Características dos Jogos Sérios Anti-Phishing Como Ferramenta de Ensino: Uma Revisão Sistemática

Ana Luiza Hoffmann Ferreira, UnB, ana.luiza.hoff@gmail.com,
https://orcid.org/0009-0007-0474-0806
André Barros de Sales, UnB, andrebdes@unb.br,
https://orcid.org/0000-0002-1728-6063
Alexander E. V. Ferreira, UnB, alexander.ferreira@iadc.edu,
https://orcid.org/0000-0001-7057-936X
Eduardo G. Q. Palmeira, UnB, eduardo.palmeira@unb.br,
https://orcid.org/0000-0002-7189-8917

Resumo: Este trabalho apresenta uma revisão sistemática de literatura em busca de compreender a percepção dos jogadores sobre as características dos jogos sérios anti-phishing como ferramenta de ensino. Foram selecionados 14 estudos para análise, permitindo identificar as estratégias de design e implementação dos treinamentos por meio de jogos sérios, os métodos de avaliação empregados, e as percepções dos usuários sobre os jogos utilizados. A análise revelou a necessidade de uma melhor integração de teorias de aprendizagem, padronização na categorização das características dos jogos, abordagem mais rigorosa na coleta de feedback dos usuários, e revisão das plataformas de recrutamento de participantes dos estudos.

Palavras-chave: phishing, jogos sérios, percepção dos jogadores, cibersegurança.

Characteristics of Anti-Phishing Serious Games as a Teaching Tool: A Systematic Review

Abstract: This work presents a systematic literature review aimed at understanding players' perceptions of the features of anti-phishing serious games as an educational tool. Fourteen studies were selected for analysis, enabling the identification of design and implementation strategies of serious game-based training, the evaluation methods employed, and users' perceptions of the games used. The analysis revealed the need for better integration of learning theories, standardization in categorizing game features, improved user feedback collection, and a review of the participant recruitment platforms used in the studies.

Keywords: phishing, serious games, players' perception, cybersecurity.

1. Introdução

O aumento exponencial de ataques cibernéticos nos últimos anos, especialmente no contexto do *phishing*, tem gerado urgência para o desenvolvimento e implementação de métodos eficazes de proteção dos usuários da internet. Relatórios recentes da Anti-Phishing Working Group (APWG) corroboram essa tendência, evidenciando um aumento significativo de 22,46% nos ataques de *phishing* no primeiro semestre de 2023 em comparação com o mesmo período do ano anterior (Anti-Phishing Working Group, 2023a).

A observação de um recorde no número de ataques entre janeiro e março de 2023 pela APWG reforça a gravidade da situação. Os ataques de *voice-mail phishing* (*vishing*) continuam a crescer, tendo o setor financeiro como principal alvo, seguido pelas mídias sociais e serviços de e-mail. Embora a quantidade de ataques detectados tenha diminuído entre abril e junho de 2023, a ameaça persiste e representa uma preocupação para a segurança dos dados pessoais e financeiros dos usuários, bem como para a integridade das organizações em todo o mundo (Anti-Phishing Working Group, 2023b).

Diante desse cenário, uma abordagem promissora para mitigar os riscos associados ao *phishing* é o uso de jogos sérios *anti-phishing*. Estes jogos têm o propósito de educar os usuários sobre as táticas empregadas pelos criminosos cibernéticos, proporcionando uma experiência interativa e imersiva que combina entretenimento com objetivos educacionais (Battistella e Wangenheim, 2016). No entanto, verifica-se uma falta de sínteses sobre a percepção dos usuários em relação às características desses jogos na literatura.

Este artigo visa corroborar com o preenchimento dessa lacuna por meio de uma Revisão Sistemática de Literatura (RSL), que analisa as características dos jogos sérios *anti-phishing* como ferramentas de educação e conscientização cibernética. A análise se baseia em evidências empíricas recentes e explora estratégias de design e implementação que podem otimizar a eficácia desses jogos na prevenção de ataques de *phishing*.

2. Metodologia

Taxonomias abrangentes são utilizadas para classificar estudos científicos, incluindo aspectos como a natureza da abordagem, o propósito, os objetivos e a natureza da pesquisa. Seguindo essa estrutura conceitual, o presente estudo se enquadra na categoria de pesquisa qualitativa, de natureza descritiva e exploratória, com objetivos voltados para a análise do cenário atual do uso de jogos sérios na educação *anti-phishing*, buscando identificar e elucidar questões emergentes e formulando hipóteses correspondentes. Por fim, a natureza básica desta pesquisa visa contribuir para o avanço do conhecimento científico, sem uma aplicação prática imediata prevista (Gerhardt e Silveira, 2009).

A metodologia empregada foi a RSL. Essa abordagem segue planejamento e execução rigorosos, com o objetivo de mapear o estado da arte de maneira abrangente, permitindo a elaboração de um estudo secundário robusto e com um mínimo de viés informacional. Foram seguidas as diretrizes de planejamento propostas por Kitchenham (2004).

2.1 Planejamento

O planejamento da RSL tem início com a definição clara de um objetivo específico. Neste estudo, o objetivo foi estabelecido como sendo a identificação da percepção do usuário sobre as características mais comuns nos jogos sérios *anti-phishing*. A elaboração do protocolo se inicia com a formulação de perguntas de pesquisa precisas. Nesse sentido, foram desenvolvidas três questões de pesquisa (QP), delineadas da seguinte forma:

QP1: Qual é o público alvo dos estudos sobre os jogos sérios *anti-phishing*?

QP2: Quais são as características mais encontradas em jogos sérios *anti-phishing*?

QP3: Qual é a percepção dos usuários sobre as características dos jogos sérios *anti-phishing*?

A população alvo é composta pelos usuários de jogos sérios *anti-phishing*, enquanto a intervenção considerada são os próprios jogos sérios *anti-phishing*. A comparação proposta se concentra na análise das diferenças entre diversos jogos sérios, com o objetivo de identificar características que possam comprometer sua eficácia. Como desfecho, busca-se aprimorar a eficácia desses jogos por meio da análise realizada neste estudo.

Para identificar a bibliografia necessária e responder às questões de pesquisa, foi desenvolvida uma estratégia de busca específica. Os termos de busca selecionados foram *serious games, cybersecurity* e *phishing*. As bases de dados selecionadas foram SciELO e Scopus. Essas plataformas possuem alta confiabilidade por parte da comunidade científica; a Scopus foi selecionada devido à ampla gama de estudos que disponibiliza e a SciELO por apresentar um foco em artigos escritos por países falantes de português e espanhol, ampliando a amostra de artigos encontrados.

A adaptação da string de busca foi necessária para o êxito das pesquisas em cada base de dados. Em ambas as bases é possível aplicar alguns critérios de inclusão e exclusão por meio de filtros. Foram escolhidos os idiomas português e inglês e o tipo “artigo”. Na SciELO,

a string possui como versão final: *(“serious games”) OR (“cybersecurity”)) AND (“phishing”)*. Já na Scopus, a versão final engloba os filtros aplicados, sendo portanto: *(("serious-games") AND ("cybersecurity") AND ("phishing")) AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (LANGUAGE,"English") OR LIMIT-TO (LANGUAGE,"Portuguese")) AND (LIMIT-TO (EXACTKEYWORD,"Cybersecurity") OR LIMIT-TO (EXACTKEYWORD,"Phishing"))*.

Os critérios de inclusão e exclusão foram definidos conforme o Quadro 1 a seguir.

Quadro 1 - Critérios de inclusão e exclusão

E1	Estudos que não especificam um público alvo ou que possuam público alvo que não faz parte de um ambiente coletivo.
E2	Artigos que não abordam o *phishing*.
E3	Artigos em idiomas diferentes do português e do inglês.
E4	Estudos secundários.
I1	Estudos que abordam a efetividade, o desenvolvimento e/ou as características de jogos sérios *anti-phishing*.
I2	Estudos que abordam a conscientização digital contra ataques.
I3	Estudos que abordam métodos de ensino sobre cibersegurança.

2.2 Condução

Na SciELO, o filtro automático que limitava os resultados aos disponíveis em coleções do Brasil foi removido. Além disso, devido ao número limitado de artigos na SciELO, optou-se por trocar *AND* por *OR* na relação entre os termos *serious games* e *cybersecurity*. Essa medida retornou artigos relevantes para esse estudo. Ao término desta etapa, foram identificados 3 artigos na SciELO e 28 na Scopus na data de 27 de fevereiro de 2024. Os critérios E2 e E3 puderam ser diretamente aplicados às pesquisas por meio de filtros. Não foram encontrados estudos duplicados.

Após isto, foram analisados primeiro os títulos e resumos dos artigos. Depois, foram lidas a introdução e a conclusão. E, por fim, os artigos foram lidos na íntegra. Os critérios de seleção foram aplicados durante a realização de todos os três níveis. Foram excluídos 2 artigos da SciELO, e 15 da Scopus. No total, 14 artigos foram selecionados para o estudo, compreendendo 1 da SciELO e 13 da Scopus.

3. Resultados

Essa seção subdivide-se para responder às perguntas elaboradas. As respostas foram elaboradas utilizando os dados presentes nos artigos selecionados a partir da RSL.

QP1: Qual é o público alvo dos estudos sobre os jogos sérios *anti-phishing*?

Para responder a essa pergunta foi elaborada a Figura 1. Em seguida, são abordados os dados quantitativos relativos à experiência em tecnologia e cibersegurança exigida dos participantes desses estudos.

A Figura 1 revela que, dos 14 artigos analisados, 13 concentram-se em adultos com idades variando acima de 18 anos. Essa população majoritariamente compreende universitários e/ou profissionais da área de tecnologia. O artigo restante é direcionado a estudantes do ensino primário ao médio, ou seja, jovens com menos de 18 anos. Todos os perfis encontrados se identificaram nas categorias apresentadas na Figura 1 e nota-se um foco significativo no uso de universitários e funcionários de TI como participantes nos estudos.

Foram identificadas duas problemáticas sobre a população abordada nos estudos sobre os jogos sérios de cibersegurança. A primeira menciona estudos recentes realizados em países europeus que indicam que aproximadamente um terço da população nunca recebeu treinamento específico em cibersegurança (Kävrestad et al., 2023).

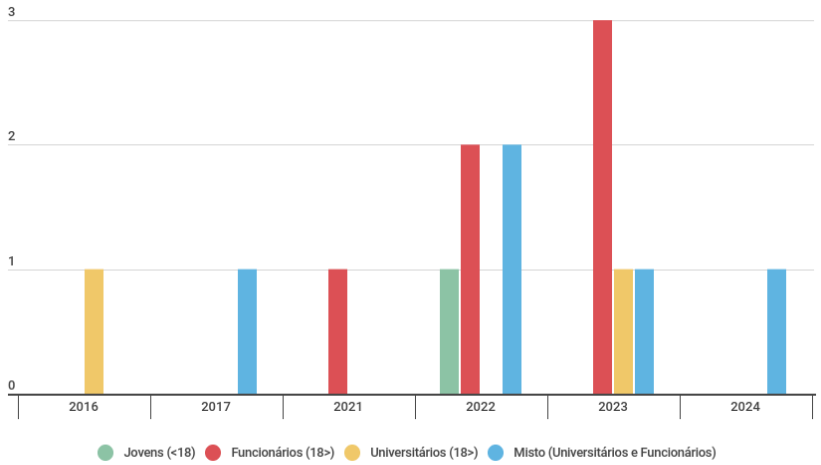

Figura 1 - Distribuição da população nos artigos selecionados por ano

A segunda problemática identificada trata das populações utilizadas para os estudos sobre os jogos sérios *anti-phishing*. Esses estudos frequentemente envolvem populações relacionadas à área de tecnologia, incluindo estudantes das universidades onde os estudos são conduzidos e funcionários de empresas ou setores de tecnologia (Marshall et al., 2024).

Quanto à experiência dos participantes, foram identificados seis artigos que concentram-se em indivíduos com pouca ou nenhuma experiência em temas relacionados à cibersegurança (Arachchilage et al., 2016; Abu-Amara et al., 2021; Kävrestad et al., 2022; Roepke et al., 2022; Shah e Agarwal, 2023; Witsenboer et al., 2022); dois artigos que exploram populações que já receberam treinamento específico ou que atuaram na área de cibersegurança em algum momento de suas carreiras profissionais ou acadêmicas (Cletus et al., 2022; Hull et al., 2023); e seis artigos que abordam participantes com níveis variados de experiência, do básico ao avançado (Angafor et al., 2023; Berens et al., 2024; Chandarman e Van Niekerk, 2017; Kävrestad et al., 2023; Pinto et al., 2022; Singh et al., 2023).

QP2: Quais são as características mais encontradas em jogos sérios *anti-phishing*?

Para responder a essa pergunta, foram analisados 6 jogos a partir da leitura dos estudos selecionados com o objetivo de identificar as características presentes em cada um e contabilizar sua ocorrência. Os jogos mencionados em cada estudo são apresentados a seguir.

Cyber Suraksha, proposto por Shah e Agarwal (2023): Um jogo de cartas que pode envolver até 27 jogadores divididos em 9 grupos, com duração aproximada de 30 minutos. O jogo possui cartas que apresentam problemas do mundo real para os jogadores discutirem entre si e, posteriormente, compartilharem suas ideias com outros grupos. O jogo foca em problemas relacionados ao uso de *smartphones*, como fraudes, e pode ser jogado por qualquer usuário de *smartphone*. Há um *game-master* que atua como guia e feedback.

Jigsaw, mencionado por Kävrestad et al. (2022): Com o formato de quiz, o jogo apresenta situações com e-mails que podem ser legítimos ou fraudulentos. Para jogá-lo, é necessário apenas um computador com acesso a internet; o jogo tem duração aproximada de 5 minutos e fornece ao final a pontuação obtida. Ao longo do jogo existem dicas sobre o que o jogador deve procurar no e-mail apresentado e feedbacks imediatos.

Anti-Phishing Phil, proposto por Arachchilage et al. (2016): O jogo é mobile, tem duração aproximada de 10 minutos e qualquer usuário de smartphone pode jogá-lo. Há uma narrativa sobre um peixe que precisa comer minhocas para crescer; as minhocas representam URLs legítimas ou *phishing*. Há um peixe professor, que funciona como um guia ao longo do jogo e fornece dicas conforme o jogador troca um valor de pontos obtidos.

All Sorts of Phish, apresentado por Roepke et al. (2022): O jogo é digital e qualquer

pessoa sem conhecimento prévio sobre tecnologia pode jogá-lo, com duração de aproximadamente 1,5 minutos por nível. O jogo apresenta um cenário com baús que representam a classificação que o jogador pode dar a cada URL. Há baús para cada tipo de estratégia *phishing* apresentada, assim como um baú para URLs legítimas e um para as URLs que o jogador não sabe como classificar. Por meio de um NPC (*Non-Playable Character*), os jogadores são introduzidos a um novo conhecimento, que será aplicado nos níveis seguintes. Cada acerto ou erro tem efeitos sobre a pontuação.

A Phisher's Bag of Tricks, também apresentado por Roepke et al. (2022): O jogo é digital e não exige conhecimento prévio sobre tecnologia. A mecânica do jogo exige que o próprio jogador crie URLs legítimas ou fraudulentas, conforme o conhecimento necessário sobre as técnicas de manipulação é apresentado. Enviar uma URL errada gera um feedback.

Cyber Shield Game, proposto por Abu-Amara et al. (2021): O jogo é digital e não exige conhecimentos anteriores. Existem quatro níveis, cada um com diferentes cenários para apresentar um problema. Os níveis abordam, respectivamente, a complexidade de senhas, a engenharia social, o *phishing*, e a segurança física. Durante o jogo são encontradas dicas que guiam o jogador a tomar boas decisões de segurança.

As informações foram obtidas também a partir da visualização de imagens dos jogos, apresentadas pelos próprios artigos. O Quadro 2 apresentado a seguir mostra uma sumarização das características encontradas nos jogos selecionados.

Quadro 2 - Relação de jogos e características

	Cyber Suraksha	Jigsaw	Anti-Phishing Phil	All Sorts of Phish	A Phisher's Bag of Tricks	Cyber Shield Game	Total de Ocorrências (T)
Estética colorida	s	s	s	s	s	s	100%
Conflito	s	s	s	s	s	s	100%
Múltiplos conflitos	s	n/m	n/m	n/m	n/m	s	33,33%
Cooperação	s	n	n	n	n	n	16,67%
Níveis	n	n	s	s	s	s	66,67%
Recompensas	n	n	s	s	s	n/m	50%
Pontuação	s	s	s	s	n	n	66,67%
Narrativas/cenários	s	s	s	s	s	s	100%
Duração (min)	30	5	10	1,5	n/m	n/m	-
Estratégia	s	s	s	s	s	s	100%
Recursos	n/m	n	s	s	s	n/m	50%
Corrida para terminar	n/m	n/m	s	s	n/m	n/m	33,33%
Coleta	n	n	s	n	n	n	16,67%
Alinhamento	n	n	n	s	s	n	33,33%
Solução	s	s	s	s	s	s	100%
Construção	n	n	n	n	s	n	16,67%
Correspondência	n/m	n/m	s	s	s	n/m	50%
Categoria	Cartas	PC	Mobile	PC	PC	PC	-
Jogadores	1 a 27	1	1	1	1	1	-
Guia/tutorial	s	s	s	s	s	s	100%
Valor	n/m	R$0,00	R$0,00	n/m	n/m	R$0,00	-
Feedback	s	s	s	s	s	s	100%
Feedback imediato	s	s	s	n	n	s	66,67%

O número total de ocorrências (T) de cada característica pode ser conferido no Quadro 2, variando de 0 a 100% de acordo com a quantidade de "s" presentes na respectiva linha. As características abordadas em cada estudo variam; para lidar com isso, foi utilizada a sigla

"n/m", retratando que uma característica pode não ter sido mencionada no estudo sobre um jogo em questão, porém não é possível presumir que ela não existe.

Aspectos como valor, duração, categoria e jogadores não são mensuráveis quantitativamente neste estudo, visto que não se classificam binariamente. As definições de cada característica são apresentadas no Quadro 3.

Quadro 3 - Definição adaptada das características

Categoria	Característica	Definição
Elementos do jogo	Estética colorida	O design incorpora uma paleta de cores que realça o apelo visual do jogo.
	Conflito	Desafio que o jogador deve superar.
	Múltiplos conflitos	Uma série de desafios variados que o jogador enfrenta.
	Narrativas/cenários	Histórias ou contextos que permeiam o jogo.
	Duração	Pode ser um recurso variável ou uma métrica temporal.
	Estratégia	Requer que o jogador faça escolhas informadas entre múltiplas opções.
	Níveis	Indicam progressão na dificuldade, evoluindo o jogador de novato a mestre.
	Pontuação	Representa a performance do jogador.
	Recompensas	Prêmios concedidos pelo desempenho ou progresso.
	Recursos	Elementos, como moedas, que beneficiam o jogador.
	Cooperação	Jogadores trabalham em conjunto.
Dinâmica central	Solução	Resolução de problemas ou enigmas.
	Correspondência	Identificação de elementos similares ou que se enquadram em uma descrição.
	Coleta	Aquisição de objetos específicos.
	Construção	Criação de algo a partir de recursos determinados.
	Corrida contra o tempo	Completar o jogo ou nível antes que o tempo expire.
	Alinhamento	Organizar peças em uma sequência específica.
Especificações do jogo	Categoria	Refere-se ao ambiente necessário para jogar, podendo ser *mobile* (dispositivos móveis), PC ou de mesa.
	Guia/tutorial	Instruções fornecidas ao longo do jogo.
	Valor	Custo financeiro do jogo para o jogador.
	Feedback	Informações retornadas ao jogador sobre suas ações.
	Feedback Imediato	Respostas instantâneas sobre as ações do jogador.
	Jogadores	Número de jogadores aceitos em uma sessão de jogo. Os jogos podem ser *single player* (um jogador) ou *multiplayer* (mais de um jogador).

O Quadro 3 apresenta as características dos jogos conforme as definições utilizadas por Boller e Kapp (2017), com adaptações e adição de informações relacionadas às especificações dos jogos. As características mais prevalentes ($T \geq 50\%$) incluem estética colorida, conflito, narrativas/cenários, estratégia, guia/tutorial, feedback, *single player*, níveis, pontuação, feedback imediato, recompensas e recursos. Por outro lado, múltiplos conflitos e cooperação apresentaram menor frequência ($T < 50\%$).

QP3: Qual é a percepção dos usuários sobre as características dos jogos sérios *anti-phishing*?

Para responder a esta questão, serão utilizados os feedbacks dos participantes e relatos de preferência presentes nos estudos analisados. As características e os jogos mencionados referem-se ao que foi apresentado na resposta da QP2.

A estética colorida é bem recebida pelos jogadores. Estudos indicam que o uso de cores transcende a mera atribuição de um visual agradável ao jogo; elas são elementos psicológicos que influenciam diretamente a eficácia das estratégias digitais (Roepke et al., 2022). As cores podem ser empregadas como meio de categorização de informações, como

observado em Cyber Suraksha (Shah e Agarwal, 2023), onde as cartas possuem categorias representadas por diferentes cores. Os jogadores relatam que esses fatores contribuem positivamente para a experiência com o jogo.

A presença de tutoriais e guias durante o jogo é bem avaliada. Os jogadores relatam sentir-se mais confiantes durante a experiência quando recebem instruções e dicas para ter sucesso no desafio proposto (Shah e Agarwal, 2023). No entanto, se os tutoriais ou guias forem complexos, podem gerar confusão e frustração (Kävrestad et al., 2022).

A presença de múltiplos conflitos é vista de forma positiva pelos jogadores e amplia o conhecimento dos jogadores sobre ameaças reais (Kävrestad et al., 2022). Se o jogo focar apenas em um tipo de ataque, os jogadores podem perder a oportunidade de aprender sobre outras ameaças (Hull et al., 2023).

Jogos com histórias envolventes e cenários realistas são apreciados. Os jogadores sentem-se mais envolvidos quando a narrativa é relevante para o tema da segurança cibernética. Em contrapartida, narrativas fracas ou irrelevantes podem diminuir o interesse dos jogadores. Se o contexto não fizer sentido, a experiência pode parecer superficial (Chandarman & Van Niekerk, 2017).

A utilização de vídeos foi bem recebida por participantes de métodos de treinamento *anti-phishing*, onde constatou-se que um vídeo de 5 minutos pode ter efeitos no comportamento seguro do usuário por 5 meses (Berens et al., 2024). A implementação de vídeos em métodos de treinamento baseado em jogos é um fator a ser experimentado.

A dinâmica central dos jogos tem sido criticada por seus limitados mecanismos que não permitem uma avaliação detalhada do conhecimento adquirido pelos jogadores. Apesar disso, dinâmicas simples foram bem recebidas pelos jogadores, que relatam se concentrar melhor em utilizar o conhecimento adquirido quando o jogo é centrado em jogabilidade simples, sem grandes desafios mecânicos (Roepke et al., 2022).

O feedback e o feedback imediato foram bem avaliados em todos os jogos que os possuem. Apesar de ambos os feedbacks serem avaliados de forma positiva, foi identificada uma preferência dos jogadores pelo feedback imediato. Essa preferência deve-se à possibilidade de saber quais erros foram cometidos assim que uma resposta é enviada, auxiliando na retenção do conhecimento proposto (Abu-Amara et al., 2021). As consequências das ações dos jogadores devem ser claras, caso contrário, podem gerar confusão e prejudicar a experiência do jogador (Angafor et al., 2023).

Os jogos multiplayer são bem recebidos por incentivarem a colaboração e a competição saudável entre os jogadores. A interação social aumenta o engajamento dos jogadores com os jogos (Witsenboer et al., 2022), como visto em Cyber Suraksha (Shah e Agarwal, 2023). No entanto, foi relatado que, se a interação social for mal implementada, os jogadores podem se sentir desconfortáveis ou desinteressados (Cletus et al., 2022).

Os sistemas de pontuação foram bem recebidos pelos jogadores. Eles relatam que esse elemento aumenta o engajamento e a motivação para continuar jogando e melhorar suas habilidades (Roepke et al., 2022). Por outro lado, alguns jogadores relataram que sistemas de pontuação complexos ou confusos podem ser desmotivadores. Se os jogadores não entenderem como ganhar pontos ou o que os pontos representam, eles podem se sentir frustrados e menos propensos a continuar jogando (Kävrestad et al., 2023).

A duração é uma característica que apresenta variações de acordo com cada mecânica de jogo e experiência prévia do usuário com os temas abordados. O método de treinamento Game-Based Training é caracterizado por sua curta duração, assim como o Context-Based Micro-Training. Estudos indicam que a disseminação do conhecimento ciber seguro por meio desses é efetiva (Kävrestad et al., 2022). Em contrapartida, as opiniões de usuários sobre a duração dos treinamentos indicam que métodos de treinamento completo, realizados eventualmente, são preferíveis aos treinamentos curtos constantes (Kävrestad et al., 2023).

Quanto ao valor dos jogos, pesquisas indicam que há uma divisão de opiniões entre os usuários. Parte deles expressa interesse em jogar os jogos propostos caso sejam gratuitos. Outros usuários afirmam que algo bom e gratuito não parece confiável e, portanto, estariam dispostos a pagar pequenas quantias pelo jogo (Arachchilage et al., 2016).

4. Discussão

Os resultados indicam uma diversidade de características nos jogos sérios *anti-phishing*, com todos os artigos analisados relatando sua eficácia. No entanto, a literatura costuma não detalhar a integração de teorias de aprendizagem e métodos de ensino, gerando incertezas quanto à aplicação desses recursos (Hwang e Helser, 2022). Análises mais aprofundadas sobre o tema podem ser feitas visando otimizar o aprendizado dos jogadores.

Outra lacuna identificada é a falta de especificação dos requisitos essenciais de hardware e software, além da escassez de informações sobre as tecnologias utilizadas no desenvolvimento. Disponibilizar tais informações facilitaria o desenvolvimento colaborativo entre os interessados no software, corroborando com as ideias de Connolly et al. (2012).

Em relação às características dos jogos, Silva et al. (2021) relatam que as mais apreciadas são: design atraente, feedback e regras claras. A apreciação dessas por parte dos jogadores vai de acordo com o encontrado no presente estudo. Entretanto, Silva et al. (2021) relatam também que os sistemas de pontuação e as narrativas não são consideradas relevantes pelos jogadores, fator que contrapõe parcialmente os resultados encontrados e denota a necessidade de maiores investigações sobre a aplicação e avaliação dessas características.

Uma problemática foi identificada por meio deste estudo: os jogos são desenvolvidos para serem métodos de treinamento eficazes e rápidos. Kävrestad et al. (2023) discutem que, enquanto treinamentos completos são bem recebidos, treinamentos menores e contínuos não despertam tanto interesse, possivelmente devido à percepção de aprendizado mais profundo com grandes quantidades de informação. Isso levanta questões sobre a necessidade de continuar desenvolvendo treinamentos rápidos (Kumaraguru et al., 2010).

A compreensão do conhecimento tecnológico dos usuários finais é mencionada, mas muitas vezes os estudos se concentram em populações com conhecimento técnico prévio, selecionando participantes de plataformas universitárias de cursos de tecnologia. Isso deixa lacunas sobre as expectativas em relação a usuários sem conhecimento tecnológico, (Abawajy, 2014). Além disso, faltam evidências sobre o sucesso dos programas em promover mudanças comportamentais sustentadas, como apontado por Marshall et al. (2024).

A percepção dos jogadores sobre os jogos sérios *anti-phishing* varia conforme sua familiaridade com jogos, tecnologia e *phishing*. Portanto, é necessário revisar a população utilizada nos estudos para refletir o usuário final do jogo. O perfil identificado neste estudo é semelhante ao de trabalhos recentes, como Marshall et al. (2024), corroborando a validade dos resultados obtidos. As análises direcionadas ao público-alvo indicam ainda que, entre 2022 e 2024, houve um crescente interesse em compreender como o público adulto com pouca ou nenhuma experiência em cibersegurança lida com ameaças cibernéticas.

Uma proporção menor de estudos focaram em populações experientes com ameaças. Observou-se que o número de estudos sobre essa área aumentou durante a pandemia de Covid-19. O interesse pelo tema se manteve no período pós-pandemia, sugerindo que a mudança no ambiente de trabalho destacou a importância da cibersegurança no trabalho remoto e da ampliação do ensino desses conceitos básicos para diferentes perfis de usuários.

Por fim, embora se explorem os resultados do aprendizado e sua relação com as características do jogo, a teoria de aprendizado e as características do jogador, a coleta de feedback dos jogadores não é mencionada como um procedimento padrão na avaliação dos jogos (Hwang e Helser, 2022). Ainda, notou-se a falta de uniformidade e direcionamento na obtenção de feedback, o que pode afetar a compreensão sobre a preferência do jogador,

refletindo negativamente na experiência e no engajamento do usuário final dos jogos em um cenário de aplicação real de treinamento, conforme Ifinedo (2012).

5. Conclusões

Este estudo examinou a percepção dos jogadores sobre as características dos jogos sérios *anti-phishing* através de uma RSL, focando em estratégias de design e implementação que otimizem sua eficácia na prevenção de ataques de phishing e promoção de comportamentos seguros. Foi identificado um viés de seleção nos participantes dos estudos, frequentemente recrutados em plataformas de tecnologia, o que pode não refletir o usuário final dos jogos. Além disso, características menos comuns, como múltiplos conflitos e cooperação, foram bem recebidas pelos jogadores, enquanto características mais comuns, como a curta duração dos métodos de treinamento, geram percepções divergentes, sugerindo a necessidade de investigações adicionais sobre a percepção do jogador com relação às características dos jogos sérios *anti-phishing*.

Os resultados evidenciam a necessidade de aprimorar a integração entre teorias de aprendizagem e metodologias padronizadas para a categorização das características dos jogos. Também foi identificada uma falta de uniformidade na coleta de feedback dos jogadores, destacando a necessidade de uma avaliação mais abrangente de sua percepção sobre os jogos. Para aumentar a eficácia dos jogos sérios *anti-phishing*, recomenda-se uma reavaliação da população estudada, a categorização detalhada das características dos jogos e o desenvolvimento de métodos rigorosos para coleta e análise do feedback dos jogadores.

Agradecimento

A realização desse trabalho contou com o apoio da Fundação de Apoio à Pesquisa do Distrito Federal (FAPDF).

Referências

ABAWAJY, J. User preference of cyber security awareness delivery methods. **Behaviour & Information Technology**, v. 33, n. 3, p. 237-248, 2012. DOI: 10.1080/0144929X.2012.708787.

ABU-AMARA, F.; ALMANSOORI, R.; ALHARBI, S.; ALHARBI, M.; ALSHEHHI, A. A novel SETA-based gamification framework to raise cybersecurity awareness. **International Journal of Information Technology**, v. 13, p. 2371–2380, ago. 2021. DOI: 10.1007/s41870-021-00760-5.

ANGAFOR, G. N.; YEVSEEVA, I.; MAGLARAS, L. Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise. **Information and Computer Security**, v. 31, n. 4, p. 404-426, 2023. DOI: 10.1108/ICS-05-2022-0085.

ANTI-PHISHING WORKING GROUP (APWG). **Attack Phishing Trends Report - 1Q 2023**. 2023. Disponível em: <https://apwg.org/trendsreports/>. Acesso em: 20 mar. 2024.

ANTI-PHISHING WORKING GROUP (APWG). **Phishing Attack Trends Report - 2Q 2023**. 2023. Disponível em: <https://apwg.org/trendsreports/>. Acesso em: 20 mar. 2024.

ARACHCHILAGE, N. A. G.; LOVE, S.; BEZNOSOV, K. Phishing threat avoidance behaviour: An empirical investigation. **Computers in Human Behavior**, v. 60, p. 185-197, jul. 2016. DOI: 10.1016/j.chb.2016.02.065.

BATTISTELLA, P. E; WANGENHEIM, C. G. von. Games for Teaching Computing in Higher Education – A Systematic Review. **IEEE Technology and Engineering Education (ITEE)**, v. 1, no. 3, p. 8-30 mar. 2016. Disponível em: <https://api.semanticscholar.org/CorpusID:64431187>.

BERENS, B. M.; MOSSANO, M.; VOLKAMER, M. Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video. **Computers & Security**, v. 137, Art.

103620, 2024. DOI: 10.1016/j.cose.2023.103620.
BOLLER, S.; KAPP, K. M. **Play to Learn: Everything You Need to Know about Designing Effective Learning Games**. Alexandria, VA, EUA: ATD Press, 2017. 168 p.
CHANDARMAN, R.; VAN NIEKERK, B. Students' cybersecurity awareness at a private tertiary educational institution. **The African Journal of Information and Communication**, v. 20, p. 133-155, 2017. DOI: 10.23962/10539/23572.
CLETUS, A.; WEYORY, B.; OPOKU, A. Improving Social Engineering Awareness, Training and Education (SEATE) using a Behavioral Change Model. **International Journal of Advanced Computer Science and Applications**, v. 13, n. 5, 2022. DOI: 10.14569/IJACSA.2022.0130572.
CONNOLLY, T. M.; BOYLE, E. A.; MACARTHUR, E.; HAINEY, T.; BOYLE, J. M. A systematic literature review of empirical evidence on computer games and serious games. **Computers & Education**, v. 59, n. 2, p. 661-686, 2012. DOI: 10.1016/j.compedu.2012.03.004.
FELIZARDO, K. R.; NAKAGAWA, E. Y.; FABBRI, S. C. P. F.; FERRARI, F. C. **Revisão Sistemática da Literatura em Engenharia de Software: Teoria e Prática**. 1. ed. Rio de Janeiro: Elsevier, 2017. 125 p.
GERHARDT, T. E.; SILVEIRA, D. T. (Orgs.). **Métodos de Pesquisa**. 1. ed. Porto Alegre: Editora da UFRGS, 2009. 120 p.
HULL, D. M.; SCHUETZ, S. W.; LOWRY, P. B. Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. **Computers & Security**, v. 129, Art. 103252, 2023. DOI: 10.1016/j.cose.2023.103252.
HWANG, M. I.; HELSER, S. Cybersecurity educational games: a theoretical framework. **Information and Computer Security**, v. 30, n. 2, p. 225-242, 2022. DOI: 10.1108/ICS-10-2020-0173.
IFINEDO, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. **Computers & Security**, v. 31, n. 1, p. 83-95, 2012. DOI: 10.1016/j.cose.2011.10.007.
KITCHENHAM, B. **Procedures for performing systematic reviews**. Keele, UK: Keele University, 2004. 28 p. Disponível em: <https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf>.
KÄVRESTAD, J.; HAGBERG, A.; NOHLBERG, M.; RAMBUSCH, J.; ROOS, R.; FURNELL, S. Evaluation of Contextual and Game-Based Training for Phishing Detection. **Future Internet**, v. 14, n. 4, Art. 104, 2022. DOI: 10.3390/fi14040104.
KÄVRESTAD, J.; FURNELL, S.; NOHLBERG, M. User perception of Context-Based Micro-Training – a method for cybersecurity training. **Information Security Journal: A Global Perspective**, v. 33, n. 2, p. 121–137, 2023. DOI: 10.1080/19393555.2023.2222713.
KUMARAGURU, P.; SHENG, S.; ACQUISTI, A.; CRANOR, L. F.; HONG, J. Teaching Johnny not to fall for phish. **ACM Transactions on Internet Technology**, v. 10, n. 2, Art. 7, p. 1-31, jun. 2010. DOI: 10.1145/1754393.1754396.
MARSHALL, N.; STURMAN, D.; AUTON, J. C. Exploring the evidence for email phishing training: A scoping review. **Computers & Security**, v. 139, Art. 103695, 2024. DOI: 10.1016/j.cose.2023.103695.
PINTO, L.; BRITO, C.; MARINHO, V.; PINTO, P. Assessing the Relevance of Cybersecurity Training and Policies to Prevent and Mitigate the Impact of Phishing Attacks. **Journal of Internet Services and Information Security**, v. 12, n. 4, p. 23-38, nov. 2022. DOI: 10.58346/JISIS.2022.I4.002.
ROEPKE, R.; DRURY, V.; MEYER, U.; SCHROEDER, U. Exploring and Evaluating Different Game Mechanics for Anti-Phishing Learning Games. **International Journal of Serious Games**, v. 9, n. 3, p. 23-41, 2022. DOI: 10.17083/ijsg.v9i3.501.
SHAH, P.; AGARWAL, A. Cyber Suraksha: a card game for smartphone security awareness.

Information and Computer Security, v. 31, n. 5, p. 576-600, 2023. DOI: 10.1108/ICS-05-2022-0087.

SILVA, M. A. S.; SALES, A. B. de; MENDES, F. F. Aspectos de qualidade em jogos sérios digitais. **Revista Novas Tecnologias na Educação**, v. 19, n. 1, p. 207–216, 2021. DOI: 10.22456/1679-1916.118428.

SINGH, K.; AGGARWAL, P.; RAJIVAN, P.; GONZALEZ, C. Cognitive elements of learning and discriminability in anti-phishing training. **Computers & Security**, v. 127, Art. 103105, abr. 2023. DOI: 10.1016/j.cose.2023.103105.

WITSENBOER, J. W. A.; SIJTSMA, K.; SCHEELE, F. Measuring cyber secure behavior of elementary and high school students in the Netherlands. **Computers & Education**, v. 186, Art. 104536, 2022. DOI: 10.1016/j.compedu.2022.104536.

Data de submissão: 02/06/2024 | Data de revisão: 19/06/2024 | Data de aceite: 28/06/2024 | Data de publicação: 31/07/2024