

# Jogos Digitais Educativos como Ferramenta de Ensino e Conscientização sobre Golpes de Engenharia Social: Uma Revisão Sistemática da Literatura

Uilisses Viana da Silva<sup>1</sup>, Heleno Fülber<sup>1</sup>, Bruno Merlin<sup>1</sup>, Tânia Lobo Viana<sup>1</sup>,  
Viviane Almeida dos Santos<sup>1</sup>, Andressa da Silva<sup>2</sup>

<sup>1</sup>Programa de Pós-graduação em Computação Aplicada – Universidade Federal do Pará (UFPA) – Campus Tucuruí – Tucuruí – PA – Brasil

<sup>2</sup>Instituto Federal do Ceará (IFCE) – Campus Acaraú – Acaraú – CE – Brasil

{uilissesviana, andressa.ene}@gmail.com,  
{fulber, brunomerlin, vsantos}@ufpa.br, tania.viana@tucuruui.ufpa.br

**Abstract.** *The increase in digital threats in Brazil is alarming, particularly scams disseminated through social media, text messages, and emails using social engineering (SE) techniques. The human factor continues to represent the weakest link in the digital environment due to the lack of specialized knowledge or inattention in everyday technological activities. Educational digital games (EDGs) have emerged as an active learning tool, enabling users to interact with simulated environments, engage in interactive dialogues, and receive immediate feedback. This study presents an analysis of 46 articles identified through a systematic literature review (SLR) that investigated the use of EDGs for teaching and raising awareness about SE scams. The results indicate phishing as the predominant technique addressed in the studies, highlight the educational theories incorporated into the games, and demonstrate positive effectiveness in 89% of the evaluations.*

**Resumo.** *É alarmante o aumento de ameaças digitais no Brasil, especialmente os golpes disseminados por redes sociais, mensagens de texto e e-mails, utilizando técnicas de engenharia social (ES). O fator humano continua a representar o elo mais fraco do ambiente digital, em decorrência da ausência de conhecimento especializado ou falta de atenção no cotidiano tecnológico. Os jogos digitais educativos (JDEs) têm constituído uma ferramenta de ensino, do contexto ativo, que possibilita aos usuários a interação com ambientes simulados, diálogos interativos e mecanismo de feedback imediato. Esta pesquisa apresenta a análise de 46 artigos identificados a partir de uma revisão sistemática da literatura (RSL), que investigam o uso de JDEs para o ensino e a conscientização sobre golpes de ES. Os resultados desta revisão apresentam o phishing como a técnica predominante nos estudos, as teorias educacionais incorporadas aos jogos e a eficácia positiva em 89% das avaliações.*

## 1. Introdução

Os golpes digitais no Brasil impactam os mais diversos públicos de consumo e faixas etárias. Como suporte a essas práticas criminosas, a ES é um método que utiliza diferentes técnicas e se beneficia da vulnerabilidade do fator humano em sistemas computacionais [Lopes et al. 2024]. Para a ABIN (Associação Brasileira de Inteligência) [ABIN 2021], é

um modelo de ataque, sem violência física, capaz de manipular e explorar a confiança das vítimas, utilizando aspectos psicológicos visa obter informações a partir de pressões: de tempo, de autoridade, de ganho e empatia. Os ataques podem ocorrer por diferentes meios, sendo o mais comum via e-mail (*phishing*), mas também em suas variantes, via mensagens de texto (*smishing*) e ligações telefônicas (*vishing*) [Neves and Pereira 2020].

Segundo dados do Instituto de Pesquisa DataSena [DataSena 2024], mais de 24% dos brasileiros maiores de 16 anos foram vítimas de golpes digitais entre 2023 e 2024. De 2022 a 2023, os estelionatos por meio digital aumentaram 13,6% no Brasil, e de maneira alarmante os estados da Paraíba, Roraima, Piauí e Amazonas, que apresentaram mais que o dobro de ocorrências das fraudes digitais [FBSP 2024].

Nesse contexto, o conhecimento em segurança da informação exerce papel fundamental para prevenir e combater as atividades criminosas que exploram vulnerabilidades em sistemas e serviços dos mais diversos tipos. Ademais, tem como meta a criação de mecanismos de instrução para os usuários sobre conceitos e práticas a serem adotadas no cotidiano, seja no uso de seus próprios dispositivos ou em ambientes corporativos [Baars et al. 2017].

Dada a grandeza e o expressivo número de vítimas, identificar metodologias de ensino para capacitar os usuários em conhecimento de segurança digital é fundamental para a redução dos danos. Sob essa ótica, [Sousa et al. 2024] sugerem que as instituições educacionais exercem um papel fundamental no processo de ensino sobre segurança digital, ao promover o diálogo contínuo sobre a temática, e evidenciando práticas como: identificação de atividades suspeitas, criação de senhas fortes e o cuidado ao compartilhar dados.

Ainda sobre o papel das instituições no processo de aprendizagem, a BNCC (Base Nacional Comum Curricular) [Brasil, 2022] recomenda, em seu eixo Mundo Digital, o desenvolvimento de competências relacionadas à segurança cibernética. Os estudantes devem compreender formas seguras de acessar, armazenar e distribuir informações na internet, incluindo a sugestão de utilizar ou implementar soluções tecnológicas que apoiem esse processo.

Segundo [Moran 2015], as metodologias ativas de aprendizagem promovem um maior engajamento dos alunos ao incorporarem elementos disruptivos, como desafios, resolução de problemas e jogos no processo de ensino. Com o auxílio da simulação de situações e problemas reais, os jogos, coletivos ou individuais, favorecem um envolvimento mais profundo, permitindo aos estudantes evoluírem no seu próprio ritmo e de modo a atender suas necessidades específicas. Nesse sentido, a área de jogos digitais, que surgiram com a finalidade de entreter, também possui vertentes educacionais e é capaz de promover melhorias na aprendizagem, ao oferecer um ambiente mais interativo e lúdico [Alves and Coutinho 2016].

O objetivo deste trabalho é realizar uma RSL para identificar, analisar e sintetizar evidências científicas que utilizam JDEs como ferramenta de aprendizagem e conscientização sobre golpes de engenharia social. Esse tipo de pesquisa mostra-se relevante, podendo identificar características, melhorias e lacunas existentes para futuros estudos que propõem a utilização de JDEs para o tema investigado.

Este trabalho está organizado da seguinte forma: a Seção 2 apresenta trabalhos com propostas correlatas de investigação, a Seção 3 a metodologia utilizada para

identificação dos trabalhos analisados; a Seção 4 detalha os resultados obtidos neste estudo; a Seção 5 as discussões acerca das lacunas percebidas, conclusões e trabalhos futuros.

## 2. Trabalhos Correlatos

Estão disponíveis algumas revisões correlatas à investigação proposta, dentre elas duas fornecem informações relevantes para entendimento do cenário de JDEs para a área de segurança cibernética.

[Ferreira et al. 2024] conduziram uma RSL para analisar a percepção dos jogadores acerca de jogos sérios como ferramentas de apoio na aprendizagem sobre *phishing*. Após a análise de 6 jogos, informam que as características predominantes nos jogos são: estética colorida, desafios a serem superados, narrativa envolvente e seleções estratégicas relacionadas aos jogos; a resolução de problemas para a dinâmica do jogo; guias e *feedback* instantâneo para as especificações. Além disso, os jogadores têm preferência por jogos de curta duração e de mecânica simples.

[Souza et al. 2025] propõem analisar como jogos sérios podem ser ferramentas de apoio educativo na conscientização de práticas de higiene cibernética através de uma RSL. Após a análise de 14 estudos, os autores identificaram que a maior parte do público são universitários e profissionais de TI (tecnologia da informação), com predominância do gênero masculino. A técnica mais abordada nos estudos é a de simulação, para criação de ambientes realistas, seguido pelo foco em identificar ameaças e melhorar a segurança.

Os achados deste trabalho estão alinhados às revisões anteriores nesses aspectos, entretanto fica claro que limitações metodológicas continuam sem solução. [Ferreira et al. 2024] destacam a ausência de análises consistentes sobre as teorias de aprendizagem, apesar de não deixar claro como identificou esses aspectos, e [Souza et al. 2025] ressaltam a importância de alinhar as reais necessidades do cotidiano aos temas propostos nos jogos e a padronização em critérios de avaliação.

Acrescenta-se a constatação de que poucos estudos adotaram grupos de controle ou realizaram testes longitudinais. Como consequência, apesar do consenso de que os JDEs auxiliam no engajamento, aprendizagem e conscientização, faltam mais evidências com sua superioridade em relação aos métodos tradicionais de ensino ou a eficácia na retenção do conhecimento a longo prazo. Assim, pesquisas futuras devem propor testes e aplicações mais robustas, capazes de superar ou minimizar essas limitações.

## 3. Metodologia da Pesquisa

A RSL, segundo [Kitchenham and Charters 2007], é um método utilizado para identificar e avaliar pesquisas relevantes para uma determinada questão de pesquisa ou área temática de interesse. Difere-se de uma revisão convencional por apresentar um protocolo que identifica: os objetivos da revisão e as questões de pesquisa; uma estratégia de busca bem definida; a documentação da estratégia adotada, para replicabilidade do processo; a exigência de critérios de inclusão, exclusão e qualidade; e a apresentação dos resultados obtidos. Assim, a RSL é considerada uma abordagem justa, por seguir uma metodologia rigorosa, confiável e auditável.

Para dar suporte a apresentação dos resultados, optou-se pelo fluxograma do método PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-*

*Analyses*), que é uma diretriz amplamente adotada, possibilitando melhor compreensão e rastreabilidade das etapas realizadas na triagem dos estudos [Page et al. 2020].

### 3.1. Questões de Pesquisa

Por meio da estratégia PICO foram definidos os seguintes elementos: *Problem* (golpes de engenharia social), *Intervention* (JDEs como ferramenta de ensino), *Comparison* (utilização ou não de métodos tradicionais de ensino) e *Outcome* (aprendizagem e conscientização sobre golpes de engenharia social). A partir dessas definições surgem as questões de pesquisa (QP):

**QP1:** Quais os golpes de engenharia social abordados nos JDEs dos estudos?

**QP2:** Quais as metodologias ou teorias educacionais inseridas nos JDEs dos estudos?

**QP3:** Qual a eficácia na aprendizagem e conscientização sobre golpes de engenharia social ao aplicar JDEs?

### 3.2. String de busca

Diante das QPs e dos elementos PICO, realizou-se uma análise de descritores para identificar os principais termos relacionados ao tema proposto, com a finalidade de facilitar a elaboração da *string* de busca, e suas adaptações, a ser utilizada nas fontes dos estudos. As palavras-chave e seus sinônimos, nas línguas portuguesa e inglesa, estão identificadas no Quadro 1.

**Quadro 1. Palavras-chave em português e inglês.**

| Palavra-chave em português | Palavra-chave em inglês   | Sinônimo em Inglês       |
|----------------------------|---------------------------|--------------------------|
| Jogo Sérió                 | <i>Serious Games</i>      |                          |
| Jogo Educativo             | <i>Educational Game</i>   |                          |
| Jogo                       | <i>Game</i>               |                          |
| Engenharia Social          | <i>Social Engineering</i> |                          |
|                            | <i>Phishing</i>           | <i>Smishing, Vishing</i> |
| Aprendizagem               | <i>Awareness</i>          |                          |
| Prevenção                  | <i>Prevention</i>         |                          |
| Educação                   | <i>Education</i>          |                          |

As palavras-chave foram agrupadas em três blocos, a partir dos elementos PICO, para abranger a metodologia utilizada, a área foco e o objetivo da pesquisa. Nesse cenário o elemento Comparison não foi aplicado na string, pois é intuito deste trabalho analisar estudos com ou sem adoção de métodos tradicionais, caso existam grupos de controle. Os sinônimos foram agrupados com o operador lógico OR, os termos do mesmo elemento foram agrupados com parênteses () e os blocos agrupados com o operador AND. Portanto, após testes nas combinações das sentenças, resultou-se na seguinte versão final da string de busca: (“serious game” OR “educational game” OR game) AND (“social engineering” OR phishing OR smishing OR vishing OR cybersecurity) AND (awareness OR education

OR prevention). As adaptações na *string* para as diferentes bases estão descritas no protocolo de revisão<sup>1</sup>.

### 3.3. Bases de dados

As bases de dados utilizadas foram a ACM, IEEE Xplore, Scopus e Web of Science. A escolha dessas fontes ocorreu em virtude da indexação de periódicos de alta qualidade, seus recursos de filtragem e pelo número expressivo de estudos da área de computação. O acesso ocorreu por intermédio da rede CAFE (Comunidade Acadêmica Federada da RNP) do Portal CAPES. Além das bases indexadas, também foram analisados, de modo manual, os anais do CBIE, SBIE, WIE e Educomp, assim como os repositórios das revistas Renote e RBIE. A escolha dessas fontes não indexadas deu-se pela relevância de trabalhos relacionados à informática no âmbito educacional brasileiro. Todos os acessos ocorreram entre os meses de março a maio de 2026.

### 3.4. Critérios de inclusão e exclusão

Os critérios de inclusão e exclusão foram definidos para identificar os trabalhos que respondam às questões de pesquisa. Os critérios de inclusão (CI) e exclusão (CE) foram adotados ao longo da RSL, visando extrair estudos recentes, que sejam primários e concluídos com o uso de JDEs para a temática investigada, incluindo a aplicação com usuários. Os idiomas inglês e português foram definidos tendo em vista o cenário brasileiro, assim como o padrão internacional de publicações com resumo ou todo o conteúdo em inglês. Todos os critérios estabelecidos estão descritos no Quadro 2.

**Quadro 2. Critérios de inclusão e exclusão.**

| <b>Tipo</b> | <b>Critério adotado</b>                                                   |
|-------------|---------------------------------------------------------------------------|
| CI1         | Os estudos devem ter o ano de publicação entre 2015 e 2026.               |
| CI2         | O idioma de publicação seja o inglês ou português.                        |
| CI3         | Possui em seu título, resumo ou palavras-chave relação com a pesquisa.    |
| CI4         | O texto completo é acessível via Portal CAPES ou acesso institucional.    |
| CE1         | Os estudos que estejam duplicados nas diferentes bases.                   |
| CE2         | Estudos com temas que não abordem sobre golpes de engenharia social.      |
| CE3         | Estudos que não sejam pesquisa primária (revisão, survey, tutorial etc.). |
| CE4         | Os estudos cuja metodologia não esteja relacionada a jogos digitais.      |
| CE5         | Estudos que não sejam artigos completos (índice, notícia, resumo etc.).   |
| CE6         | Estudos que não foram concluídos (apenas modelagem, sem avaliação etc.).  |

### 3.5. Triagem e seleção dos estudos

A busca inicial revelou 645 publicações nas bases de dados, 98 da ACM, 190 da IEEE, 217 da Scopus e 140 da Web of Science, além de 4 publicações por outros métodos, 2 dos Anais Extendidos do SBGames e 2 da revista Renote. Na primeira etapa aplicou-se o filtro de recorte temporal de 2015 a 2026 e a identificação de duplicados, sendo retirados

<sup>1</sup> <https://osf.io/j4dxy/overview>.

190 trabalhos. Dos 459 restantes para o processo de triagem, 19 não foram recuperados. Na fase de triagem, a segunda etapa consistiu na identificação dos termos de busca e aplicação dos critérios de inclusão e exclusão nos títulos, resumos e palavras-chave, totalizando 287 estudos não elegíveis. Na terceira etapa realizou-se a leitura completa, extração de dados e aplicação dos CE, em que dos 153 analisados apenas 46 foram incluídos no corpus final. A Figura 1 possibilita a visualização de todo o processo de triagem e seleção dos estudos, a partir de uma adaptação do método PRISMA 2020.

O processo de triagem e seleção foi realizado por 2 revisores independentes, com a intervenção de um terceiro revisor em casos de discordância na inclusão ou exclusão dos estudos. Ressalta-se a aplicação dos filtros das próprias bases para o recorte temporal, assim como as ferramentas: Rayyan, para identificação de duplicatas e a segunda etapa na fase de triagem; e Zotero, para a terceira etapa. O *NotebookLM*, um assistente de pesquisa baseado em inteligência artificial generativa, foi utilizado exclusivamente como ferramenta de apoio na fase de extração de dados da terceira etapa, com os resultados supervisionados pelos revisores. A adoção do *NotebookLM* nesta pesquisa e os *prompts* executados estão disponíveis no termo de uso de inteligência artificial.

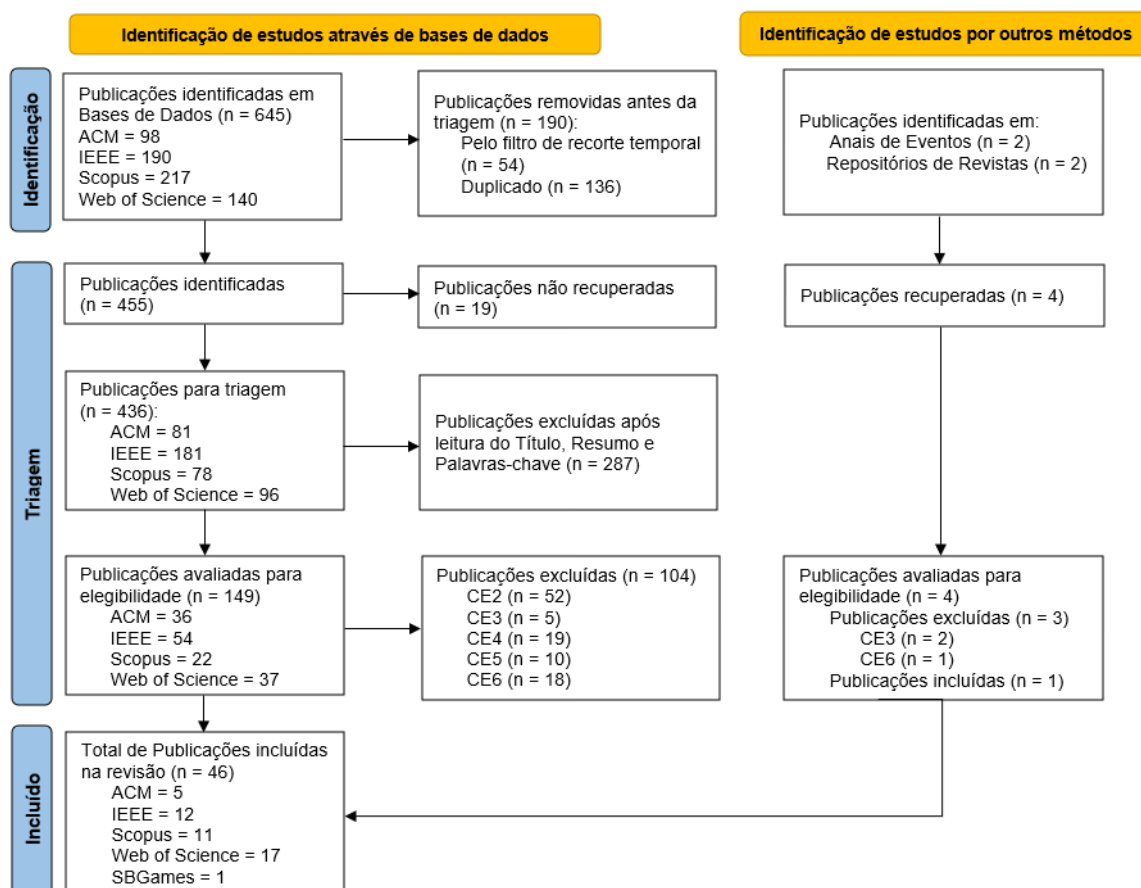


Figura 1. Fluxograma de seleção dos artigos. Adaptado de [Page et al. 2022].

### 3.6. Critérios de qualidade

Além dos critérios de inclusão e exclusão, Kitchenham e Charters [2007] sugerem a avaliação do rigor metodológico dos estudos selecionados, incluindo a análise qualitativa dos resultados. Diante dessa proposta, foram definidos critérios com as seguintes notas: Não Adequado/Informado (0), Parcialmente Adequado/Informado (0,5) e Totalmente

Adequado/Informado (1). Além da identificação foram atribuídos pesos, com base na relevância das ameaças às validades internas e externas dos estudos. O Quadro 3 apresenta os 10 critérios estabelecidos e seus pesos, de tal modo que um estudo pode ir de *score* 0 a 10.

**Quadro 3. Critérios de qualidade.**

| <b>Critério Avaliado</b>                                                                                  | <b>Peso</b> |
|-----------------------------------------------------------------------------------------------------------|-------------|
| CQ1 - Apresenta de forma clara os objetivos, hipóteses e/ou questões de pesquisa?                         | 0,5         |
| CQ2 - Descreve as tecnologias utilizadas (linguagem, plataforma de distribuição etc.) no desenvolvimento? | 0,5         |
| CQ3 - Descreve de forma detalhada o JDE (mecânicas, objetivos, enredo etc.)?                              | 0,5         |
| CQ4 - Apresenta de forma clara as técnicas e golpes de engenharia social abordados no jogo?               | 0,5         |
| CQ5 - Apresenta de forma clara alguma teoria de aprendizagem adotada no JDE?                              | 1           |
| CQ6 - Apresenta de forma clara o perfil e quantidade de participantes?                                    | 1,5         |
| CQ7 - Utiliza coleta de dados adequada (questionários pré-teste e pós-teste, entrevista, testes etc.)?    | 1,5         |
| CQ8 - Caso utilize de grupo de controle, apresenta de forma clara o método tradicional de ensino?         | 1           |
| CQ9 - Apresenta de forma adequada os resultados da análise qualitativa e/ou quantitativa?                 | 1,5         |
| CQ10 - O estudo apresenta as limitações ou ameaças à validade?                                            | 1,5         |

#### 4. Resultados

Os artigos selecionados com seus identificadores e *scores*, de acordo com a qualidade metodológica, estão descritos na Tabela 1.

**Tabela 1. Identificação dos estudos incluídos e seus scores de qualidade.**

| <b>ID</b> | <b>Autor(es)</b>     | <b>Ano</b> | <b>Score</b> | <b>ID</b> | <b>Autor(es)</b>      | <b>Ano</b> | <b>Score</b> |
|-----------|----------------------|------------|--------------|-----------|-----------------------|------------|--------------|
| A1        | Panga et al.         | 2022       | 9,25         | A24       | Wibawa et al.         | 2022       | 6,75         |
| A2        | Keller et al.        | 2025       | 9            | A25       | Alma'ariz et al.      | 2022       | 6,75         |
| A3        | Roepke et al.        | 2022       | 9            | A26       | Kävrestad et al.      | 2022       | 6,75         |
| A4        | Maqsood and Chiasson | 2021       | 9            | A27       | Garcia and Parra      | 2021       | 6,5          |
| A5        | Yasin et al.         | 2025       | 8,75         | A28       | Zolkifly et al.       | 2025       | 6,5          |
| A6        | Wen et al.           | 2019       | 8,75         | A29       | Uiphanit et al.       | 2025       | 6,5          |
| A7        | Monoharan et al.     | 2025       | 8,5          | A30       | Jennings et al.       | 2025       | 6,5          |
| A8        | Rahartomo et al.     | 2025       | 8,5          | A31       | Tu et al.             | 2025       | 6,25         |
| A9        | Sabo et al.          | 2023       | 8,5          | A32       | Tinubu et al.         | 2023       | 6,25         |
| A10       | Kletenik et al.      | 2021       | 8,5          | A33       | Azzahra et al.        | 2024       | 6,25         |
| A11       | Fu et al.            | 2025       | 8,25         | A34       | Scherb et al.         | 2023       | 6,25         |
| A12       | Sun et al.           | 2017       | 8,25         | A35       | Laucis et al.         | 2025       | 6,25         |
| A13       | Li et al.            | 2025       | 8,25         | A36       | Abreu et al.          | 2024       | 6            |
| A14       | Aladawy et al.       | 2018       | 8            | A37       | Khoja and Dintakurthy | 2025       | 5,75         |
| A15       | Videnovik et al.     | 2025       | 8            | A38       | Morocutti et al.      | 2025       | 5,75         |

|     |                     |      |      |     |                       |      |      |
|-----|---------------------|------|------|-----|-----------------------|------|------|
| A16 | Arachchilage et al. | 2016 | 7,75 | A39 | Sudha et al.          | 2023 | 5,5  |
| A17 | Matovu et al.       | 2022 | 7,75 | A40 | Abu-Amara et al.      | 2021 | 5,5  |
| A18 | Hale et al.         | 2015 | 7,75 | A41 | Löffler et al.        | 2021 | 5,5  |
| A19 | Laksono et al.      | 2025 | 7,5  | A42 | Kassner and Schönbohm | 2022 | 5,5  |
| A20 | Roepke et al.       | 2022 | 7,25 | A43 | Visoottiviseth et al. | 2018 | 5,5  |
| A21 | Jin et al.          | 2018 | 7    | A44 | Goeke et al.          | 2020 | 5    |
| A22 | Jaafar et al.       | 2024 | 7    | A45 | Abu-Amara et al.      | 2024 | 4,75 |
| A23 | Barth et al.        | 2024 | 7    | A46 | Salman et al.         | 2023 | 4,75 |

#### 4.1. Síntese dos Resultados

A partir da leitura e análise dos trabalhos identificados, pode-se responder às questões de pesquisa propostas neste estudo.

##### a) QP1 – Quais as técnicas de engenharia social apresentadas nos JDEs dos estudos?

A análise das técnicas abordadas pelos trabalhos sugere uma forte concentração em ensinar e conscientizar sobre os golpes do tipo *phishing* e suas variações. A1, A6, A8, A9, A10, A11, A14, A15, A18, A21, A23, A29, A31, A32 tratam do tipo mais comum da técnica, via e-mail. A4, A7, A22, A25, A27, A29, A30, A33, A34, A35, A36, A37, A39, A40, A41, A42, A43, A44, A45, A46 não deixam evidente quais outros tipos de golpe explorados, além dos identificados. Os estudos A1, A2, A14 e A17 destacam-se por abordar diversas técnicas no mesmo jogo, como *smishing*, *vishing*, *phishing* tradicional, *baiting* ou *tailgating*, criando circunstâncias mais específicas. As técnicas identificadas e os estudos que as abordam estão descritos no Quadro 4.

**Quadro 4. Golpes abordados nos estudos.**

| Técnica             | Estudo(s)                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------|
| Phishing (Genérico) | A4, A7, A22, A25, A27, A29, A30, A33, A34, A35, A36, A37, A39, A40, A41, A42, A43, A44, A45, A46 |
| Phishing por e-mail | A1, A6, A8, A9, A10, A11, A14, A15, A18, A21, A23, A29, A31, A32                                 |
| Phishing (URL/Link) | A3, A5, A9, A12, A16, A18, A20, A24, A26, A32, A38                                               |
| Smishing            | A1, A2, A8, A17, A31, A37                                                                        |
| Phishing (Site)     | A8, A18, A19, A32                                                                                |
| Spear Phishing      | A6, A17, A18, A37                                                                                |
| Vishing             | A1, A2, A14, A17                                                                                 |
| Tailgating          | A13, A14                                                                                         |

Para além dos golpes de ES, alguns estudos costumam abordar também práticas preventivas de segurança da informação. Em A10, A21 e A23, por exemplo, há desafios e simulações para avaliação e teste na criação de senhas seguras.

Por outro lado, muitos estudos acabam abordando temas que, por vezes, fogem da área proposta, o que pode dificultar a aprendizagem mediante a exposição de tantos termos e técnicas. Estudos como A30, A34, A35, A36, A39, A40, A41, A42, A43, A45 e A46 abordam phishing juntamente com outros temas de cibersegurança como firewall,

antivírus, malware, *cyberbulling*. Apesar do interesse em ensinar aspectos de engenharia social, esse conteúdo surge de forma superficial.

#### **b) QP2 – Quais as metodologias ou teorias de aprendizagem inseridas nos JDEs dos estudos?**

Ao analisar os estudos, pode-se identificar a correlação de abordagens pedagógicas e de ensino, estruturadas da seguinte forma:

**Cognitivas:** Os trabalhos de A5 e A6 utilizaram elementos ligados às teorias cognitivas. A5 fundamenta-se na teoria da carga cognitiva, tentando equilibrar o volume de informações apresentadas aos usuários para evitar sobrecarga mental. Já em A6, evidencia-se o princípio da elaboração, favorecendo a aprendizagem a partir da conexão de novos conhecimentos aos anteriores.

**Metodologias Ativas e Experienciais:** A21, A31 e A32 relatam princípios de aprendizagem ativa, ao possibilitar que os jogadores assumam o papel central da aprendizagem. A2 e A41 adotaram a ABP (Aprendizagem Baseada em Problemas), enquanto A11 e A35 a ABC (Aprendizagem Baseada em Cenários). Ambas promovem a resolução de desafios como forma de construção do conhecimento. Complementar a essas, A1 e A5 utilizam o princípio da reflexão, estimulando uma análise crítica nas decisões a serem tomadas pelos jogadores.

**Socioconstrutivistas:** Em A15, os pesquisadores adotaram a aprendizagem entre pares, que enfatiza a construção do conhecimento via colaboração. De modo semelhante, A5 e A11 propõem a teoria da aprendizagem social, na qual os participantes poderiam aprender diante de observação e modelagem de comportamentos. Já em A27, aparece o construtivismo, que reforça a ideia da participação ativa no processo de aprendizagem.

**Aprendizagem Baseada em Jogos:** A aprendizagem baseada em jogos (GBL) é nítida em estudos dessa natureza, pois 37% dos estudos (A2, A7, A8, A15, A18, A19, A20, A21, A23, A25, A29, A32, A33, A34, A35, A37 e A43) citam sua utilização nos jogos desenvolvidos. A GBL propõe-se a criar um ambiente educativo sem perder o componente lúdico e divertido, tornando a aprendizagem engajadora. Do mesmo modo, A25, A37, A40, A42, A45 e A46 adotam gamificação em seus jogos, com elementos como pontuação, desafios, recompensas e placar de liderança.

**Outras Abordagens:** Em A14 e A44 consta a teoria da inoculação, de modo a preparar os jogadores para reconhecer e resistir às tentativas de persuasão e manipulação. A22 utiliza um método específico da sua região, chamado “*Eight Ways of Indigenous Learning*”, baseado em formas tradicionais de ensino aos indígenas locais. Os trabalhos de A22 e A24 apresentam *frameworks* específicos para a conexão entre *design*, experiência e aprendizagem, sendo o *Experience, Dynamics and Artifacts* (EDP) e o *Design, Play and Experience* (DPE), respectivamente.

Ainda que haja uma variedade de teorias e metodologias, predominam abordagens como GBL, gamificação e metodologias ativas, mais alinhadas ao objetivo lúdico do jogo. Entretanto, há margem para teorias mais consolidadas, como as cognitivas, a ABP ou teoria da inoculação, que podem favorecer a retenção de conhecimento para o longo prazo.

A análise sugere que a escolha metodológica influencia diretamente a forma como os jogos são avaliados ou percebidos. Jogos com predominância de aspectos como GBL

e gamificação estão mais relacionados ao engajamento, usabilidade, diversão, motivação e satisfação ao jogar, geralmente percebidos com a aplicação de questionários pós-jogo. Por outro lado, abordagens pedagógicas (ABP, ABC) podem favorecer avaliações com foco na evolução do conhecimento, resolução de problemas e tomada de decisão, possibilitando análises mais profundas de aprendizagem.

Além disso, percebe-se que teorias socioconstrutivistas e a aprendizagem em pares são pouco adotadas, embora tenham potencial para o tema proposto, considerando que os golpes envolvem aspectos sociais, tomada de decisão e elementos de comunicação. Da mesma forma, a teoria da inoculação está diretamente ligada ao objetivo de conscientização, por preparar os jogadores para o reconhecimento das estratégias de ataque antes da efetiva exposição. Ainda assim, a baixa adoção sugere oportunidades de desenvolvimento de jogos e ferramentas com foco em uma mudança comportamental duradoura, para além da simples identificação de golpes durante as sessões dos jogos.

### c) QP3 – Qual a eficácia na aprendizagem e conscientização sobre golpes de engenharia social ao aplicar JDEs?

Ao analisar os métodos de avaliação estabelecidos nos artigos, constata-se um senso comum na aplicação de questionários pré-jogo e/ou pós-jogo. O propósito desses questionários é identificar a evolução ou não dos jogadores sobre a temática abordada, além de obter *feedback* sobre elementos do jogo apresentado e aspectos emocionais durante as sessões de uso, como diversão e entusiasmo. Também observa-se uma variação significativa no tamanho da quantidade de participantes entre os estudos.

**Quadro 5. Identificação dos métodos de avaliação e resultados obtidos**

| Avaliação                   | Artigos                                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pré-Jogo                    | A1, A3, A4, A6, A7, A8, A10, A12, A13, A14, A15, A16, A17, A19, A20, A23, A24, A25, A29, A30, A31, A33, A34, A37, A39, A40, A43, A45, A46                                                 |
| Pós-Jogo                    | A1, A3, A4, A5, A6, A7, A8, A10, A12, A13, A14, A15, A16, A17, A19, A20, A21, A23, A24, A25, A26, A27, A29, A30, A31, A32, A33, A34, A35, A36, A37, A39, A40, A41, A42, A43, A45, A46     |
| Entrevista, Observação etc. | A2, A9, A11, A18, A22, A28, A38, A44                                                                                                                                                      |
| Teste Longitudinal          | A3, A15, A20                                                                                                                                                                              |
| Grupo de Controle           | A1, A5, A6, A8, A9, A10, A15, A26, A30                                                                                                                                                    |
| Melhoria Percebida          | A1, A2, A3, A4, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A17, A19, A21, A22, A23, A24, A25, A28, A29, A30, A31, A32, A33, A34, A36, A37, A38, A39, A40, A41, A42, A43, A45, A46 |

Mediante os resultados, nota-se que a maioria (89%) dos jogos educativos apresentam melhorias no aspecto de aprendizagem e engajamento aos participantes. Os trabalhos A1, A3, A6, A8, A10, A20, A24, A29, A31 e A32 demonstraram evoluções significativas na capacidade de reconhecimento de ataques de *phishing* e correlatos, a partir dos questionários pré-jogo e pós-jogo. Em alguns casos, como A3 e A15, os ganhos

foram acompanhados de evidências de retenção do conhecimento em longo prazo, indicando que a aprendizagem promovida pelos jogos ultrapassou os efeitos imediatos da intervenção. Igualmente, A16, A25, A33, A36 e A46 relataram avanços em habilidades práticas de prevenção, identificação e resposta a ameaças, sugerindo que os jogos não apenas ampliaram o conhecimento dos jogadores, mas também contribuíram para a adoção de comportamentos mais seguros.

Apesar da predominância de resultados positivos, alguns estudos apresentaram evidências discretas ou com limitações relevantes. O trabalho A5 não identificou melhorias significativas na aprendizagem ou na detecção de URL *phishing* quando comparado aos métodos tradicionais comparados, concluindo que a simples adição de elementos de gamificação não garantem melhores resultados educacionais. Similarmente, A9 verificou melhorias em relação ao grupo de controle, porém sem ganhos adicionais significativos decorrentes da gamificação quando comparada à intervenção básica.

A alta adoção de avaliações com aplicação de questionários pré-jogo e pós-jogo fornece a identificação de ganhos imediatos na aprendizagem, mas não deixa clara a retenção desse aprendizado e a transferência para o uso no cotidiano. Portanto, embora a maioria dos estudos identifiquem melhorias relevantes na adoção dos JDEs, poucos realizaram testes longitudinais para avaliar o grau de retenção a longo prazo sobre os aspectos abordados. Do mesmo modo, há a carência de estudos com grupos de controle, utilizando intervenções básicas como apostilas, cartilhas e vídeos instrucionais. Logo, torna-se difícil estabelecer relações de causalidade entre resultados mais significativos ao adotar JDEs, sugerindo que, embora as evidências sejam positivas, ainda há a necessidade de delineamentos experimentais mais robustos para o fortalecimento de conclusões sobre o uso de jogos para o contexto de ensino sobre engenharia social.

#### 4.2. Ameaças à validade

Apesar dos resultados apresentados nesta pesquisa serem rastreáveis, constata-se ameaças internas na condução do método. A possibilidade de omissão de outros artigos relevantes, em decorrência da composição da *string* de busca, das bases de dados e técnicas adotadas. Pois, por exemplo, não foi executado *snowballing* para mapear evidências anteriores, a partir dos artigos selecionados. Os critérios de inclusão, exclusão e qualidade também podem apresentar viés de seleção, assim como a etapa das extrações, cabendo ajustes futuros para considerar maior rigor metodológico das publicações.

Como ameaças externas, a síntese limita-se aos estudos incluídos. Dessa forma, embora os achados sugiram eficácia na utilização dos JDEs para ensino e conscientização sobre golpes de ES, a utilização em outros ambientes ou áreas de estudo pode não representar mesma significância positiva ou negativa.

#### 5. Considerações

A partir da análise dos estudos, observa-se a preocupação e os esforços para capacitar os usuários em segurança cibernética, no âmbito de golpes digitais que utilizam técnicas de ES. A técnica de *phishing* e suas variações são as que mais destacam, mas deixam em aberto tantas outras.

Somado a isso, os estudos apresentam diversas visões sobre práticas educacionais de proporcionar o aumento da conscientização no tema investigado, mas predominam as metodologias de aprendizado baseado em jogos e gamificação enquanto elemento

estruturante dos jogos dos trabalhos. Diante dessa realidade, nota-se poucas aplicações de teorias como a da inoculação, que busca influenciar comportamento seguros para os aspectos de ES.

Os resultados dos estudos divergem, mas na maior parte da amostra analisada pela RSL, apresenta-se um elevado grau de satisfação relatada pelos participantes, nos aspectos de aprendizagem, imersão e foco. Esse cenário revela lacunas importantes: a aplicação de metodologias e teorias pedagógicas robustas; adoção de novos mecanismos para jogos, como a utilização de IA em ajustes automáticos das dificuldade do jogo [Schwanck et al. 2024] ou para adaptação de contexto, incluindo análise da evolução do que foi aprendido [Simão et al. 2025]; jogos com maior variedade de golpes (especialmente no contexto brasileiro, como golpes do PIX e variações); a baixa adesão de grupos de controle para melhor análise entre participantes que utilizaram os jogos em detrimento a outros tipos de intervenção; a variedade dos perfis analisados, com estudos apresentando uma quantidade de participantes aquém da necessária para análises mais criteriosas; e finalmente a necessidade de um método de avaliação de jogos apropriado como o questionário MEEGA+, identificado por [Santana et al. 2025] como melhorias para o seu próprio jogo.

Esta revisão fortalece o interesse de adotar JDEs como ferramenta de ensino e conscientização sobre golpes digitais, que sejam apoiados por técnicas de ES. Professores e alunos se beneficiam dos jogos como ferramenta pedagógica por meio das teorias de aprendizagem inseridas e os elementos de gamificação, facilitando o ensino, fortalecendo o engajamento e promovendo a discussão e solução de problemas reais em ambientes seguros.

Para desenvolvedores, os achados indicam que apenas elementos de gamificação, dificuldade aprimorada e motivação podem não ser suficientes para melhoria de resultados educacionais, sendo mais efetivos quando envoltos por teorias da aprendizagem que relacionem os aspectos sociais, organização progressiva dos conteúdos, reflexões autênticas e o desenvolvimento de comportamentos preventivos. Por fim, para pesquisadores, permanece a necessidade de estudos comparativos com diferentes intervenções, investigando princípios educacionais mais relevantes ao conhecimento sobre golpes de engenharia social e avaliações longitudinais.

O próximo passo desta pesquisa é o desenvolvimento de um protótipo de JDE sobre golpes digitais do cenário brasileiro para estudantes do ensino médio.

### **Disponibilidade de Artefatos**

As informações de extração dos artigos incluídos no corpus final deste trabalho, assim como as pontuações dos *scores* de qualidade e o protocolo da revisão estão disponíveis em: <https://osf.io/j4dxy/overview>.

### **Declaração sobre uso de Inteligência Artificial**

Os autores deste trabalho informam o Uso de Ferramentas de Inteligência Artificial (IA) Generativa, descrito a seguir.

Durante o desenvolvimento, as seguintes ferramentas foram utilizadas de maneira a apoiar a seleção e análise de estudos, com a supervisão de pelo menos um dos revisores nos processos de triagem e extração de dados:

**NotebookLM** - a ferramenta, sem versão específica, é uma IA difundida no meio acadêmico, por possibilitar a análise de conteúdos escritos ou de arquivos (pdf) como fontes de pesquisa. Evita-se a busca pela internet, diminui-se o risco de alucinações e recuperação ou extração de conteúdo de fontes inexistentes, possibilitando a localização dos resultados encontrados dentro de cada estudo analisado.

**ChatGPT** - a ferramenta da OpenAI, em sua versão 5.5, foi utilizada nos processos de: revisão de linguagem, como sugestão de sinônimos, indicativo de palavras erradas; tradução; sugestões metodológicas, como os principais itens de uma RSL; análises pontuais; erros de referências.

Os autores atestam que a utilização das ferramentas foi exclusivamente para os propósitos relatados.

Em conformidade com os princípios de ética, declara-se que as informações são verdadeiras e um breve relatório de uso das IAs está disponível em: <https://osf.io/j4dxy/overview>.

## Referências

- Abdullah, Z. B., Dahlan, N. B. M., Dahlan, A. B., Irfan Bin, A. F. and Arifin, A. S. (2023). Cybersecurity Awareness on Personal Data Protection Using Game-Based Learning. *Information Management and Business Review*, v. 15, n. 3(I), p. 497–503.
- ABIN, Associação Brasileira de Inteligência (2021). Engenharia Social: Guia para Proteção de Conhecimentos Sensíveis. <https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis>. [accessed on April 05].
- Garcia, A. V. and Parra, D. R. (2021). Phishing Video Game to Validate the Principles of Persuasion in University Students. In *Proceedings of the 27th Americas Conference on Information Systems (AMCIS 2021)*, Paper 1708. Association for Information Systems. <https://hdl.handle.net/20.500.12724/16130>. [accessed on Apr 02].
- Abreu, J. M. De, Miani, R. S. and Nomura, S. (2024). Encrypta: A Missão da Liga dos Robôs – Um Jogo Educacional para Aprendizagem em Cibersegurança. In *Anais do XXIII Simpósio Brasileiro de Jogos e Entretenimento Digital (SBGames 2024)*. Sociedade Brasileira de Computação. <https://sol.sbc.org.br/index.php/sbgames/article/view/32401>. DOI: <https://doi.org/10.5753/sbgames.2024.240133>
- Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M. and Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, v. 13, n. 6, p. 2371–2380.
- Abu-Amara, F., Hosani, R. A., Tamimi, H. A. and Hamdi, B. A. (2024). Spreading cybersecurity awareness via gamification: zero-day game. *International Journal of Information Technology*, v. 16, n. 5, p. 2945–2953.
- Aladawy, D., Beckers, K. and Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In Furnell, S., Mouratidis, H. and Pernul, G. (Eds.). *Trust, Privacy and Security in Digital Business*. Cham: Springer International Publishing, v. 11033, p. 103–118.

- Alma'ariz, S., Hadiprakoso, R. B., Girinoto and Qomariasih, N. (2022). Soceng Warriors: Game-Based Learning to Increase Security Awareness Against Social Engineering Attacks. In 2022 IEEE 8th Information Technology International Seminar (ITIS). IEEE. DOI: 10.1109/ITIS57155.2022.10009041.
- Alves, L. and Coutinho, I. de J. (2016). Jogos digitais e aprendizagem: Fundamentos para uma prática baseada em evidências. Papirus Editora.
- Arachchilage, N. A. G., Love, S. and Beznosov, K. (2016). Phishing Threat Avoidance Behaviour: An Empirical Investigation. *Computers in Human Behavior*, v. 60, p. 185–197.
- Azzahra, F., Qomariasih, N., Kabetta, H., et al. (2024). SocengGo: Social Engineering Educational Application Based on Attack-Defense Multiplayer Card Game. In 2024 10th International Conference on Education and Technology (ICET). IEEE. DOI: 10.1109/ICET64717.2024.10778458.
- Baars, H., Hintzbergen, K., Hintzbergen, J. and Smulders, A. (7). Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. BRASPORT.
- Baiomy, A., Mostafa, M. and Youssif, A. (2019). Anti-Phishing Game Framework to Educate Arabic Users: Avoidance of URLs Phishing Attacks. *Indian Journal of Science and Technology*, v. 12, n. 44, p. 01–10.
- Barth, V., Wanner, T., Gelderie, M. and Schüle, J. (2024). Is Attacking More Fun than Defending? Observations from Developing and Evaluating Practical Game-Based Learning. *Procedia Computer Science*, v. 246, p. 3148–3157.
- Brasil (2022). Base Nacional Comum Curricular: Educação é a Base. Ministério da Educação. <https://basenacionalcomum.mec.gov.br/>. [accessed on May 20].
- Coqui, Lucas; Maia, Vitor; and Castro, Diego (2025). Phishing Quiz: Um Jogo Educacional para Conscientização e Prevenção de Ataques Cibernéticos. In: TRILHA DE EDUCAÇÃO – ARTIGOS CURTOS - SIMPÓSIO BRASILEIRO DE JOGOS E ENTRETENIMENTO DIGITAL (SBGAMES), 14, 2025, Salvador/BA. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2025. p. 139-145. DOI: [https://doi.org/10.5753/sbgames\\_estendido.2025.10095](https://doi.org/10.5753/sbgames_estendido.2025.10095).
- DataSenado, Instituto de Pesquisa (2024). Panorama Político 2024: Apostas esportivas, golpes digitais e endividamento. Senado Federal. Instituto de Pesquisa DataSenado. [https://www12.senado.leg.br/noticias/arquivos/2024/09/30/relatorio\\_apostasesportiva-s-golpesdigitais-endividamento-1.pdf](https://www12.senado.leg.br/noticias/arquivos/2024/09/30/relatorio_apostasesportiva-s-golpesdigitais-endividamento-1.pdf). [accessed on April 04].
- FBSP, Fórum Brasileiro de Segurança Pública (2024). 18º Anuário Brasileiro de Segurança Pública. São Paulo: Fórum Brasileiro de Segurança Pública. ISSN: 1983-7364. <https://publicacoes.forumseguranca.org.br/handle/123456789/253>. [accessed on April 05].
- Ferreira, A. L. H., Sales, A. B. D., Ferreira, A. E. V. and Palmeira, E. G. Q. (2024). Características dos jogos sérios Anti-Phishing como ferramenta de ensino: uma revisão sistemática. *RENOTE*, v. 22, n. 1, p. 340–350.
- Fu, J., Lu, Y., Yang, Z., Nah, F. and Lc, R. (2025). Cracking Aegis: An Adversarial LLM-Based Game for Raising Awareness of Vulnerabilities in Privacy Protection. In

- Proceedings of the 2025 ACM Designing Interactive Systems Conference. ACM. DOI: <https://doi.org/10.1145/3715336.3735812>.
- Goeke, L., Quintanar, A., Beckers, K. and Pape, S. (2020). PROTECT: An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. In Fournaris, A. P., Athanatos, M., Lampropoulos, K., et al. (Eds.). Computer Security. Cham: Springer International Publishing, v. 11981, p. 156–171.
- Hale, M. L., Gamble, R. F. and Gamble, P. (2015). CyberPhishing: A Game-Based Platform for Phishing Awareness Testing. In 2015 48th Hawaii International Conference on System Sciences. IEEE. DOI: 10.1109/HICSS.2015.670.
- Jaafar, N. H., Ismail, Z., Zamani, N. D., Abd Rahman, M. and Mokhtar, R. (2024). Empowering Indigenous Pupils: Enhancing Cyber Security Awareness Through Interactive Gaming Experiences. In Proceedings of the 2024 10th International Conference on Frontiers of Educational Technologies. ACM. DOI: <https://doi.org/10.1145/3678392.3678397>.
- Jennings, C., Pham, S. and Dupuis, M. J. (2025). Engagement, Usability, and Learning in Narrative-Driven Cybersecurity Awareness Games. In 2025 IEEE 16th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). IEEE. DOI: 10.1109/UEMCON67449.2025.11267542.
- Jin, G., Tu, M., Kim, T.-H., Heffron, J. and White, J. (2018). Game-Based Cybersecurity Training for High School Students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education. ACM. DOI: <https://doi.org/10.1145/3159450.3159591>.
- Kassner, L. and Schönbohm, A. (2022). A Serious Game to Improve Phishing Awareness. In Kiili, K., Kickmeier-Rust, M. D., De Rosa, F., et al. (Eds.). Games and Learning Alliance. Cham: Springer International Publishing, v. 13647, p. 109–117.
- Kävrestad, J., Hagberg, A., Nohlberg, M., et al. (2022). Evaluation of Contextual and Game-Based Training for Phishing Detection. Future Internet, v. 14, n. 4, p. 104.
- Keller, T., Guggemos, J. and Warwas, J. (2025). Digital Educational Escape Rooms as a Novel Approach to Cybersecurity Education: An Empirical Study on Learner Perceptions of Usefulness and Usability. Computers in Human Behavior Reports, v. 20, p. 100785.
- Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In: Technical report, Ver. 2.3 EBSE Technical Report. EBSE.
- Kletenik, D., Butbul, A., Chan, D., Kwok, D. and LaSpina, M. (2021). Game On: Teaching Cybersecurity to Novices Through the Use of a Serious Game. Journal of Computing Sciences in Colleges, v. 36, n. 8, p. 11–21. DOI: <https://dl.acm.org/doi/10.5555/3470135.3470136>.
- Laksono, R. D., Sussolaikah, K., Din, M. B. M., Mansor, S. and Dawam, S. R. M. (2025). Assessment of Cyber Security Awareness Using Developed Game From H5P on Users Aged at Elementary and First Secondary School in Madiun City. Journal of Applied Engineering and Technological Science, v. 7, n. 1, p. 539–549. DOI: <https://doi.org/10.37385/jaets.v7i1.6705>.

- Laucis, E., Roponena, E., Brilingaite, A., Bukauskas, L., Citskovska, E. and Pirta, R. (2025). Sea Safe: Designing a Serious Game to Develop Awareness in Maritime Cybersecurity. In 2025 66th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS 2025). IEEE, p. 106–111. Available at: <https://doi.org/10.1109/ITMS67030.2025.11236514>.
- Li, T., Dong, F. and Wen, C. (2025). The Security Awareness Adventure: A Serious Game for Security Awareness Training Utilizing a State Transition System and a Probabilistic Model. *Computers & Security*, v. 156, p. 104500.
- Löffler, E., Schneider, B., Zanwar, T. and Asprion, P. M. (2021). CySecEscape 2.0: A Virtual Escape Room to Raise Cybersecurity Awareness. *International Journal of Serious Games*, v. 8, n. 1, p. 59–70.
- Lopes, A., Mamede, H. S., Reis, L. and Santos, A. (2024). Common Techniques, Success Attack Factors and Obstacles to Social Engineering: A Systematic Literature Review. *Emerging Science Journal*, v. 8, n. 2, p. 761–794.
- Monoharan, A., Sriskantharajah, A., Herath, H. M. K. K. M. B., Guruge, L. G. P. K. and Yasakethu, S. L. P. (2025). MetaHuman Based Phishing Attacks in the Metaverse Realm: Awareness for Cyber Security Education. *Education and Information Technologies*, v. 30, n. 9, p. 12939–12965.
- Maqsood, S. and Chiasson, S. (2021). Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security*, v. 24, n. 4, p. 1–37.
- Matovu, R., Nwokeji, J. C., Holmes, T. and Rahman, T. (2022). Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges. In 2022 IEEE Frontiers in Education Conference (FIE). IEEE. DOI: 10.1109/FIE56618.2022.9962519.
- Moran, José. (2015). Mudando a educação com metodologias ativas. *Coleção mídias contemporâneas. Convergências midiáticas, educação e cidadania: aproximações jovens*, v. 2, n. 1, p. 15-33.
- Morocutti, L., Pasquali, D., Bencetti, S., et al. (2025). Caught in the Net: An Explorative HCI Study on Human Behavioral Vulnerabilities Against Phishing. In Proceedings of the 16th Biannual Conference of the Italian SIGCHI Chapter. ACM. DOI: <https://doi.org/10.1145/3750069.3750152>.
- Neves, L. M. and Pereira, N. de L. B. (2020). Ransomware e phishing durante a pandemia covid-19 (coronavírus). [https://ric.cps.sp.gov.br/bitstream/123456789/10438/1/2S2020\\_LucasMirandaNeves\\_OD01018.pdf](https://ric.cps.sp.gov.br/bitstream/123456789/10438/1/2S2020_LucasMirandaNeves_OD01018.pdf). [accessed on April 11]
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., et al. (2022). A declaração PRISMA 2020: diretriz atualizada para relatar revisões sistemáticas. *Revista Panamericana de Salud Pública*, v. 46, p. 1.
- Panga, R. C. T., Marwa, J. and Ndibwile, J. D. (2022). A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania. *Journal of Cybersecurity and Privacy*, v. 2, n. 3, p. 466–489.
- Priya, P. M. and Ranganathan, A. (2022). Cyber Awareness Learning Imitation Environment (CALIE): A Card Game to provide Cyber Security Awareness for

- Various Group of Practitioners. International Journal of Advanced Networking and Applications, v. 14, n. 02, p. 5334–5341.
- Rahartomo, A., Ghaleb, A. T. A. and Ghafari, M. (2025). Phishing Awareness via Game-Based Learning. In 2025 IEEE/ACM 37th International Conference on Software Engineering Education and Training (CSEET&T). IEEE. DOI: 10.1109/CSEET66350.2025.00036.
- Roepke, R., Drury, V., Meyer, U. and Schroeder, U. (2022). Better the Phish You Know: Evaluating Personalization in Anti-Phishing Learning Games. In Proceedings of the 14th International Conference on Computer Supported Education. SCITEPRESS – Science and Technology Publications. DOI: 10.5220/0011042100003182.
- Roepke, R., Drury, V., Meyer, U. and Schroeder, U. (2022). Exploring and Evaluating Different Game Mechanics for Anti-Phishing Learning Games. International Journal of Serious Games, v. 9, n. 3, p. 23–41.
- Sabo, K. E., Black, J. and Sarno, D. M. (2023). Developing IMPAWSTER: Improving Meaningful Phishing Awareness With Simulated Training and Email Roleplay. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, v. 67, n. 1, p. 1665–1670.
- Salman, O. H., Alawida, M., Abu Hazeem, R. M., Sameer Zeyadeh, M. and Alameri, M. R. (2023). CyberSafe: A Gamified Cyber Security Training Method. In 2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE). IEEE. DOI: 10.1109/ICECCE61019.2023.10442243.
- Santana, R. M. S., Rizzi, C. B. and Boscarioli, C. (24 nov 2025). Uso da Taxonomia de Bloom Revisada em um Jogo de RPG Educacional sobre Conceitos Introdutórios de Programação. In *Anais do XXXVI Simpósio Brasileiro de Informática na Educação (SBIE 2025)*. Sociedade Brasileira de Computação - SBC. <https://sol.sbc.org.br/index.php/sbie/article/view/38480>, [accessed on May 20].
- Scherb, C., Heitz, L. B., Grimberg, F., Grieder, H. and Maurer, M. (2023). A Cyber Attack Simulation for Teaching Cybersecurity. EPiC Series in Computing, v. 93, p. 129–140. DOI: 10.29007/dkdw.
- Schwanck, S. B., Cipriano, L. W., Pozzebon, E. and Bilessimo, S. M. S. (4 nov 2024). A utilização da Inteligência Artificial para adaptar o nível de dificuldade e manter os alunos engajados na aprendizagem com jogos. In *Anais do XXXV Simpósio Brasileiro de Informática na Educação (SBIE 2024)*. Sociedade Brasileira de Computação - SBC. <https://sol.sbc.org.br/index.php/sbie/article/view/31272>, [accessed on May 20].
- Simão, J. P. S., Machado, L. S. R., Silva, J. B. D. and Behar, P. A. (24 nov 2025). Inteligência Artificial Agêntica na Educação: Um Agente Conversacional para Construção de Competências na Educação Básica. In *Anais do XXXVI Simpósio Brasileiro de Informática na Educação (SBIE 2025)*. Sociedade Brasileira de Computação - SBC. <https://sol.sbc.org.br/index.php/sbie/article/view/38434>, [accessed on Jul 20].
- Sousa, M. D., Ferreira, F. D. C., Silva, J. D. S., Silva, M. A. D. and Oliveira, R. F. D. (2024). Caminhos da Educação Digital: Integrando Tecnologias, Cidadania e Inovação. Revista Amor Mundi, v. 5, n. 2, p. 173–181.

- Souza, N. C., Ferreira, A. L. H., Palmeira, G. Q., Ferreira, A. E. V., and Sales, A. B. de. (2025). O Uso de Jogos Sérios para o Ensino de Higiene Cibernética: Uma Revisão Sistemática. *RENTE*, v. 24, n. 2, p. 382–393.
- Sudha, S. S., Aguayo, G. C., Angulo, A. R., et al. (2023). Changes in High-School Student Attitude and Perception Towards Cybersecurity Through the Use of an Interactive Animated Visualization Framework. In *2023 IEEE Global Engineering Education Conference (EDUCON)*. IEEE. DOI: 10.1109/EDUCON54358.2023.10125195.
- Sun, J. C.-Y., Kuo, C.-Y., Hou, H.-T. and Lin, Y.-Y. (2017). Exploring Learners’ Sequential Behavioral Patterns, Flow Experience, and Learning Performance in an Anti-Phishing Educational Game. *Educational Technology & Society*, v. 20, n. 1, p. 45–60.
- Tinubu, C. O., Falana, O. J., Oluwumi, E. O., Sodiya, A. S. and Rufai, S. A. (3 jul 2023). PHISHGEM: a mobile game-based learning for phishing awareness. *Journal of Cyber Security Technology*, v. 7, n. 3, p. 134–153.
- Tu, W., Lim, B., Ong, V., et al. (2025). Narrative-Based Interactive Learning for Scam Prevention: Rich Within Reach. In *Proceedings of the 17th International Conference on Computer Supported Education*. SCITEPRESS – Science and Technology Publications. DOI: <https://doi.org/10.5220/0013436100003932>.
- Uiphanit, T., Chutosri, T., Wattanaprapa, N., et al. (2025). Phishing Awareness through Game-Based Learning: A Mobile-Responsive Web Application for Middle School Learners. *International Journal of Interactive Mobile Technologies (iJIM)*, v. 19, n. 12, p. 55–67.
- Videnovik, M., Trajkovik, V., Vold, T., et al. (2025). Using Peer-Learning and Game-Based Instruction for Achieving Long-Lasting Knowledge of Cybersecurity in Primary Schools. *IEEE Access*, v. 13, p. 11679–11688.
- Yasin, A., Fatima, R., Wen, L., JiangBin, Z. and Niazi, M. (2025). What goes wrong during phishing education? A probe into a game-based assessment with unfavorable results. *Entertainment Computing*, v. 52, p. 100815.
- Visoottiviseth, V., Sainont, R., Boonnak, T. and Thammakulkrajang, V. (2018). POMECA: Security Game for Building Security Awareness. In *2018 Seventh ICT International Student Project Conference (ICT-ISPC)*. IEEE. DOI: 10.1109/ICT-ISPC.2018.8523965.
- Wen, Z. A., Lin, Z., Chen, R. and Andersen, E. (2019). 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*. ACM. DOI: <https://doi.org/10.1145/3290605.3300338>.
- Wibawa, D. A. S., Setiawan, H. and Girinoto (2022). Anti-Phishing Game Framework Based on Extended Design Play Experience (DPE) Framework as an Educational Media. In *2022 7th International Workshop on Big Data and Information Security (IWBIS)*. IEEE. DOI: 10.1109/IWBIS56557.2022.9924935.
- Zolkifly, I. A., Suaib, N. M. and Tanalol, S. H. (2025). Game Mechanics for Technical Education: Framework and Evaluation in Cybersecurity Contexts. In *2025 IEEE*

International Conference on Computing (ICOCO). IEEE. DOI:  
10.1109/ICOCO67189.2025.11334079.