Phishing War: Gamificação e inteligência artificial no combate a *phishing*

GUSTAVO DE OLIVEIRA GOMES
JOÃO EMMANUEL D ALKMIN NEVES

Resumo

Este artigo aborda o desenvolvimento de um protótipo de jogo educativo, denominado *Phishing War*, para capacitação para prevenção de ataques de *phishing*, utilizando gamificação e Inteligência Artificial como estratégias inovadoras. O objetivo é oferecer uma alternativa mais eficaz aos métodos tradicionais de treinamento em Segurança da Informação, proporcionando uma experiência interativa e engajadora. A metodologia envolve uma revisão bibliográfica em fontes como Google Acadêmico e SciELO, seguida da criação do jogo, cujas mecânicas e design foram desenvolvidos com auxílio de ferramentas de Inteligência Artificial. Os resultados esperados indicam que a gamificação, apoiada por Inteligência Artificial, podem tornar o treinamento mais dinâmico, reforçando a conscientização dos colaboradores e ampliando a resiliência das organizações contra ciberameaças. Conclui-se que o avanço das ameaças cibernéticas exige inovação contínua nos métodos de treinamento, sendo a gamificação, como a desenvolvida neste estudo, uma abordagem promissora para capacitar futuras gerações na prevenção de ataques no ambiente corporativo.
Palavras-chave: *Gamificação; Treinamento Corporativo; Segurança da Informação; Ciberameaça; Phishing.*

Phishing War: Gamification and artificial intelligence in combating phishing

Abstract

This article discusses the development of a prototype educational game, called Phishing War, for training in the prevention of phishing attacks, using gamification and Artificial Intelligence as innovative strategies. The objective is to offer a more effective alternative to traditional Information Security training methods, providing an interactive and engaging experience. The methodology involves a literature review in sources such as Google Scholar and SciELO, followed by the creation of the game, whose mechanics and design were developed with the aid of Artificial Intelligence tools. The expected results indicate that gamification, supported by Artificial Intelligence, can make training more dynamic, reinforcing employee awareness and increasing the resilience of organizations against cyber threats. It is concluded that the advancement of cyber threats requires continuous innovation in training methods, with gamification, as developed in this study, being a promising approach to empower future generations in the prevention of attacks in the corporate environment.

Keywords: *Gamification; Corporate Training; Information Security; Cyber Threat; Phishing.*

---

1 INTRODUÇÃO

No atual cenário do mercado de jogos digitais corporativos, evidencia-se uma lacuna significativa destinada às empresas de Segurança da Informação, caracterizada pela escassez de opções disponíveis. Esta circunstância observa a urgência e a relevância de investigações no campo da pesquisa de novas metodologias e tecnologias educacionais voltadas para a área de Segurança da Informação, visando lidar com as necessidades emergentes do mercado e promover uma abordagem mais dinâmica e eficaz no treinamento e capacitação dos profissionais dessa área.

Considerando o avanço da Inteligência Artificial em diversos setores, incluindo os mercados de games, surge a necessidade de uma abordagem inovadora para o treinamento nas empresas. Nesse contexto, surge uma hipótese: a criação de um jogo físico dinâmico e lúdico,

com o auxílio da Inteligência Artificial, que possa tornar o aprendizado mais eficaz, concreto e visível para os colaboradores.

Portanto, o objetivo geral é desenvolver um jogo usando conceitos de gamificação e simulação para ensinar boas práticas de Segurança da Informação em ataques *phishing* (fraude digital), utilizando ferramentas de Inteligência Artificial para tornar o desenvolvimento mais dinâmico, tangível e personalizado às empresas e gerando engajamento de seus funcionários.

Essa proposta se justifica pela necessidade de superar as limitações dos métodos tradicionais de treinamento, oferecendo uma abordagem mais engajadora e eficiente para capacitar os funcionários, especialmente diante das demandas e desafios crescentes enfrentados pelas empresas na era digital.

2 REFERENCIAL TEÓRICO

Esta seção será dividida em três partes: Inteligência Artificial e Inteligência Artificial Cognitiva, Gamificação e Simulação na Capacitação Corporativa e Treinamento em Segurança da Informação e *phishing*.

Na primeira parte, serão abordados os conceitos e aplicações da Inteligência Artificial e Cognitiva, focando em como essas tecnologias podem otimizar processos organizacionais. Na segunda parte serão tratados da gamificação e a simulação como métodos inovadores para aumentar o engajamento e facilitar o aprendizado prático no ambiente corporativo. Por fim, a seção sobre Segurança da Informação e *phishing* destacará a importância da proteção de dados e sistemas, apresentando os diferentes tipos de *phishing* e a necessidade de capacitar colaboradores para reconhecer e lidar com essas ameaças.

2.1 Inteligência Artificial e Inteligência Artificial Cognitiva

A Inteligência Artificial (IA) é um campo multidisciplinar da ciência da computação que se dedica à criação de sistemas e algoritmos capazes de simular comportamentos humanos, como a percepção, o raciocínio e a resolução de problemas complexos (Araújo; Bastos; Silva, 2019).

Compreender a IA é essencial, uma vez que sua evolução tem impacto significativo em diversas áreas, desde o ambiente corporativo até o campo educacional. À medida que a tecnologia avança, a IA tem sido amplamente integrada em processos que vão desde a automatização até o suporte à tomada de decisões estratégicas (Neves, 2024). No entanto, a crescente difusão da IA na sociedade também gerou um fenômeno de interpretação variável do termo, o que ressalta a necessidade de uma delimitação clara para que se possa conduzir estudos e discussões de forma precisa.

De acordo com Ludemir (2021), a IA pode ser classificada em três categorias principais, cada uma com suas características e aplicações específicas:

- IA Focada (ou Fraca): Esta categoria abrange sistemas que são projetados para resolver problemas específicos, como algoritmos de recomendação ou sistemas de reconhecimento facial. Apesar de sua capacidade de executar tarefas complexas, a atuação da IA Focada é restrita ao domínio para o qual foi programada, limitando sua aplicação a contextos específicos.
- IA Generalizada (ou Forte): Esta categoria refere-se a sistemas que possuem capacidades amplas, que se aproximam das habilidades humanas em uma variedade de tarefas. A IA Generalizada é especialmente relevante em áreas que envolvem aprendizado adaptativo, como a Visão Computacional, onde algoritmos podem aprender e se aprimorar continuamente em resposta a novas informações e contextos.

- IA Superinteligente: Este conceito representa uma forma hipotética de IA que ultrapassaria as capacidades humanas em praticamente todas as áreas de atuação. Embora seja um conceito intrigante, atualmente não existem sistemas que possam ser classificados como IA Superinteligente, e sua viabilidade futura permanece uma questão em aberto na pesquisa em IA.

O progresso no desenvolvimento da IA tem sido amplamente impulsionado pelas inovações nas técnicas de Aprendizado de Máquina (AM). Este campo específico da IA permite que os algoritmos processem dados de forma eficaz, utilizando diferentes abordagens, como o aprendizado supervisionado, não supervisionado e por reforço (Neves *et al*., 2023).

No aprendizado supervisionado, os sistemas são treinados com dados rotulados, onde cada entrada é acompanhada pela resposta desejada. Em contraste, no aprendizado não supervisionado, os algoritmos analisam dados que não possuem rótulos, identificando padrões e estruturas subjacentes sem a orientação de um conjunto de respostas. O aprendizado por reforço, por sua vez, envolve um sistema que aprende a partir de recompensas e punições, melhorando seu desempenho ao longo do tempo com base no feedback recebido (Ludemir, 2021).

A Inteligência Artificial Cognitiva (IAC) representa uma ampliação do conceito tradicional de IA, ao se concentrar em simular os processos de raciocínio humano, permitindo que sistemas computacionais resolvam problemas e tomem decisões de maneira mais autônoma e flexível (Pires; Neves, 2023).

Este campo é inspirado pela psicologia cognitiva e visa modelar o raciocínio humano em sistemas que são capazes de interpretar e processar informações em contextos variados. Essa habilidade de adaptação sem a necessidade de intervenção humana direta é uma das principais inovações que a IAC traz para o desenvolvimento tecnológico (Araújo; Bastos; Silva, 2019).

A IAC tem encontrado um campo fértil de aplicação em diversas áreas, especialmente em soluções voltadas para cibersegurança e educação. Ao facilitar o desenvolvimento de simuladores que imitam cenários reais de ameaças, a IAC proporciona uma experiência de aprendizado prática e relevante, contribuindo para a formação de profissionais mais bem preparados para lidar com os desafios contemporâneos. Assim, a integração da IAC em programas de treinamento e desenvolvimento pode resultar em um aprimoramento significativo das capacidades cognitivas e operacionais dos usuários, promovendo um ambiente de aprendizado dinâmico e envolvente (Santos; Neves, 2023).

2.2 Treinamento em Segurança da Informação e *phishing*

A Segurança da Informação (SI) emerge como uma área de crescente relevância no contexto corporativo contemporâneo, especialmente diante da digitalização e da interconectividade que caracterizam o ambiente de negócios atual. A SI é essencial para a proteção de dados sensíveis, a salvaguarda da privacidade de usuários e clientes, e a manutenção da integridade das operações organizacionais (Moura; D'Alkmin Neves, 2021).

Como afirmado por Rezende (2022), a prática da SI envolve a mitigação de ameaças cibernéticas, que representam riscos significativos à confiabilidade das informações. Esses riscos podem se manifestar em diversas formas, incluindo acesso não autorizado, vazamento de dados e ataques cibernéticos, comprometendo a continuidade dos negócios e a reputação das organizações.

Nesse cenário, o treinamento dos colaboradores desempenha um papel crucial na formação de uma cultura de segurança dentro da organização (Campos; Britto, 2020). A maioria das vulnerabilidades em sistemas de informação pode ser atribuída, direta ou indiretamente, ao

fator humano. Em particular, comportamentos inadequados ou desinformados de funcionários podem abrir brechas para ataques maliciosos, como os de *phishing* (Tonezer *et al*., 2024).

Esses ataques são especialmente preocupantes, uma vez que utilizam técnicas de engenharia social para enganar as vítimas, explorando a confiança e a curiosidade humana. Portanto, capacitar os colaboradores para reconhecer e responder adequadamente a tais ameaças é uma medida essencial para reduzir os riscos associados à SI (Pedro *et al*., 2024).

O *phishing* pode ser definido como uma técnica de fraude digital que visa enganar indivíduos para que revelem informações sensíveis, como credenciais de login, dados bancários e informações pessoais. O modus operandi dos ataques de *phishing* frequentemente envolve o uso de e-mails fraudulentos ou sites falsificados que imitam a aparência de instituições legítimas, levando as vítimas a acreditarem que estão interagindo com uma fonte confiável (Rezende, 2022).

Este tipo de ataque não apenas compromete dados pessoais, mas também pode ter repercussões devastadoras para as organizações, que podem enfrentar perdas financeiras, danos à reputação e complicações legais decorrentes de vazamentos de dados (Barbosa *et al*., 2023).

Rodrigues e Bastos (2018) oferecem uma classificação abrangente dos ataques de *phishing*, destacando diversas modalidades que refletem a sofisticação e a especialização dos cibercriminosos. Essa classificação inclui:

- *Phishing* tradicional: Este tipo de ataque consiste em mensagens genéricas que contêm links ou anexos maliciosos. Os criminosos frequentemente enviam e-mails em massa na esperança de que um pequeno número de destinatários caia na armadilha.
- *Spear phishing*: Diferentemente do *phishing* tradicional, o *spear phishing* é altamente personalizado e direcionado a indivíduos ou organizações específicas. Os atacantes realizam pesquisas para coletar informações que possam aumentar a credibilidade da mensagem, tornando-a mais convincente.
- *Whaling*: Essa modalidade é uma forma de *spear phishing*, mas seu alvo são altos executivos ou pessoas de influência dentro de uma organização. Os ataques *de whaling* são particularmente perigosos, pois podem comprometer informações estratégicas e de alto valor.
- *Smishing* e *Vishing*: Estas formas de *phishing* utilizam mensagens de texto (*smishing*) e chamadas telefônicas (*vishing*) para tentar enganar as vítimas. Tanto o *smishing* quanto o *vishing* exploram a natureza imediata e pessoal das comunicações móveis, o que pode dificultar a detecção de fraudes.

Essas táticas de *phishing* evoluem rapidamente, adaptando-se às novas tecnologias e aos padrões de comportamento dos usuários, o que torna a conscientização e o treinamento contínuos aspectos cruciais na proteção contra esses ataques (Damasceno *et al*., 2021).

As organizações devem investir em programas de capacitação que não apenas informem os colaboradores sobre os riscos associados ao *phishing*, mas que também desenvolvam suas habilidades para identificar e responder a tentativas de ataque. Dessa forma, o treinamento em SI não se limita apenas ao conhecimento teórico, mas se estende à aplicação prática, promovendo uma cultura organizacional resiliente diante das ameaças cibernéticas contemporâneas (Campos; Britto, 2020).

2.3 Gamificação e Simulação na Capacitação Corporativa

A gamificação se define como a aplicação de elementos e técnicas de design de jogos em contextos não lúdicos, visando promover a motivação, o engajamento e a facilitação do aprendizado Alves (2024). Essa abordagem inovadora surgiu a partir da introdução de estratégias lúdicas, inicialmente nos campos do marketing e da educação, e rapidamente se consolidou como

uma ferramenta valiosa no ambiente corporativo, especialmente em processos de capacitação e desenvolvimento de habilidades (Silva, 2018).

Segundo (Rodrigues, 2023), embora a prática de incorporar elementos de jogos tenha raízes que remontam a 1912, foi somente em 2003 que o conceito de gamificação começou a ser amplamente reconhecido e adotado em ambientes de ensino e treinamento profissional.

No contexto corporativo, a gamificação se revela como uma alternativa altamente eficaz para aprimorar o aprendizado, em particular na área de SI. A capacidade de criar cenários simulados permite que os colaboradores enfrentem desafios relacionados à cibersegurança de maneira prática e interativa, promovendo um ambiente de aprendizado dinâmico (Dweck, 2017).

Este tipo de abordagem não apenas engaja os participantes, mas também facilita a assimilação de conhecimentos complexos por meio da aplicação de mecânicas de jogos, como sistemas de pontuação, recompensas e feedback imediato. Tais elementos são fundamentais para criar um ciclo de aprendizado que se destaca pela sua eficácia, superando muitas das limitações encontradas em métodos tradicionais de ensino (Venturi; Konell; Giovanela, 2021).

A utilização da gamificação no treinamento em SI é particularmente pertinente, dado que essa área demanda uma compreensão não apenas teórica, mas também prática dos riscos e das ameaças cibernéticas.

A gamificação proporciona um ambiente seguro onde os colaboradores podem experimentar e testar suas habilidades sem as repercussões negativas que poderiam surgir em situações do mundo real. Através de simulações de cenários de ataque, os participantes podem aprender a identificar fraudes e responder a incidentes de forma mais eficiente, ao mesmo tempo em que desenvolvem um sentido de responsabilidade e compromisso com a segurança organizacional Alves (2024).

A simulação se apresenta como uma ferramenta poderosa para o estudo de sistemas complexos, possibilitando a recriação de cenários que replicam situações do mundo real (Celestino; Valente, 2021).

No contexto de SI, essa metodologia permite que os colaboradores pratiquem suas respostas a incidentes cibernéticos, como ataques de *phishing*, dentro de um ambiente controlado e seguro. As simulações não apenas oferecem um espaço para a experimentação, mas também são cruciais para a construção da confiança do aprendiz, permitindo que este cometa erros e aprenda com eles antes de enfrentar os desafios reais que a segurança cibernética impõe (Souza *et al*., 2024).

A capacidade de errar e aprender com esses erros em um ambiente simulado é fundamental, uma vez que a realidade de um ataque cibernético pode resultar em consequências significativas para a organização. Celestino e Valente (2021) ressaltam que a simulação ajuda a internalizar a dinâmica dos incidentes de segurança, preparando os colaboradores para responder de maneira eficiente e eficaz quando confrontados com situações reais.

Além disso, as gerações atuais, frequentemente referidas como "nativos digitais", apresentam uma tendência marcante a aprender de forma prática e interativa. Este perfil demográfico revela uma clara preferência por métodos de aprendizado que incorporam tecnologias contemporâneas, como a gamificação e a simulação, que oferecem experiências de ensino ativas e significativas.

A aplicação dessas técnicas não apenas torna o aprendizado mais atraente, mas também o alinha às expectativas e necessidades dos novos profissionais no mercado, que buscam experiências que ressoem com seu estilo de vida digital (Venturi; Konell; Giovanela, 2021).

Ao implementar técnicas de gamificação e simulação, as empresas conseguem treinar seus colaboradores para reconhecerem sinais de *phishing* de maneira prática e envolvente. Estudos indicam que o uso de jogos e simuladores para SI aumenta significativamente a retenção de conhecimento e a capacidade de identificar ataques (Rodrigues, 2023). Simuladores gamificados oferecem cenários onde os participantes devem identificar possíveis ataques de *phishing*,

tornando o processo de aprendizado mais dinâmico e interativo, o que contribui para o desenvolvimento de um "mindset de segurança" entre os colaboradores.

Dessa forma, a gamificação e a simulação representam abordagens inovadoras para fortalecer a segurança organizacional. Incorporar esses elementos no treinamento *anti-phishing* permite que os colaboradores se familiarizem com ataques reais de forma prática, ajudando a construir uma base de conhecimento que pode ser aplicada diretamente em situações do dia a dia (Celestino; Valente, 2021).

Em suma, o uso da IA e da IAC está se mostrando cada vez mais relevante na criação de treinamentos que simulam cenários de cibersegurança, particularmente em defesa contra os ataques de *phishing*. A aplicação de gamificação e simulação não apenas fortalece a aprendizagem em SI, mas também promove uma mudança comportamental nos colaboradores, fazendo com que estes adotem práticas seguras e conscientes no ambiente digital. A combinação dessas tecnologias oferece uma abordagem integrada e eficaz para capacitar colaboradores de maneira ativa e significativa, promovendo uma cultura de segurança em toda a organização.

3 METODOLOGIA

A metodologia deste estudo é estruturada em duas etapas principais: a pesquisa bibliográfica, seguida pela criação de um jogo, cujos detalhes serão apresentados na seção Resultados.

3.1 Pesquisa Bibliográfica

O método de pesquisa realizado neste trabalho corresponde na busca de soluções de um problema por meio de referências teóricos publicados, analisando e discutindo as colaborações científicas.

Diversas técnicas foram empregadas para identificação e análise das fontes relevantes sobre os temas de IA e IAC, Treinamentos e Simulações e o *phishing*. A investigação abrangeu uma ampla gama de materiais, incluindo livros, artigos científicos, vídeos e dissertações e teses, todos relacionados a tópicos como "treinamentos corporativos", "Inteligência Artificial", "Inteligência Artificial Cognitiva", "a importância da simulação", "gamificação em ambientes corporativos" e "*phishing".*

As fontes foram localizadas em bases de dados como Google Acadêmico e SciELO. Estas bases foram escolhidas devido ao fato de possuírem repositórios de trabalhos científicos que proveem acesso gratuito a informação.

A partir dos materiais encontrados nas fontes mencionadas acima, se utilizou como critério para a análise de dados a leitura preliminar dos resumos e títulos, foi possível refinar a seleção para incluir aqueles que mais se alinhavam aos objetivos do estudo. A Tabela 1 apresenta um resumo dos termos de busca utilizados e o número de artigos encontrados para cada um deles e suas respectivas relevâncias.

Tabela 1 – Tabela de dados.

Termos de busca	Relevância	Quantidade de Artigos
Treinamentos corporativos	**Baixa**	**2**
Inteligência Artificial	**Média**	**5**
Inteligência Artificial Cognitiva	**Alta**	**3**
A importância da Simulação	**Alta**	**2**
Gamificação em Ambientes Corporativos	**Média**	**10**
Phishing	**Alta**	**4**

Fonte: Elaborada pelos autores (2024).

3.2 Desenvolvimento do jogo

A abordagem adotada neste estudo estabeleceu uma base teórica sólida, providenciando as condições preliminares para o desenvolvimento do jogo. O método escolhido visa proporcionar um treinamento inovador, com um enfoque aprofundado nos ataques cibernéticos, especificamente no *phishing*.

Nesse contexto, ao longo da pesquisa, foi elaborado um jogo que se relaciona intimamente com o referencial teórico obtido através da pesquisa bibliográfica, a qual foi orientada pelos objetivos gerais do estudo, assim possibilitando a sua criação como ferramenta para treinamentos sobre ataques de *phishing*. No Quadro 1 é exibido as ferramentas usadas no desenvolvimento do jogo.

Quadro 1 – Ferramentas usadas

Ferramentas	Aplicação
Leonardo.AI	Gerar imagens
Leonardo.AI	Editar imagens
Google Imagens	Pesquisar imagens
Canva	Criar páginas
QR *Tiger*	Gerar QR *Codes*

Fonte: Elaborada pelos autores (2024).

O processo de criação visual do jogo utilizou a ferramenta de IA Leonardo.ai, esta ferramenta permite gerar imagens com base nos prompts de comando, além disso ela também fornece uma ferramenta de edição que permite realizar edições nas imagens geradas, ambas foram fundamentais para criar o visual do jogo.

A ferramenta de busca do Google foi utilizada para complementar o visual, nos casos em que não era possível gerar a imagem desejada, foi utlizada imagens pesquisadas para dar referência na geração de imagens. Vale ressaltar o uso da ferramenta QR *Tiger*, que foi usada para criar os QR *Codes* presentes em alguns itens do jogo.

O jogo foi concebido a partir de mecânicas inspiradas em um jogo consolidado, o Cuop, o que facilita a simulação de ataques de *phishing* por meio de narrativas variadas para imaginar cenários a partir de suas ações básicas de jogo. Dentre essas mecânicas se destacam as cartas que tem como funções atacar e defender, assim cada carta tem uma função específica de *phishing*, similar as cartas de influência e que funcionam de acordo com seus determinados tipos de *phishing* mencionados na revisão da literatura. O Quadro 2 apresenta estas ações.

Quadro 2 – Ações de jogo

Elemento	Descrição	Impacto no jogo
Minerar criptomoeda	Permite coletar criptomoeda	Estratégia básica para acumular moedas
Realizar ataque	Permite realizar um ataque	Realiza um ataque com base nas suas cartas ou nos seus blefes
Realizar troca de dispositivo	Permite trocar uma carta de dispositivo	Realiza a troca da carta de dispositivo a troco de 1 criptomoeda
Trocar carta de ataque ou defesa	Permite trocar uma carta de ataque ou de defesa	Realizar a troca de uma carta de ataque ou defesa a troco de 1 criptomoeda
Realizar ataque com IA	Permite realizar um ataque indefensável	Realiza um ataque que não pode ser defendido por nenhuma carta de defesa a troco de 10 criptomoedas

Fonte: Elaborada pelos autores (2024).

Além disso, deve-se destacar as mecânicas de interações como blefe, contestação, bloquear e revelar, estas similares as mecânicas presentes no Coup, adicionadas para tornar o jogo mais divertido e acessível. No Quadro 3 é possível entender melhor estas mecânicas.

Quadro 3 – Interações de jogo

Elemento	Descrição	Impacto no jogo
Bloqueio	Permite realizar um bloqueio	Bloqueia um ataque do adversário
Contestar	Contesta a ação de um jogador	Ao contestar você desafia um jogador a provar que tem determinada carta e vice-versa
Revelar	Revela as cartas	Ao perder para uma contestação você é obrigado a revelar suas cartas
Blefar	Blefa para fingir que tem determinada carta	Ao blefar o indivíduo corre um risco que pode ser vantajoso ou não

Fonte: Elaborada pelos autores (2024).

Existem quatro tipos de cartas no jogo, as cartas de ataque, defesa, dispositivos e as criptomoedas. O Quadro 4 remete ao Sistema de jogo, sendo possível compreender como funciona a organização para iniciar o jogo.

Quadro 4 – Sistema de jogo

Elemento	Descrição	Impacto no jogo

Cartas de Ataque	Cada jogador começa com 3 cartas de ataque	Permite atacar os adversários
Cartas de Defesa	Cada jogador começa com 3 cartas de defesa	Permite bloquear ataques adversários
Cartas de Dispositivo	Cada jogador deve receber 1 carta de dispositivo	Permite não sofrer alguns tipos de ataques dependendo da carta que possui
Criptomoeda	Blefa para fingir que tem determinada carta	Coletar criptomoedas ao longo da partida pode ser vantajoso para realizar ataques ou mudar de estratégia

Fonte: Elaborada pelos autores (2024).

As cartas de ataque são completamente baseadas nos ataques *phishing* e cada uma delas tem uma função de atacar extremamente similar aos eu tipo de *phishing*. O Quadro 5 exibe as cartas de ataque a as diferenças entre cada uma.

Quadro 5 – Cartas de ataque

Elemento	Descrição	Impacto no jogo
Phishing	Realizar um ataque p*hishing*	Permite realizar ataques que eliminam outras cartas e acumula criptomoedas
Spear - phishing	Realiza um ataque de s*pear – phishing*	Permite realizar um ataque contra mais de um adversário. Elimina outras cartas e rouba criptomoedas
Whaling	Realiza um ataque de w*haling*	Permite atacar diretamente o oponente mais forte, eliminando outras cartas e roubando criptomoedas
Smishing	Realiza um ataque de s*mishing*	Permite realizar um ataque com o objetivo de roubar criptomoedas
Vishing	Realiza um ataque de v*ishing*	Permite realizar um ataque que elimina uma carta do adversário

Fonte: Elaborada pelos autores (2024).

As cartas de defesa foram criadas para se defender de suas respectivas contrapartes e citar as contramedidas recomendadas para lidar com o determinado ataque *phishing*. No Quadro 6 é mostrado as funções delas.

Quadro 6 – Cartas de defesa

Elemento	Descrição	Impacto no jogo

Phishing	Bloqueia o ataque da carta de ataque p*hishing*	Realiza a defesa contra os ataques p*hishing*, permitindo manter suas cartas e suas moedas intactas
Spear - phishing	Bloqueia o ataque da carta de ataque de s*pear - phishing*	Realiza a defesa contra os ataques s*pear - phishing*, permitindo manter suas cartas intactas
Whaling	Bloqueia o ataque da carta de ataque de w*haling*	Realiza a defesa contra os ataques w*haling*, permitindo manter suas cartas e moedas intactas
Smishing	Bloqueia o ataque da carta de ataque de s*mishing*	Realiza a defesa contra os ataques de s*mishing*, permitindo manter suas moedas intactas
Vishing	Bloqueia o ataque da carta de ataque de v*ishing*	Realiza a defesa contra os ataques de v*ishing*, permitindo manter suas cartas intactas

Fonte: Elaborada pelos autores (2024).

As cartas de Dispositivos foram feitas para representar um dos dois dispositivos mais tradicionais usados pelas pessoas comuns, essas cartas servem como uma defesa básica e não podem ser afetados por alguns ataques devido à natureza de deles. Já as moedas, tem a função literal onde os jogadores "pagam" determinados valores para realizar os ataques ou perdem moedas devidos a não proteção contra eles.

Para um entendimento melhor do desenrolar do jogo, estará listado a seguir um fluxo do jogo.

1. Início do Jogo: Preparação da mesa, regras explicadas, o jogo começa.
2. Distribuição de Cartas: Cada jogador recebe 4 cartas, sendo elas duas de ataque e duas de defesa, todas viradas para baixo.
3. Turno dos Jogadores: Verifica de quem é a vez:

Jogador X escolhe uma ação (minerar criptomoeda, realizar ataque, trocar carta de dispositivo, trocar carta de ataque ou defesa, realizar ataque com IA) ou responde a uma ação anterior.

4. Desafio ou Bloqueio: O jogador Y pode contestar a ação, aceitá-la ou bloqueá-la com uma carta de influência, blefando ou não.
5. Resolução de Desafio: Se há uma contestação, revela ou perde a carta.
6. Verificar Eliminação: Se um dos jogadores perder as quatro cartas, ele é eliminado.
7. Próximo Jogador: Passa-se a vez até restar apenas um jogador.
8. Fim do Jogo: Quando só resta um jogador com cartas na mão ele vence.

Vale ressaltar a presença de QR *codes* presentes nas cartas de defesa, estes que tem como função informar os usuários sobre as contramedidas de determinado *phishing*. Destaca-se o uso da ferramenta de IAC *Amazon Comprehend*, que usa algoritmos de processamento de linguagem natural que permite analisar texto e extrair informações relevantes. Tais como: Sentimentos, entidades, tópicos, sintaxe e idioma. Dessa forma sendo possível fazer uma análise de feedbacks e realizar melhorias no jogo para aplicar em futuros treinamentos.

4 RESULTADOS

Como resultado pode-se destacar a criação de um protótipo do jogo com base no referencial teórico. O jogo foi denominado *Phishing War*, nele o jogador deve gerenciar suas cartas de ataque e defesa para se proteger de outros ataques e eliminar todas as cartas dos adversários e consequentemente ganhar o jogo. O jogo ilustra de uma forma lúdica e interativa os tipos de ataques *phishing* mencionados anteriormente e seus diferentes funcionamentos. Dessa forma, gerando engajamento dos jogadores e desenvolvendo o conhecimento em relação a esse tipo de ciberataque.

A composição do jogo é dividida em 30 cartas de ataque e 30 cartas de defesa, além de 15 cartas de dispositivos e 100 cartas de criptomoedas. As cartas de dispositivo são divididas entre dispositivos celulares e computadores, as cartas de ataque são divididas entre 5 tipos de ataque *phishing* e as cartas de defesa são divididas em 5 tipos de defesa contra esses ataques.

Começando pelas cartas de ataque, na parte superior se encontra o ícone da carta de dispositivo que ela pode atacar, no meio possuem um símbolo para seus determinados tipos de ataque *phishing* e na parte inferior o tipo de ataque. Abaixo na Figura 1 tem um exemplo de uma carta de ataque *spear phishing* com frente e verso.

Figura 1 – Carta de ataque *spear phishing* frente e verso

Fonte: Elaborada pelos autores (2024).

Estas estão divididas em:

- Carta de ataque *phishing*: Pode tirar uma carta de defesa ou de ataque do adversário. Pode retirar metades das moedas, se o adversário estiver com um número ímpar de criptomoedas, o atacante fica com a metade maior. Só funciona se o oponente estiver com carta de dispositivo do Computador, similar ao *phishing* tradicional que era enviado por e-mail para atacar dispositivos computadores.
- Carta de ataque *spear phishing*: É uma carta que só pode ser usada para atacar 2 adversários de uma vez e que tenham alguma carta em comum, tanto de ataque, defesa ou dispositivo. Deve retirar 1 carta de ataque e 1 de defesa, mas somente uma por adversário, se já tirou uma carta de ataque, a outra a ser tirada deve ser a de defesa e vice e versa. O funcionamento desta carta simula a personalização de ataque característico do *spear phishing*, como atacar indivíduos que possuem coisas em comum, como a mesma organização.

- Carta de ataque *whaling*: Esta carta só pode ser usada para atacar a pessoa que possui mais dinheiro ou mais cartas na mão. Não pode ser usada se os jogadores estiverem com a mesma quantidade de cartas e criptomoedas. Se bem-sucedido, pode retirar 1 de ataque e 1 de defesa e pode retirar metade das criptomoedas do oponente. Se o adversário estiver com um número ímpar de criptomoedas, o atacante fica com a metade menor. Como o próprio ataque que dá o nome a carta, a função dela simula a forma destinada de atacar indivíduos poderosos, como executivos. Neste caso, os poderosos são os jogadores que estão mais fortes no jogo.
- Carta de ataque *smishing*: Pode retirar metade das moedas do adversário, se o adversário estiver com um número ímpar de criptomoedas, o atacante fica com a metade maior. Só funciona em oponentes que possuem a carta de dispositivo celular, da mesma maneira que o *smishing* é usado contra celulares.
- Carta de ataque *vishing*: Esta carta consegue retirar 1 carta de ataque ou defesa do oponente. Só funciona em oponentes que possuem a carta de dispositivo celular, similar a forma como o *vishing* é utilizado contra celulares.

Já as cartas de defesa servem exclusivamente para defender suas respectivas contrapartes. Na parte superior elas possuem o símbolo do ataque que ela defende, além do ícone de bloqueio para reforçar sua função. No meio tem o QR *code* e na parte inferior tem o nome do ataque bloqueado. Na Figura 2 é exibido um exemplo de uma carta de defesa *spear phishing* com frente e verso.

Figura 2 – Carta de defesa *spear phishing* frente e verso

Fonte: Elaborada pelos autores (2024).

Ao interagir com o QR *code*, ele redireciona para uma página do site do jogo para que o jogador veja informações relevantes sobre o ataque bloqueado. A Figura 3 mostra umas das páginas informativas.

Figura 3 – Página informativa

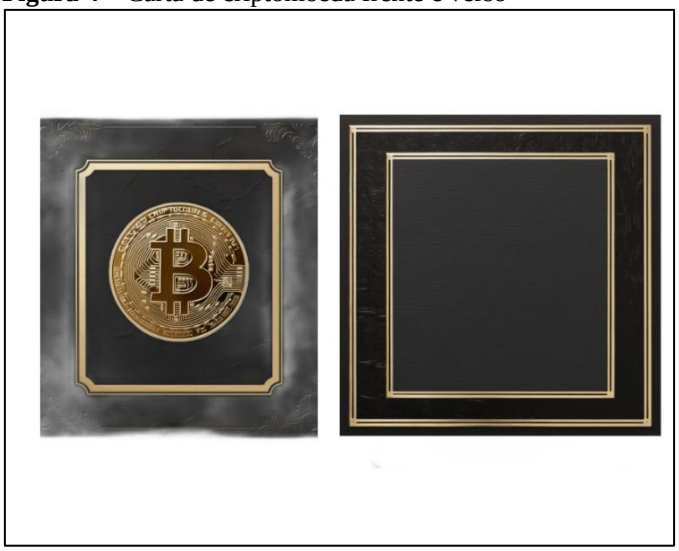
Fonte: Elaborada pelos autores (2024).

Das cartas de defesa tem-se:

- Carta de defesa de *phishing*.
- Carta de defesa de *spear phishing*.
- Carta de defesa de *whaling*.
- Carta de defesa de *smishing*.
- Carta de defesa de *vishing*.

Além disso, tem-se as cartas de criptomoedas, que são as moedas do jogo, está carta possuem em sua composição somente um ícone de bitcoin para ilustrar o significado de criptomoeda. Na Figura 4 é exibido a carta de criptomoeda e seu verso.

Figura 4 – Carta de criptomoeda frente e verso

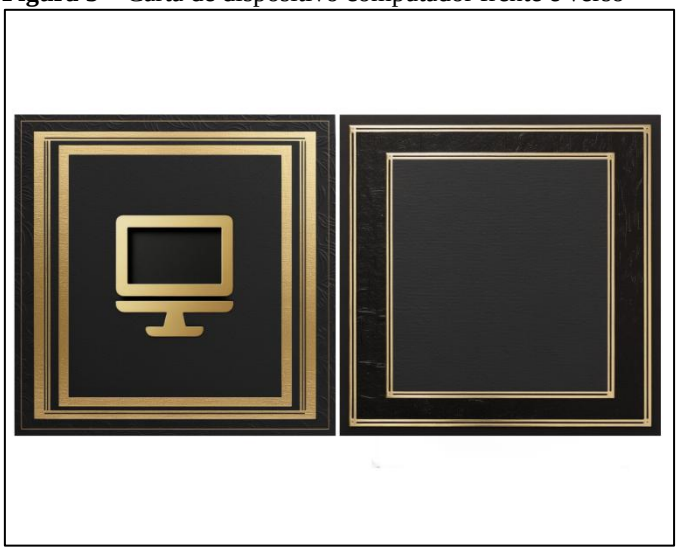


Fonte: Elaborada pelos autores (2024).

A respeito sobre as cartas de dispositivos, elas servem como uma primeira barreira de proteção do jogador, não é necessário ter uma carta de defesa para determinado ataque, se ele

não for permitido atacar oponentes com determinada carta de dispositivo. Elas possuem somente um ícone do dispositivo em sua composição. Na Figura 5 é mostrado uma carta de dispositivo computador e seu verso.

Figura 5 – Carta de dispositivo computador frente e verso



Fonte: Elaborada pelos autores (2024).

Estas cartas serão mais bem explicadas abaixo:

- Carta de dispositivo computador: O jogador que deter essa carta fica imune das cartas de ataque *vishing* e *smishing*, mesmo que ele não tenha as cartas de defesa para com esses respectivos ataques.
- Carta de dispositivo celular: O jogador que deter essa carta fica imune das cartas de ataque *phishing*, mesmo que ele não tenha as cartas de defesa para com esses respectivos ataques.

O objetivo do jogo é simular de forma simples os tipos de ataques *phishing* e suas diferenças de um para o outro. O jogo pode ser jogado de 2 a 8 pessoas, podendo ser jogado individualmente ou entre times, contanto que tenha no mínimo 4 jogadores. O vencedor ou equipe vencedora será aquele ou aqueles que tirarem todas as cartas de ataque e defesa dos seus adversários.

Os jogadores terão cinco opções de ação no jogo em suas determinadas vezes, sendo estas opções coletar uma criptomoeda, realizar uma ação de ataque, trocar uma carta de dispositivo, trocar uma carta de ataque ou defesa a troco de uma criptomoeda ou realizar um ataque *phishing* com IA, vale ressaltar que esse último requer 10 criptomoedas e não pode ser defendido pelo adversário, levando o mesmo a perder 2 cartas a escolha do atacante.

No modo de jogo básico, os jogadores devem receber 3 cartas de ataque e 3 cartas de defesa e 1 carta de dispositivo no começo do jogo, tirando a carta de dispositivo as outras cartas não devem ser mostradas. O jogador da vez poderá realizar umas das cinco ações mencionadas anteriormente, se estiver no alcance dele. Dessa forma, o jogo segue sucessivamente até que sobre somente um jogador ou equipe com cartas de ataque ou defesa.

Existem três mecânicas importantes que interagem no decorrer do jogo, a contestação, o blefe e a revelação das cartas. Um jogador pode blefar ao realizar um ataque ou um bloqueio, se o rival cair no blefe o jogo segue normalmente, mas caso ele não caia, ele pode contestar sua carta. Se o jogador não tiver a carta que ele blefou ter, ele é obrigado a revelar a carta deixando para cima e a ação da carta é cancelada. Caso o contrário ocorra e o atacante ou bloqueador

prove que tem a carta, o rival que contestou perde uma carta e é obrigado a revelar outra carta a escolha dele. E o adversário que precisou provar, pode trocar a carta que ele revelou por outra carta e sem custos.

É de extrema importância frisar o uso da IAC, afinal ela é peça fundamental para a evolução do jogo como instrumento de treinamentos futuros, a habilidade que ela tem em simular pensamentos humanos pode ser muito importante para capitalizar no que precisa ser melhorado no contexto do jogo como prever o que pode ser melhorado. Fora a habilidade de entender emoções pode ser útil para nivelar esse tipo de ferramenta através de *feedbacks*.

O jogo como instrumento de treinamentos pode ser uma abordagem interessante para com a aprendizagem. Por ser uma ferramenta mais engajadora e fácil de absorver, é possível reter o conhecimento desenvolvimento ao jogar o jogo, principalmente com as interações entre ataque e defesa, onde na prática, se presencia diferentes cenários aplicáveis no cotidiano das empresas e até mesmo no dia a dia comum.

5 CONSIDERAÇÕES FINAIS

Neste artigo, desenvolveu-se um jogo focado em ataques de *phishing*, com o intuito de oferecer uma alternativa mais interativa e eficaz aos métodos tradicionais de treinamento em SI. O jogo integra conceitos de gamificação e simulação, criando uma experiência prática e lúdica para que os colaboradores aprendam sobre diferentes tipos de *phishing* e métodos de defesa. Observou-se que a IA desempenhou um papel fundamental, auxiliando tanto na criação dos visuais quanto na pesquisa teórica que fundamentou o jogo. Futuramente, acredita-se que a IA poderá contribuir ainda mais, ao proporcionar uma experiência personalizada, adaptando os desafios ao nível de conhecimento de cada jogador e fornecendo feedback em tempo real.

Os resultados deste estudo indicam que a gamificação pode desempenhar um papel significativo na atualização das práticas de treinamento corporativo, especialmente em áreas críticas como a SI. Por meio de um ambiente interativo e competitivo, estimula-se o engajamento e a retenção de conhecimento entre os colaboradores, preparando-os de forma mais eficaz para lidar com ameaças cibernéticas.

Conclui-se que o avanço das ameaças cibernéticas exige constante inovação nos métodos de treinamento. A abordagem qualitativa deste estudo permitiu identificar a gamificação como uma metodologia promissora para capacitar futuras gerações para prevenção de ataques cibernéticos.

Em trabalhos futuros, sugere-se a avaliação do jogo em ambiente real, explorando o impacto da gamificação no aprendizado em SI. Além disso, recomenda-se expandir o uso da IA cognitiva para monitorar e adaptar a experiência de aprendizado dos jogadores, maximizando sua eficácia e aplicação prática em diferentes cenários organizacionais.

REFERÊNCIAS

ALVES, F. **Gamification:** como criar experiências de aprendizagem engajadoras. 2. ed. rev. e ampl. São Paulo: DVS Editora, 2024.

ARAÚJO, M. J. R. DE; BASTOS, D. F.; SILVA, F. R. DA. Inteligência Artificial e Inteligência Cognitiva: Uma abordagem sobre a atualidade. **Encontro Internacional de Gestão, Desenvolvimento e Inovação (EIGEDIN)**, v. 3, n. 1, 13 out. 2019. Disponível em: https://periodicos.ufms.br/index.php/EIGEDIN/article/view/8763.

BARBOSA, P.; FERREIRA, M.; NEVES, J. E. D**. Abordagem de Segurança no Desenvolvimento de Aplicações Web**. III FatecSeg. 2023. Disponível em:

https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/107. Acesso em 20 jun. 2024.

CAMPOS, R. C.; BRITO, V. da G. P. Treinamentos corporativos na perspectiva da prática social. **SCRIBES - Brazilian Journal of Management and Secretarial Studies**, v. 1, n. 1, p. 53-66, jul. 2020. Disponível em: https://doi.org/10.33228/scribes.2020.v1.10634. Acesso em: 1 ago. 2024.

CELESTINO, M. S.; VALENTE, V. C. P. N. Aplicabilidade e benefícios de softwares e simuladores em processos de ensino-aprendizagem. **ETD - Educação Temática Digital**, Campinas, v. 23, n. 4, p. 881-903, jan./mar. 2021. Disponível em: https://doi.org/10.20396/etd.v23i4.8658342. Acesso em: 10 set. 2024.

DAMASCENO, H.; FREIRE, V.; SANTOS, W.; FAZZION, E.; FONSECA, O.; CUNHA, I.; HOEPERS, C.; STEDING-JESSEN, K.; CHAVES, M. H. P. C.; GUEDES, D.; MEIRA JR., W. **Monitoramento e Identificação de Páginas de Phishing**. In: Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 39, 2021, Uberlândia. Anais. Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 378-391. Disponível em: https://doi.org/10.5753/sbrc.2021.16734. Acesso em: 9 set. 2024.

DWECK, C. S. **Mindset**: A nova psicologia do sucesso. 1.ed. São Paulo: Objetiva, 2017.

LUDEMIR, T. B. Inteligência Artificial e Aprendizado de Máquina: estado atual e tendências. **Estudos Avançados**, [S. l.] v. 35, n. 101, p. 85–94, jan. 2021. Disponível em: https://doi.org/10.1590/s0103-4014.2021.35101.007. Acesso em: 1 mar. 2024.

MOURA, T. M.; D' ALKMIN NEVES, J. E. **Análise de Segurança em Dispositivos Internet das Coisas. Revista Interface Tecnológica**, [S. l.], v. 18, n. 2, p. 15-27, 2021. Disponível em: https://doi.org/10.31510/infa.v18i2.1174. Acesso em 20 jun. 2024.

NEVES, J. E. D. A**. Mineração de dados aplicada a simulação de cenários complexos em sistemas multiagentes**. Orientadores: Paulo Sérgio Martins Pedro (in memoriam), Marli de Freitas Gomes Hernandez. 2024. 237 p. Tese (Doutorado em Tecnologia) - Faculdade de Tecnologia, Universidade Estadual de Campinas (UNICAMP), Limeira, 2024. Disponível em: https://www.repositorio.unicamp.br/acervo/detalhe/1395946. Acesso em: 20 jun. 2024.

NEVES, J. E. D. A.; PEDRO, P. S. M.; HERNANDEZ, M. F. G.; FABRI JUNIOR, L. A. **Simulation of the Implementation of Domestic Solar Systems Using Multi-agent Systems from Web Scraping**. Smart Innovation, Systems and Technologies. 1ed.: Springer International Publishing, 2023, v. 1, p. 88-96. Disponível em: https://doi.org/10.1007/978-3-031-04435-9_8. Acesso em: 20 jun. 2024.

PEDRO, A. M.; TURCI JUNIOR, M.; MONTEIRO, A. S.; ESPERANDIO, A. A. M.; BASTOS, C. V.; NEVES, J. E. D. **Blockchain como Fator de Transparência**. Revista Brasileira em Tecnologia da Informação, v. 5, p. 79-95, 2024. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/104. Acesso em 20 jun. 2024.

PIRES, E. F. M.; NEVES, J. E. D. **Os Benefícios do ChatGPT**: Uma Abordagem para Potencializar Técnicas de Hardening. 13º CONCISTEC - Congresso Científico da Semana

Nacional de Ciência e Tecnologia do IFSP. Artigo 41. 2023. Disponível em: https://drive.ifsp.edu.br/s/e4nk2YzbHtCHaq6/download?path=%2F&files=41_OS%20BENEFICIOS%20DO%20CHAT%20GPT_%20UMA%20ABORDAGEM%20PARA%20POTENCIALIZAR%20T%C3%89CNICAS%20DE%20HARDENING.pdf. Acesso em 20 jun. 2024.

REZENDE, G. G. **O phishing e a responsabilidade empresarial:** aspectos sobre as medidas protetivas do empresário face ao prejuízo de seus usuários. Orientador: Almir Garcia Fernandes. 2022. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Uberlândia, Uberlândia, 2022. Disponível em: https://repositorio.ufu.br/handle/123456789/34807. Acesso em: 9 de out. 2024.

RODRIGUES, D. B. **Os efeitos da gamificação na facilitação de treinamentos corporativos.** Orientadora: Florence Marie Dravet. 2023. Dissertação (Pós- Graduação em Educação) – Universidade Católica de Brasília, Brasília, 2023. Disponível em: https://bdtd.ucb.br:8443/jspui/handle/tede/3319. Acesso em: 7 de out. 2024.

RODRIGUES, L. F. F.; BASTOS, I.A.M.M. **Um sistema inteligente para prevenção de ataques *phishing*.** Orientador: Igor Augusto Mageste da Mota Bastos. 2018. Trabalho de Conclusão de Curso (Graduação em Engenharia de Redes de Comunicação) – Universidade de Brasília, Brasília, 2018. Disponível em: https://bdm.unb.br/handle/10483/28634. Acesso em: 20 de out. 2024.

SANTOS, A. M.; NEVES, J. E. D. **Exploração Maliciosa do ChatGPT para Ataques Cibernéticos.** III FatecSeg. 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/108. Acesso em 20 jun. 2024.

SILVA, C. D. S. **LUDICALIZANDO #004 - Por que alguns treinamentos corporativos falham?** 4 out. 2018. 3 min. Canal Ciro Daniel - Treinador Corporativo. Disponível em: https://www.youtube.com/watch?v=WKSo95SrATg. Acesso em: 25 jul. 2024.

SOUZA, A. L. O.; BASTOS, C. V.; SANTOS, P. M. S.; SOARES, N. M.; NEVES, J. E. D. **Cibersegurança na Agricultura de Precisão:** Exploração à Aplicação de Medidas Preventivas. Advances in Global Innovation & Technology, v. 2, p. 61-73, 2024. Disponível em: https://doi.org/10.29327/2384439.2.2-5. Acesso em 20 jun. 2024.

TONEZER, L. N.; SILVA, A. C. M.; ALMEIDA, A. H.; NEVES, J. E. D. **Simulações Multiagentes e Phishing:** Explorando a Segurança em Ambientes de Nuvem. Revista Tecnológica da Fatec de Americana, v. 11, p. 1-17, 2024. Disponível em: https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/393. Acesso em 3 nov. 2024.

VENTURI, D.; KONELL, A. E.; GIOVANELA, A. **Treinamento:** importância e benefícios da disponibilização de treinamento nas organizações. **REVISTA CIENTÍFICA FAMAP**, *[S. l.]*, v. 1, n. 01, 2021. Disponível em: https://famap.emnuvens.com.br/revista/article/view/5. Acesso em: 3 nov. 2024.