diagramas necessários para que o sistema possa ser reproduzido e testado para verificar sua eficácia. A interface idealizada possui um foco em dispositivos de celulares e procura simular a experiência de um ataque real de engenharia social, através de desafios interativos propostos. Ademais, a aplicação oferece a possibilidade criar grupos com outros usuários, uma funcionalidade importante para uso em treinamentos empresariais, como forma de facilitar a administração da participação dos integrantes do grupo pelos instrutores.

6.2 RESUMO DOS RESULTADOS

Os resultados da pesquisa, que contou com a participação de 27 pessoas, geraram dados relevantes sobre a eficácia e receptividade do aplicativo gamificado SaPhish para a educação e conscientização sobre ataques de *phishing*. A diversidade de áreas de ocupação dos participantes mostrou que a aplicação atingiu tanto pessoas da área de Ciências Exatas e da Terra como de Engenharias, Linguísticas, Letras e Artes, Ciências Humanas e Ciências Sociais e Aplicadas.

A análise das respostas revelou que 81,5% dos participantes já tinham conhecimento prévio sobre *phishing*, mas ainda assim, 77,8% deles já foram alvos de ataques desse tipo, reforçando a necessidade de soluções educacionais como o SaPhish. O uso de elementos de gamificação, como desafios, pontuação e *ranking*, mostrou-se eficaz para engajar os usuários, com 89% dos participantes indicando que o *ranking* aumentou seu engajamento

com a aplicação. A facilidade de entendimento dos tópicos foi destacada por 92,6% dos participantes, e 100% afirmaram que os tópicos ajudaram na realização dos desafios.

Os resultados também sugerem que os desafios poderiam ser ajustados para melhor equilibrar a dificuldade com o conhecimento dos participantes, visto que muitos obtiveram pontuações altas. No entanto, a funcionalidade de gamificação demonstrou ser um fator positivo para a interação repetida com o aplicativo. Além disso, 81,5% dos participantes expressaram interesse em utilizar o SaPhish no dia a dia, e 63% indicaram preferência por versões acessíveis em computadores, além de dispositivos móveis.

6.2.1 Limitações da Pesquisa

Ao realizar as pesquisas por meio de um formulário difundido em grupos acadêmicos e não-acadêmicos, é importante reconhecer que funcionalidades propostas com foco em ambientes empresariais não foram abordadas na experimentação. Esse é o caso das funcionalidades de criação de grupos de usuários que, além de servir como outra funcionalidade de gamificação para engajamento dos usuários na aplicação, ela também é indicada para gerenciamento dos usuários de uma turma ou empresa que deseja fazer treinamento ou teste dos integrantes dos grupos.

Outra importante limitação identificada foi a não realização de avaliações antes e após utilização da aplicação, como forma de averiguar a eficácia do método proposto para aprender a se defender de *phishing*. Esses resultados podem trazer esclarecimentos relevantes sobre o formato de desafio escolhido para o treinamento dos usuários.

6.3 TRABALHOS FUTUROS

Para trabalhos futuros, sugere-se a adição de novas funcionalidades ao aplicativo, tais como a incorporação de mais desafios de *phishing*, não apenas focados em email, mas também explorando outros tipos mencionados nesta monografia. A expansão do escopo dos desafios permitirá uma análise mais abrangente das vulnerabilidades dos usuários diante de diferentes técnicas de ataque.

Além disso, com integração de elementos de inteligência artificial e de técnicas de aprendizado de máquina, seria possível gerar emails legítimos e fraudulentos personalizados conforme o comportamento dos usuários e suas vulnerabilidades identificadas. Isso não só aumentaria a efetividade dos desafios propostos, mas também proporcionaria um treinamento mais realista e adaptado às necessidades individuais dos usuários.

Por fim, propomos a utilização dos dados gerados pela interação dos usuários com o aplicativo para criar um conjunto de dados completo. Este conjunto poderia etiquetar e ranquear as amostras de *phishing* segundo a suscetibilidade dos usuários, identificando quais técnicas são mais eficazes. Essa análise permitiria uma compreensão mais profunda

das tendências e padrões de ataque, contribuindo para o desenvolvimento de estratégias de mitigação mais eficientes e personalizadas.

REFERÊNCIAS

ALABDAN, R. Phishing attacks survey: Types, vectors, and technical approaches. **Future internet**, MDPI, v. 12, n. 10, p. 168, 2020.

ALDAWOOD, H.; SKINNER, G. An advanced taxonomy for social engineering attacks. **International Journal of Computer Applications**, v. 177, n. 30, p. 1–11, 2020.

BASIT, A. et al. A comprehensive survey of ai-enabled phishing attacks detection techniques. **Telecommunication Systems**, Springer, v. 76, p. 139–154, 2021.

BASLYMAN, M.; CHIASSON, S. "smells phishy?": An educational game about online phishing scams. In: IEEE. **2016 APWG Symposium on Electronic Crime Research (eCrime)**. [S.l.], 2016. p. 1–11.

CHEN, Y.-H.; CHEN, J.-L. Ai@ ntiphish—machine learning mechanisms for cyber-phishing attack. **IEICE Transactions on Information and Systems**, The Institute of Electronics, Information and Communication Engineers, v. 102, n. 5, p. 878–887, 2019.

CJ, G. et al. Phishy-a serious game to train enterprise users on phishing awareness. In: **Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts**. [S.l.: s.n.], 2018. p. 169–181.

DAVIS, B. **Agile practices for waterfall projects: Shifting processes for competitive advantage**. [S.l.]: J. Ross Publishing, 2012.

FREEMAN, C. et al. The duolingo method for app-based teaching and learning. **Duolingo Research Report**, 2023.

JIA, F.; BAO, X.; YU, J. J. Gamification of digital platform: A meta-analysis. 2023.

KAPP, K. M. **The gamification of learning and instruction: game-based methods and strategies for training and education**. [S.l.]: John Wiley & Sons, 2012.

KIRYAKOVA, G.; ANGELOVA, N.; YORDANOVA, L. Gamification in education. In: **Proceedings of 9th international Balkan education and science conference**. [S.l.: s.n.], 2014. v. 1, p. 679–684.

LANE, S. H. et al. Making research delicious: An evaluation of nurses' knowledge, attitudes, and practice using the great american cookie experiment with mobile device gaming. **Journal for Nurses in Professional Development**, LWW, v. 32, n. 5, p. 256–261, 2016.

LE, D. et al. Effective cybersecurity training using microlearning and the drip concept: A case study of a large regional hospital. Drake Management Review, 2023.

NESTJS. 2024. Disponível em: https://nestjs.com/. Acesso em: 25 jul. 2024.

NIJLAND, J. **Gamification of cyber security awareness training for phishing against university students**. Dissertação (B.S. thesis) — University of Twente, 2022.

PEIXOTO, R. 2024. Disponível em: https://github.com/rf-peixoto/phishing_pot. Acesso em: 25 jul. 2024.

RANGERS, H. 2024. Disponível em: https://www.contraengenhariasocial.com/. Acesso em: 25 jul. 2024.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. **Future internet**, MDPI, v. 11, n. 4, p. 89, 2019.

SARKER, O. et al. A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness. **Journal of Systems and Software**, Elsevier, v. 208, p. 111899, 2024.

SCHÖBEL, S. et al. Adaptive and personalized gamification designs: Call for action and future research. **AIS Transactions on Human-Computer Interaction**, v. 13, n. 4, p. 479–494, 2021.

WANG, Z.; SUN, L.; ZHU, H. Defining social engineering in cybersecurity. **IEEE Access**, IEEE, v. 8, p. 85094–85115, 2020.

WEANQUOI, P.; JOHNSON, J.; ZHANG, J. Using a game to improve phishing awareness. **Journal of Cybersecurity Education, Research and Practice**, v. 2018, n. 2, p. 2, 2018.

WEN, Z. A. et al. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In: **Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems**. [S.l.: s.n.], 2019. p. 1–12.

WIJAYA, W. et al. Gamified tailored roleplay story-based phishing awareness training. **International Journal of Data Science and Advanced Analytics**, v. 4, p. 146–153, 2022.

X-FORCE, I. S. **X-Force Threat Intelligence Index**. 2023. Disponível em: https://mysecuritymarketplace.com/reports/x-force-threat-intelligence-index-2023/. Acesso em: 25 jul. 2024.

YEBOAH-BOATENG, E. O.; AMANOR, P. M. Phishing, smishing & vishing: an assessment of threats against mobile devices. **Journal of Emerging Trends in Computing and Information Sciences**, Asian Research Publishing Network (ARPN), v. 5, n. 4, p. 297–307, 2014.

APÊNDICE A – FORMULÁRIO DE AVALIAÇÃO DO SAPHISH

A.1 DADOS PESSOAIS

1. Você confirma que já interagiu com a aplicação e concorda em participar da pesquisa?

    a) Sim

    b) Não

2. Qual a sua faixa etária?

    a) 18 a 25 anos

    b) 26 a 35 anos

    c) 36 a 45 anos

    d) 46 a 55 anos

    e) 56 a 65 anos

    f) Mais de 65 anos

3. Qual o seu gênero?

    a) Feminino

    b) Masculino

    c) Não-binário

    d) Outro

    e) Prefiro não responder

4. Qual sua ocupação atual?

    a) Estudante

    b) Trabalhando

    c) Prefiro não dizer

5. Qual a área da sua ocupação?

    a) Ciências Exatas e da Terra

    b) Ciências Biológicas

    c) Engenharias

d) Ciências da Saúde

e) Ciências Agrárias

f) Linguística, Letras e Artes

g) Ciências Sociais e Aplicadas

h) Ciências Humanas

A.2 CONHECIMENTO SOBRE PHISHING

6. Você sabia o que era Phishing antes de jogar?

   a) Sim

   b) Não

7. Você já foi alvo de algum desses golpes de Phishing?

   a) Phishing de Email

   b) Phishing de Mensagem de texto

   c) Phishing de site

   d) Phishing de Voz

   e) Nenhuma das Opções Anteriores

8. Você já usou algum aplicativo de aprendizado que possui elementos de jogo antes do SaPhish (Pontos, desafios, ranqueamento, etc)? Ex: Duolingo, Kahoot, etc. Se sim, quais?

A.3 EXPERIÊNCIA COM O APLICATIVO SAPHISH

9. Você teve alguma dificuldade em navegar pela interface? Qual? Poderia explicar?

10. De 1 a 5, quanto foi sua facilidade em entender os tópicos sobre Phishing?

11. Você achou que os tópicos te ajudaram a resolver os desafios?

    a) Sim

    b) Não

12. Vá até o perfil e procure seus pontos. Qual foi sua pontuação final?

13. Você acredita que a presença de um Ranking (geral ou de grupo) gerou mais engajamento para utilizar a aplicação?

a) Sim

b) Não

14. Quantos desafios você fez antes de preencher esse formulário?

a) Sim, tenho interesse

b) Não, mas jogaria se fosse obrigatório

c) Não, não tenho interesse no jogo

15. Você conseguiu adquirir a pontuação máxima em algum desafio (250)?

a) Sim

b) Não

De 1 a 5, o quanto você acha que o SaPhish te ajudou a conhecer como se defender de phishing?

Você usaria um aplicativo de ensino gamificado (utilizando elementos de jogos como o Duolingo) para aprender como se proteger na Internet?

a) Sim

b) Não

No seu dia a dia, você se beneficiaria desse tipo de aplicação em dispositivios celular ou em computadores (acessar direto no navegador)?

a) Dispositivos Celulares

b) Computador

c) Ambos

d) Nenhum dos dois