Phishing Quiz: Um Jogo Educacional para Conscientização e Prevenção de Ataques Cibernéticos

Lucas Coqui[1], **Vitor Maia**[2], **Diego Castro**[1]

[1]Centro Federal de Educação TecnológicaCelso Suckow da Fonseca (CEFET/RJ),Rio de Janeiro, Brasil

[2]Pesquisador Independente

lucascoqui14@gmail.com, vcm@ufrj.br , diegocbcastro07@gmail.com

Resumo. Introdução: *Os ataques de phishing continuam sendo uma das principais ameaças à segurança digital, explorando a falta de conhecimento dos usuários para capturar informações sensíveis. Neste cenário, estratégias educativas inovadoras, como o uso de jogos digitais, têm se mostrado eficazes para promover a conscientização e a aprendizagem ativa.* ***Objetivo:*** *Este projeto apresenta o desenvolvimento do jogo educativo Phishing Quiz, um jogo em formato de quiz que visa ensinar boas práticas de segurança cibernética por meio da análise de e-mails suspeitos e perguntas com feedback explicativo.* ***Etapas:*** *O jogo foi desenvolvido com foco em promover uma experiência interativa e educativa, incorporando elementos como feedback imediato, identificação de sinais de fraude e estrutura de perguntas contextualizadas com situações reais.* ***Resultados Esperados:*** *Espera-se que o jogo contribua para o aumento da conscientização sobre segurança digital e melhore a habilidade dos usuários em reconhecer tentativas de phishing. Como trabalhos futuros, estão previstos testes práticos com usuários, aplicação de questionários para avaliação da experiência, além da adição de novas mecânicas, como sistema de pontuação e controle de tempo.*

Palavras-Chave *Phishing, Segurança digital, Game-based Learning, Jogos educativos, Conscientização Cibernética.*

Abstract. Introduction: *Phishing attacks remain one of the main threats to digital security, exploiting users' lack of knowledge to steal sensitive information. In this context, innovative educational strategies such as the use of digital games have proven effective in promoting awareness and active learning.* ***Objective:*** *This project presents the development of the educational game Phishing Quiz, a quiz-style game designed to teach good cybersecurity practices through the analysis of suspicious emails and questions with explanatory feedback.* ***Stages:*** *The game was developed with a focus on delivering an interactive and educational experience, incorporating elements such as immediate feedback, identification of fraud indicators, and question structures based on real-world situations.* ***Expected Results:*** *The game is expected to increase digital security awareness and improve users' ability to recognize phishing attempts. Future work includes practical testing with users, application of evaluation questionnaires, and the addition of new mechanics such as a scoring system and time control.*

Keywords *Phishing, Digital Security, Game-based Learning, Educational Games, Cybersecurity Awareness*

1. Introdução

Nas últimas décadas, o ciberespaço tornou-se fundamental para as relações sociais, econômicas e governamentais, ao facilitar o acesso à informação e ampliar a comunicação digital. No entanto, esse avanço trouxe desafios relevantes, sobretudo em relação à segurança da informação. O aumento dos crimes cibernéticos evidencia a vulnerabilidade de usuários e instituições diante de ameaças cada vez mais sofisticadas. Em 2017, o Brasil figurou como o segundo país mais atacado do mundo, com mais de 70 milhões de vítimas [Alves, 2022], o que reforça a urgência de medidas educativas e preventivas.

Entre os ataques virtuais, o Phishing se destaca por empregar técnicas de engenharia social para capturar dados sensíveis[Aleroud and Zhou, 2017]. Estratégias como baiting e pretexting são utilizadas[Montagner and Westphall, 2022], envolvendo fraudes por e-mails, mensagens, ligações telefônicas e sites falsos. Esses conteúdos também circulam em redes sociais, aplicativos, anúncios e outras plataformas, o que dificulta a identificação por usuários despreparados.

A baixa percepção de risco e a falta de conhecimento tornam os usuários alvos fáceis. Nesse contexto, estratégias educativas ganham destaque, e os jogos digitais surgem como ferramentas eficazes de ensino-aprendizagem. Abordagens como jogos sérios e *Game-Based Learning* mostram-se promissoras para o treinamento em temas como segurança da informação [Pho and Dinscore, 2015].

Este trabalho apresenta o desenvolvimento do **Phishing Quiz**, um jogo educativo voltado para o ensino da identificação de sinais de Phishing, sem exigir conhecimentos prévios em cibersegurança. Estruturado em formato de quiz, o jogo utiliza casos reais para proporcionar uma experiência interativa. A dinâmica de perguntas e desafios favorece o aprendizado por repetição, estimula a curiosidade e incentiva uma competição saudável, contribuindo para o fortalecimento do conhecimento de maneira lúdica [Vargas, 2018].

2. Fundamentação teórica

2.1. Ataques Cibernéticos

A digitalização de processos trouxe eficiência, mas também originou crimes cibernéticos. Em 1971, Bob Thomas criou o primeiro malware, *The Creeper*, marcando o início das preocupações com segurança digital [ARAÚJO and Rossi, 2020]. Com o tempo, as ameaças evoluíram, como o Phishing, surgido em 1995 e baseado em engenharia social [Roza and Pegoraro, 2020]. Táticas como *baiting*, com iscas em anúncios falsos [Alves, 2024], e *pretexting*, que utiliza dados públicos da vítima para criar armadilhas [Montagner and Westphall, 2022], tornaram-se comuns.

2.2. Jogos Sérios na Educação

Os jogos digitais, antes voltados ao entretenimento, passaram a ter versões educativas aplicadas ao ensino, política e saúde, promovendo desenvolvimento cognitivo e motor [Silva et al., 2017]. Na educação, facilitam o aprendizado de temas complexos, como no jogo "EVOLUÇÃO: A LUTA PELA SOBREVIVÊNCIA", voltado ao ensino da evolução dos vertebrados a partir dos 12 anos[Campos et al., 2003]. Assim, consolidam-se como ferramentas pedagógicas engajadoras e eficazes.

2.3. Jogos em Contextos Militares e de Saúde

Jogos também são utilizados em contextos militares e terapêuticos. O Exército dos EUA emprega simulações e adaptações de jogos como o *Rainbow Six Rogue Spear* para o treinamento de soldados [Macedonia, 2002]. Na área da saúde, os *Exergames* combinam atividades físicas com mecânicas de jogo, como o *Nintendo Wii Sports* (2006), promovendo o bem-estar de maneira lúdica[Vaghetti and da Costa Botelho, 2010].

2.4. Game Based Learning (GBL)

O *Game-Based Learnin*g (GBL) incorpora jogos ao processo pedagógico para potencializar a aprendizagem por meio da interação. Segundo [Steiner et al., 2009], o GBL direciona o tempo dedicado aos jogos para objetivos educacionais. Diferentemente dos jogos recreativos, aqueles voltados ao GBL são estruturados para promover conhecimento em ambientes lúdicos [Pho and Dinscore, 2015]. Elementos como competição, recompensas e progressão favorecem o engajamento e a eficácia do ensino.

2.5. Modelo LM-GM(Learning Mechanics-Game Mechanics)

O LM-GM é um modelo para analisar e desenvolver jogos sérios, correlacionando mecânicas pedagógicas e de jogabilidade e mostrando como interagem no ensino com entretenimento. Suas listas flexíveis permitem adaptações, úteis no design e avaliação. Em jogos de prevenção de Phishing, o LM-GM mapeia como essas mecânicas engajam e instruem o usuário no reconhecimento de ataques, integrando aspectos educativos e lúdicos [Sabino and Cardoso, 2019, Venson et al., 2018, Venson et al., 2022].

3. Trabalhos relacionados

Esta seção apresenta estudos sobre segurança digital e jogos educativos. Embora o tema seja relevante, não foram encontrados jogos com proposta idêntica à do projeto aqui descrito.[Bispo, 2024] apresenta um jogo interativo em Pygame para ensinar segurança digital de forma prática, promovendo maior autonomia dos usuários. Outro exemplo é o *Anti-Phishing Phil*, de[Sheng et al., 2007], que ensina a reconhecer URLs maliciosas e usar mecanismos de busca para verificar sites suspeitos.

[Jin et al., 2018] exploraram o ensino de segurança cibernética para estudantes do ensino médio com jogos como o *Secure Online Behavior Game*, que ensina a identificar e-mails de phishing, reconhecer links e ligações fraudulentas e proteger dados pessoais. Também foi apresentado um jogo do tipo *tower defense*, onde o jogador protege um servidor virtual contra ataques cibernéticos, com níveis de dificuldade progressiva. O objetivo era despertar o interesse dos jovens e ampliar a conscientização. Por fim, [Ferreira et al., 2024] realizaram uma revisão sistemática sobre jogos sérios anti-phishing como ferramentas educacionais. O estudo reforça a abordagem adotada neste projeto, defendendo o uso de jogos como estratégia eficaz de mitigação de ataques.

O *Phishing Quiz* destaca-se pela abordagem prática e interativa, utilizando e-mails simulados de ataques reais e quizzes com feedback detalhado. Oferece uma experiência de aprendizado acessível e envolvente, estimulando a análise crítica e identificação de fraudes, mesmo para usuários sem conhecimentos prévios em segurança digital. Sua relevância se evidencia no contexto atual de alta conectividade e vulnerabilidade digital, ao oferecer uma ferramenta educativa eficaz para ampliar a conscientização e promover boas práticas de segurança online[Salviano et al., 2022].

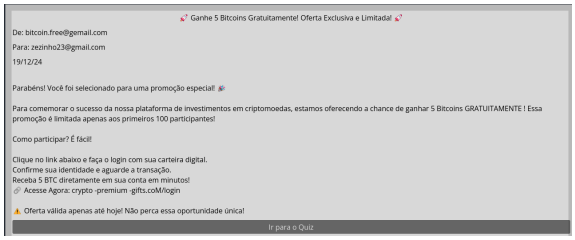

Figura 1. Tela de E-mail: Fase 1

4. Proposta do Jogo

Este projeto foi motivado pelo aumento dos ataques de Phishing, conforme destacado por [Salviano et al., 2022], e pela necessidade de educar os usuários sobre segurança digital de maneira acessível. Optou-se por um jogo no formato de quiz, considerando sua capacidade de engajar e estimular o aprendizado ativo.

A metodologia definiu competências e objetivos mensuráveis, usando o LM-GM para alinhar mecânicas de aprendizagem e jogo. Competências como identificar e prevenir Phishing basearam-se em referenciais de segurança e orientaram os desafios. A avaliação ocorre na gameplay, por indicadores como acertos, tempo de resposta e feedback contínuo, permitindo acompanhar progresso e eficácia[Arnab et al., 2015].

4.1. Desenvolvimento

O jogo foi desenvolvido na Godot Engine, uma plataforma gratuita e de código aberto. A escolha levou em conta fatores como a ausência de taxas e a liberdade de personalização, em comparação com outras ferramentas, como a Unity. Inicialmente, o projeto foi direcionado para computadores escolares, havendo planos futuros de adaptação para dispositivos móveis, a fim de ampliar seu alcance.

4.2. Visão Geral e Público-Alvo

O Phishing Quiz ensina os jogadores a identificar ataques de Phishing por e-mail, abordando práticas de segurança como a detecção de links suspeitos, análise crítica de mensagens e cautela diante de solicitações de dados. A dinâmica consiste em e-mails simulados, seguidos de perguntas explicativas com feedback detalhado, permitindo que o aprendizado ocorra a partir dos próprios erros. O jogo é direcionado a qualquer pessoa interessada em cibersegurança, incluindo usuários experientes, devido à sofisticação das ameaças atuais. Sua proposta é fortalecer a percepção de risco e promover boas práticas de forma acessível e didática.

4.3. Mecânicas do Jogo

O *Phishing Quiz* compõe 10 fases com dificuldade progressiva, nas quais o jogador interage com e-mails que simulam tentativas reais ou fictícias de *Phishing*. Cada fase apresenta um e-mail que pode ou não conter indícios de fraude, como erros gramaticais, senso de urgência, links suspeitos, solicitações de dados pessoais, entre outros sinais típicos ataques. Após analisar o conteúdo do e-mail, o jogador é redirecionado para uma tela de perguntas e respostas, onde deve avaliar a veracidade da mensagem. Independentemente da resposta escolhida, o jogo fornece um feedback detalhado, explicando os motivos da correção e reforçando os conceitos de segurança digital.

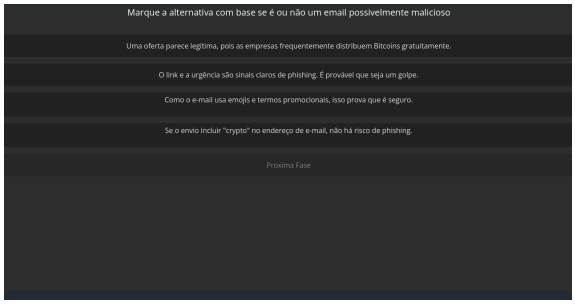

Figura 2. Tela do Quiz: Fase 1

As fases começam com situações simples, como falsas ofertas, e avançam para ataques sofisticados baseados em casos reais. O fluxo inclui introdução, análise do e-mail, quiz com perguntas como *"Há indício de phishing nesta proposta de emprego?"* (se o domínio não for oficial, é golpe) ou *"Este e-mail de reembolso é verídico?"* (sem solicitar dados bancários, é confiável), seguido de feedback detalhado e avanço de fase. Elementos de gamificação e feedback constante reforçam o aprendizado, promovem retenção, engajamento e tornam a experiência realista.

5. Trabalhos futuros

Futuras etapas incluirão a realização de testes práticos com usuários em laboratórios. Após a experiência de jogo, será aplicado um questionário para avaliar a usabilidade e coletar sugestões . Também está prevista a implementação de novas mecânicas, como controle de tempo para leitura e resposta, além de um sistema de pontuação.

6. Conclusão

Este trabalho apresentou o **Phishing Quiz**, um jogo educativo voltado ao ensino de práticas de segurança digital, com foco na identificação e prevenção de ataques de Phishing. A proposta surgiu diante do aumento desses ataques e da necessidade de estratégias educativas acessíveis para conscientizar usuários, inclusive os sem conhecimento técnico. Utilizando a abordagem *Game-Based Learning*, o jogo combina elementos de gamificação, como feedback imediato e desafios baseados em situações reais, promovendo um aprendizado lúdico e engajador.

Além de revisar trabalhos correlatos, destacou-se o diferencial da proposta: quizzes contextualizados com exemplos reais de ataques e explicações detalhadas para cada resposta, promovendo aprendizagem crítica. Futuramente, prevê-se testar a ferramenta com usuários, aplicar questionários para avaliação e implementar funções como pontuação e controle de tempo. Espera-se, assim, aprimorar a ferramenta e validar seu potencial como recurso de apoio no ensino de segurança cibernética.

Dessa forma, o *Phishing Quiz* contribui para o fortalecimento da cultura de segurança digital e demonstra o potencial dos jogos educativos como ferramentas eficazes de conscientização e formação no contexto atual.

Referências

Aleroud, A. and Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68:160–196.

Alves, D. (2022). Ataques cibernéticos ao brasil: levantamento sistemático dos últimos dez anos (2010–2020). *Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal do Rio Grande do Sul, Porto Alegre*.

Alves, L. d. M. (2024). Engenharia social: estudo de ataques e métodos de prevenção. *Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Pontifícia Universidade Católica de Goiás, Goiânia*.

ARAÚJO, F. C. d. and Rossi, J. M. (2020). A evolução dos ataques cibernéticos. *Trabalho de Conclusão de Curso (Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", Americana*.

Arnab, S., Lim, T., Carvalho, M. B., Bellotti, F., de Freitas, S., Louchart, S., Suttie, N., Berta, R., and De Gloria, A. (2015). Mapping learning and game mechanics for serious games analysis. *British Journal of Educational Technology*, 46(2):391–411.

Bispo, B. R. d. M. S. (2024). Ferramenta de educação em segurança digital: Um jogo interativo com pygame. *Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação) – Pontifícia Universidade Católica de Goiás, Goiânia*.

Campos, L. M. L., BORTOLOTO, T. M., FELÍCIO, A. K. C., et al. (2003). A produção de jogos didáticos para o ensino de ciências e biologia: uma proposta para favorecer a aprendizagem. *Caderno dos núcleos de Ensino*, 47(1):47–60.

Ferreira, A. L. H., de Sales, A. B., Ferreira, A. E., and Palmeira, E. G. (2024). Características dos jogos sérios anti-phishing como ferramenta de ensino: uma revisão sistemática. *Revista Novas Tecnologias na Educação*, 22(1):340–350.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., and White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, 12(1):150–158.

Macedonia, M. (2002). Games, simulation, and the military education dilemma. In *Internet and the University: 2001 Forum*, pages 157–167. Educause Cambridge: MA.

Montagner, A. S. and Westphall, C. M. (2022). Uma breve análise sobre phishing. *Revista ComInG-Communications and Innovations Gazette*, 6(1):46–56.

Pho, A. and Dinscore, A. (2015). Game-based learning. *tips and trends instructional technologies committee; american library association*, 2.

Roza, B. E. and Pegoraro, M. A. G. (2020). Classificador de phishing utilizando algoritmo de naive bayes. *Trabalho de Conclusão de Curso (Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", Americana*.

Sabino, E. and Cardoso, J. R. (2019). Revisão sistemática ambiente web gamificado para cursos de engenharia e tecnólogos. *PontodeAcesso*, 13(3):85–95.

Salviano, E. M., Santos, J. P. R., and Silva, M. A. (2022). Principais tipos de ataques phishing e mecanismos de segurança. *Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Centro Universitário do Planalto Central Apparecido dos Santos, Brasília*.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people

not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99.

Silva, L. F., Costa, D., and Inocêncio, A. C. (2017). Hajed-tdah: Heurísticas para avaliação de jogos educacionais digitais para pessoas com tdah. In *Anais do Workshop de Informática na Escola*, volume 23, pages 915–924.

Steiner, C. M., Kickmeier-Rust, M. D., and Albert, D. (2009). Little big difference: Gender aspects and gender-based adaptation in educational games. In *Learning by Playing. Game-based Education System Design and Development: 4th International Conference on E-Learning and Games, Edutainment 2009, Banff, Canada, August 9-11, 2009. Proceedings 4*, pages 150–161. Springer.

Vaghetti, C. A. O. and da Costa Botelho, S. S. (2010). Ambientes virtuais de aprendizagem na educação física: uma revisão sobre a utilização de exergames. *Ciências & Cognição*, 15(1):64–75.

Vargas, D. d. (2018). O processo de aprendizagem e avaliação através de quiz. *Trabalho de Conclusão de Curso (Licenciatura em Pedagogia) – Centro Universitário Univates, Lajeado*.

Venson, R., Callaghan, M., and Marcelino, R. (2022). Phototype: um jogo sério para fixação de conhecimento em sistemas fotovoltaicos. *ETD Educação Temática Digital*, 24(2):275–295.

Venson, R. et al. (2018). Utilização de jogos sérios no apoio da fixação de conhecimentos em sistemas fotovoltaicos. *Programa de Pós-Graduação em Tecnologias da Informação e Comunicação*.