CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO NO COMBATE À ENGENHARIA SOCIAL

CLEVISON DA SILVA FERREIRA[1]
JOSÉ ROBERTO DE ARAÚJO FONTOURA[2]
DAVID BACELAR COSTA SEABRA[3]

UNIVERSIDADE DO ESTADO DA BAHIA (UNEB)
2025

RESUMO

Mesmo com os avanços tecnológicos que aperfeiçoam a segurança da informação, o fator humano ainda continua sendo um dos principais elementos de vulnerabilidade. Com a engenharia social, aproveitando-se das fragilidades humanas, onde cada vez mais brechas são deixadas para que cibercriminosos realizem ataques sem a necessidade de falhas técnicas em softwares e hardwares. Este trabalho teve como objetivo analisar, por meio de revisão bibliográfica, a importância da conscientização em segurança da informação como estratégia fundamental no combate à engenharia social, destacando iniciativas, ferramentas e práticas aplicadas em diferentes contextos organizacionais. A metodologia para chegar ao objetivo é definida à natureza como básica, com objetivo descritivo, sendo a abordagem qualitativa e o método hipotético-dedutivo de procedimento de revisão bibliográfica. Os resultados da pesquisa reforçam que a aplicação de estratégias de conscientização em segurança da informação é de extrema importância, levando em consideração o contexto atual.

Palavras-chave: Segurança da Informação. Engenharia Social. Conscientização.

ABSTRACT

Even with technological advancements that improve information security, the human factor remains one of the main elements of vulnerability. Social engineering, exploiting human frailties, creates increasing loopholes that allow cybercriminals to carry out attacks without needing to exploit technical flaws in software and hardware. This work aimed to analyze, through a literature review, the importance of information security awareness as a fundamental strategy in combating social engineering, highlighting initiatives, tools, and practices applied in different organizational contexts. The methodology used to achieve this objective is defined as basic in nature, with a descriptive objective, employing a qualitative approach and a hypothetical-deductive method for the literature review procedure. The research results reinforce that the application of information security awareness strategies is extremely important, considering the current context.

Keywords: Information Security. Social Engineering. Awareness.

[1] Graduando em Sistemas de Informação: clevison_silva@hotmail.com
[2] Doutor em Difusão do Conhecimento - Orientador e Professor da UNEB: jfontoura@uneb.br
[3] Mestre em Modelagem e Simulação de Biossistemas - Coorientador: dseabra@uneb.br

1 INTRODUÇÃO

A contínua evolução digital e tecnológica traz consigo diversos benefícios para a sociedade, mudando como indivíduos e organizações interagem, armazenam e compartilham seus dados. Em um mundo que se torna cada vez mais digital e interconectado, não são somente os benefícios que chamam atenção nesse contexto. O advento da internet e as interações digitais tornaram-se, também, terreno fértil para a criminalidade cibernética. Dentre essas, destaca-se uma prática criminosa crescente denominada de “engenharia social”, que consiste essencialmente na exploração das vulnerabilidades humanas, em vez de falhas técnicas, se estabelecendo como uma das práticas mais aplicadas por cibercriminosos. Para tanto, novos desafios também emergem relacionados à segurança da informação, sendo essencial a busca por estratégias para combater esses crimes.

Conforme aponta o especialista em cibersegurança Baiardi (2024), 74% dos ataques cibernéticos em 2023 foram motivados por falhas humanas. Diante de tal percentual, levanta-se a seguinte questão a ser analisada no decorrer deste trabalho: De que maneira a conscientização em segurança da informação pode ser relevante no combate à engenharia social, considerando que a maioria dos incidentes de segurança da informação ainda são causados por falhas humanas?

O objetivo geral deste trabalho é analisar a importância da conscientização em segurança da informação como estratégia fundamental no combate à engenharia social. Como objetivos específicos, busca-se: conceituar os principais termos relacionados à engenharia social e à segurança da informação; revisar trabalhos acadêmicos, estudos de caso e iniciativas práticas voltadas para a conscientização em segurança da informação; identificar estratégias de conscientização utilizadas nas organizações; discutir os impactos e contribuições dessas estratégias para a redução de vulnerabilidades humanas.

A relevância deste estudo justifica-se tanto pelo interesse pessoal na área quanto pela crescente importância desse tema atualmente. Sendo que grande parte dos incidentes em segurança ocorre devido à falta de conhecimentos dos usuários. Desse modo, torna-se importante investigar as práticas de conscientização.

A hipótese que parte desse trabalho é a de que a conscientização em segurança da informação, quando aplicada de forma contínua e estruturada, contribui

significativamente para reduzir vulnerabilidades humanas e minimizar a efetividade dos ataques de engenharia social em organizações.

Este trabalho segue com sua estrutura contando com a introdução, que apresenta o problema, os objetivos, a justificativa e a hipótese do estudo; segue-se o referencial teórico, no qual fornece embasamentos e conceitos de autores da área; depois, a metodologia que descreve o tipo da pesquisa adotado; em seguida, a análise de resultados onde é analisada as informações coletadas para obter o resultado da pesquisa; e as considerações finais, em que apresenta as conclusões obtidas da análise da pesquisa.

2 SEGURANÇA DA INFORMAÇÃO

Nos dias atuais em que a informação é considerada o bem mais valioso, cuidar da sua segurança é extremamente importante, ainda mais em um cenário global cada vez mais digital e interligado, a proteção das informações se consolidou como um fundamento indispensável para empresas de diferentes tamanhos e segmentos. A constante evolução das tecnologias, somada ao aumento exponencial da geração e armazenamento de dados, eleva significativamente os riscos associados à exposição, vazamento e comprometimento de informações confidenciais. Nesse cenário, assegurar a segurança dos ativos de informação se torna uma tarefa estratégica essencial e inevitável.

Segundo Fontes (2012, p. 11), “segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que têm por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.”

Segundo Ponce (2021, p.19), com base na norma ISO/IEC 27001 (2013), “para proteger as informações, a segurança da informação se baseia em três pilares: confidencialidade, integridade e disponibilidade”. Esses pilares são essenciais para garantir que dados sensíveis sejam protegidos contra acessos não autorizados, alterações indevidas e indisponibilidade. A norma define os três pilares da seguinte forma:

- **Confidencialidade**: é o que garante o sigilo de informação e impede que elas não sejam roubadas ou acessadas por pessoas não autorizadas.

- **Integridade:** é que garante a veracidade da informação e restringe o acesso e/ou alteração da informação por pessoas não autorizadas, garante a completude e preservação da precisão da informação, para que não haja perda de partes da informação.
- **Disponibilidade:** está relacionada ao tempo e à acessibilidade que se tem dos dados e sistemas da organização, esse princípio é de suma importância, pois, falhas de indisponibilidade comprometem o serviço prestado pela organização.

2.1. ENGENHARIA SOCIAL

Embora Mitnick e Simon (2003) abordem a engenharia social principalmente sob a ótica de ataques cibernéticos e fraudes, Hadnagy (2011) destaca que sua aplicação vai além do mundo do crime. Na verdade, ela é uma técnica poderosa de modulação do comportamento e tomada de decisão, onipresente em nosso dia a dia, mesmo que não a percebamos. Entender seu mecanismo é crucial para reconhecer tanto seu potencial positivo quanto seus riscos.

De acordo com Hadnagy (2011, p. 22):

> A engenharia social é usada diariamente por pessoas comuns em situações cotidianas. Uma criança tentando conseguir o que quer no corredor de doces ou um funcionário em busca de um aumento está usando engenharia social. A engenharia social acontece no marketing governamental ou de pequenas empresas. Infelizmente, ela também está presente quando criminosos, vigaristas e afins enganam as pessoas para que forneçam informações que as tornem vulneráveis a crimes. Como qualquer ferramenta, a engenharia social não é boa ou má, mas simplesmente uma ferramenta com muitos usos diferentes.

Nesse mesmo sentido, Mitnick e Simon (2003) explicam que “a engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém, que na verdade ele não é”. Portanto, nota-se que a eficácia dessa técnica reside na habilidade do atacante em criar uma relação de confiança falsa, explorando a tendência humana de ser útil, cooperativo ou obediente a figuras percebidas como legítimas.

No âmbito da cibersegurança, ao se considerar ameaças, geralmente a imagem inicial que vem à mente é a de hackers invadindo sistemas avançados, explorando vulnerabilidades de softwares ou quebrando códigos. Entretanto, a realidade é que muitas das significativas falhas de segurança não se derivam de

softwares maliciosos, mas sim de uma das abordagens mais antigas e eficientes de manipulação humana: a engenharia social.

A engenharia social envolve diversas estratégias empregadas por criminosos para influenciar pessoas e obter dados sensíveis, como senhas, informações financeiras ou permissões para acessar sistemas, sem precisar atacar diretamente a segurança de uma rede. Segundo Hadnagy (2011), a engenharia social é mais do que uma simples ação, ela representa um conjunto de competências que, quando combinadas, formam o que ele define como a própria ação, habilidade e ciência da engenharia social.

De acordo com Mitnick e Simon (2003), os usuários representam o elo mais fraco da segurança, e os ataques de engenharia social geralmente têm mais sucesso ao explorar a boa vontade de uma pessoa, sem a necessidade de técnicas avançadas de invasão.

Esse cenário, no qual o comportamento humano exerce influência direta sobre a segurança da informação, pode ser melhor compreendido em uma perspectiva da Psicologia Social. Conforme Myers (2014), “Psicologia social é uma ciência que estuda as influências de nossas situações, com especial atenção a como vemos e afetamos uns aos outros. Mais precisamente, ela é o estudo científico de como as pessoas pensam, influenciam e se relacionam umas com as outras”. Essa definição evidencia que o comportamento humano segue padrões de interação e resposta a estímulos externos. Dessa forma, a engenharia social utiliza esses conceitos para explorar justamente as vulnerabilidades presentes nessas interações e influências mútuas.

2.2. PSICOLOGIA DA ENGENHARIA SOCIAL

Considerando que a Psicologia é definida por Myers (2012) como a ciência que estuda o comportamento e os processos mentais, e a engenharia social como um ato capaz de influenciar uma pessoa a tomar uma ação que pode ou não ser do seu melhor interesse (HADNAGY, 2011)**,** a Psicologia da Engenharia Social fundamenta-se na exploração do que Cialdini (2012) identifica como padrões comportamentais humanos previsíveis. O êxito das táticas utilizadas por golpistas está diretamente relacionado à capacidade de influenciar decisões e manipular sentimentos, utilizando estratégias baseadas em princípios previamente estabelecidos pela psicologia social.

Nesse contexto, compreender os princípios que regem o comportamento humano torna-se essencial para entender como e por que a engenharia social se mostra tão eficaz. De acordo com Cialdini (2012, p. 13 - 14):

> Embora os profissionais da persuasão empreguem milhares de técnicas para convencer, a maioria delas se enquadra em seis categorias básicas, sendo cada uma delas governada por um dos princípios psicológicos fundamentais que comandam a conduta humana.

Ainda conforme o autor, esses seis princípios são apresentados como: reciprocidade, coerência, aprovação social, afeição, autoridade e escassez.

Segundo Cialdini (2012), o princípio da reciprocidade, refere-se à tendência humana de retribuir favores, podendo fazer alguém aceitar um pedido após receber um pequeno presente. O princípio da coerência diz respeito à necessidade de manter consistência com decisões passadas, levando indivíduos a agirem com base em compromissos anteriores. A aprovação social indica que as pessoas tendem a seguir o comportamento da maioria, especialmente em situações de incerteza. O princípio da afeição sugere que é mais provável que pessoas aceitem solicitações de quem conhecem ou gostam, influenciadas por atratividade, semelhança e elogios. A autoridade implica na tendência de seguir especialistas percebidos, mesmo que sua influência seja apenas simbólica. Por fim, o princípio da escassez destaca que oportunidades limitadas aumentam sua percepção de valor, incentivando decisões rápidas.

2.3. TÉCNICAS DE ENGENHARIA SOCIAL

Embora a engenharia social seja um conceito amplo que abrange diversas formas de manipulação, no contexto da segurança da informação, ela se manifesta principalmente por meio de táticas específicas voltadas ao engano de usuários, com o objetivo de obter acesso não autorizado a dados ou sistemas.

Além de apontarem que o usuário é o elo mais fraco da segurança, Mitnick e Simon (2003) complementam que “a engenharia social envolve algum tipo de interação humana. Com frequência, um atacante usa vários métodos de comunicação e tecnologias para tentar atingir o seu objetivo”. Tais métodos evoluíram significativamente e, atualmente, incluem desde interações presenciais até sofisticadas estratégias digitais. Entre as técnicas mais comuns, estão quatro, cujos

nomes derivam do inglês: phishing, vishing, pretexting e baiting, cada uma com suas próprias características e métodos de aplicação.

- Phishing: Consiste na exploração da confiança do usuário através de SMS, E-mails e sites falsos, visando à obtenção de dados confidenciais ou à propagação de programas maliciosos (KOSINSKI, 2024).

A figura 01 apresenta um e-mail de phishing, que simula uma notificação oficial do Departamento de Trânsito - DETRAN. O exemplo reforça a afirmação de Seabra (2025), o “phishing não invade sistemas. Ele pede ao usuário que abra a porta”.

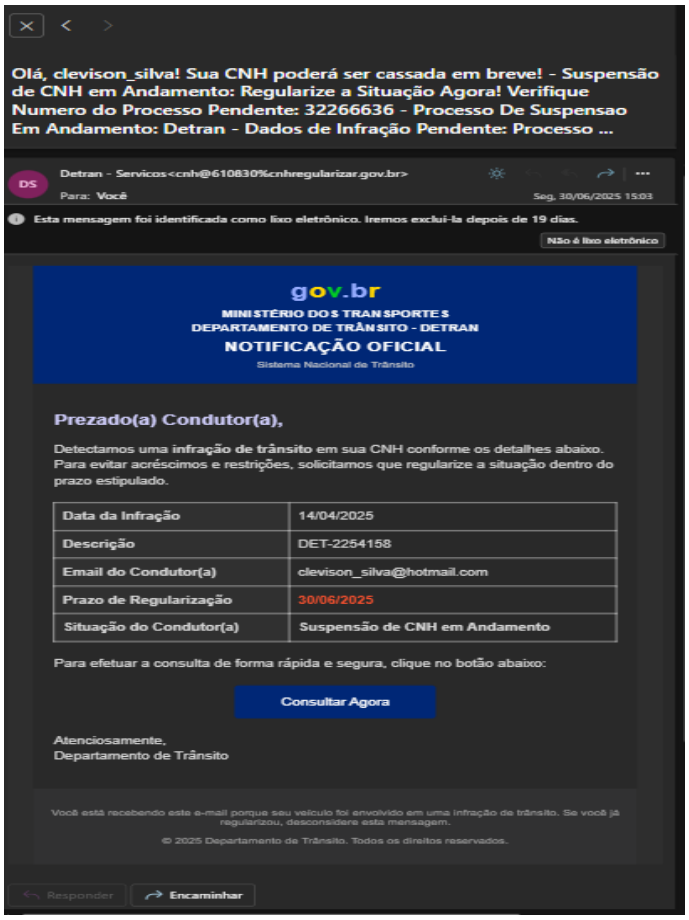

Figura 01 (Acervo do autor)

- Vishing: Para Turban e Volonino (2013, p. 199) “Também semelhante ao phishing, porém a comunicação fraudulenta vem em forma de mensagem de voz ou recado de voz incentivando a vítima a dar informações sigilosas”.

  Exemplo: Uma ligação de alguém que se apresenta como “gerente do seu banco”, alertando sobre uma transação suspeita e solicitando senhas ou códigos de verificação para “cancelá-la”.

- Pretexting: Baseia-se na criação de uma narrativa para ganhar a confiança da vítima e obter informações confidenciais, estabelecendo uma relação de confiança antes de induzi-la ao erro (BUXTON, 2025).

  Exemplo: Um criminoso liga para a vítima se passando por um técnico de suporte da empresa, solicitando o login e a senha para “resolver um problema urgente” no sistema.
- Baiting ou “iscamento”: É caracterizado por chamar a atenção da vítima por meio de promessas de benefícios ou propostas tentadoras. Ao interagir com essas iscas, geralmente disseminadas por e-mail, a vítima acaba permitindo a entrada de códigos maliciosos no sistema, comprometendo a proteção de seus dados pessoais (MARTINS, 2025). De acordo com Souza (2025), o baiting, diferente do phishing, “não depende exclusivamente do envio de e-mails ou mensagens em massa. A isca pode ser um pendrive esquecido em uma área comum de uma empresa [...] ou até mesmo uma oferta de download gratuito de músicas, filmes ou softwares em sites não-oficiais”.

  Exemplo: Um pendrive rotulado como “Planilha de Salários 2025” deixado propositalmente em um local público. Ao ser inserido em um computador, instala-se um malware que permite o acesso remoto ao sistema.

3 CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

A segurança da informação trava uma batalha constante contra ameaças digitais em evolução. Embora as empresas invistam em infraestrutura tecnológica e sistemas de proteção cada vez mais sofisticados, é importante direcionar a atenção para uma questão cultural: a necessidade de criar uma cultura de segurança da informação nas organizações. Desse modo, a tecnologia deixa de ser a única barreira de proteção e conta com o comportamento consciente dos colaboradores.

Mesmo com todos os avanços tecnológicos e diversas medidas de proteção implantadas, as organizações ainda continuam expostas a riscos significativos. Esse ponto é destacado por Mitnick e Simon (2003, p. 15), ao afirmarem que:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma

> das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.

Nessa citação, podemos entender que mesmo com todo o investimento massivo em segurança, um único erro humano, como clicar em uma tentativa de golpe enviado para seu e-mail, por exemplo, pode comprometer todo o investimento em segurança feito. Essas ações, muitas vezes motivadas por pressa, desatenção ou desconhecimento, revelam como comportamentos aparentemente simples podem comprometer toda a estrutura de segurança de uma organização.

Entende-se que o 'fator humano' não deve ser visto somente como o elo mais fraco, mas como uma camada ativa de proteção que precisa ser fortalecida.

3.1 IMPORTÂNCIA DA CONSCIENTIZAÇÃO

Na maioria dos ataques bem-sucedidos, não é necessariamente um software malicioso invencível, mas geralmente um simples erro humano que abre as portas para os invasores. Nesse mesmo contexto, reforçando o cenário preocupante citado anteriormente, Baiardi (2024), em publicação no site Security Leaders, aponta que 74% dos ataques cibernéticos em 2023 foram motivados por falhas humanas.

Esse dado reforça a percepção de que a conscientização, mais do que um complemento, é uma necessidade estratégica nas organizações. Segundo Fattori (2024), “em tempos de constantes ameaças digitais, a conscientização em segurança da informação se tornou um pilar indispensável para proteger dados e minimizar vulnerabilidades dentro das organizações”.

Essa relevância é reconhecida também por meio de trabalhos acadêmicos, que apresentam diversas iniciativas com abordagens distintas. A pesquisa de Pires (2023), evidencia que treinamentos práticos e simulações de ataques são eficazes para fortalecer a cultura de segurança da informação em ambientes financeiros.

Cardoso, W. (2024), com o desenvolvimento do Awareness and Prevention Expert System against Engineering Attacks (APSEA), em tradução para o português: “Sistema Especialista de Conscientização e Prevenção contra Ataques de Engenharia”, explora o uso de inteligência artificial para simular raciocínios humanos e fornece recomendações personalizadas baseadas nas interações do usuário.

O trabalho de Santos (2022), analisou a vulnerabilidade de usuários de dispositivos de Internet das Coisas (IoT) frente a ataques de engenharia social, propondo o desenvolvimento de um portal para conscientização voltado para usuários domésticos.

Por outro lado, Cardoso, V. (2024), utiliza a gamificação no desenvolvimento do aplicativo Saphish para conscientização contra ataques de phishing, evidencia que a utilização de elementos lúdicos, como rankings e desafios interativos, aumenta a motivação dos usuários e facilita a retenção de conhecimento, tornando o aprendizado mais envolvente e aplicável ao cotidiano.

3.2 INICIATIVAS EM SEGURANÇA DA INFORMAÇÃO

Além das pesquisas acadêmicas, diversas instituições tanto públicas quanto privados têm desenvolvido iniciativas de conscientização que complementam estratégias defensivas contra ataques de engenharia social. Observam-se as seguintes:

- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br): Mantém a Cartilha de Segurança para Internet, material gratuito que apresenta conceitos básicos, exemplos de golpes e orientações práticas para usuários comuns.
- Escola Virtual de Governo (EV.G): Oferece cursos de capacitação em segurança da informação, gratuitos e com certificado, tendo como público-alvo servidores públicos e cidadãos interessados na temática.
- Setor Privado (KnowBe4 e Kaspersky): Plataformas como a KnowBe4 e o Kaspersky Security Awareness disponibilizam treinamentos personalizados e simulações de phishing para avaliar a vulnerabilidade dos colaboradores e gerar relatórios de desempenho.
- Capacitação Profissional (Clavis e Instituto Brasileiro de Cibersegurança – IBSEC): Oferecem treinamentos focados em técnicas de defesa, boas práticas e fundamentos de cibersegurança.

Observa-se, portanto, que tanto o setor público quanto o privado seguem na mesma direção, na qual a educação é uma ferramenta importante para redução de vulnerabilidades humanas.

4 METODOLOGIA

Nesta seção será apresentado o modo como a pesquisa foi realizada, destacando sua natureza, objetivos, abordagem, método e procedimentos usados, bem como o local de coleta dos dados usados para conseguir os resultados obtidos.

Buscou-se reunir conhecimentos sobre estratégias de conscientização para mitigar a engenharia social, visando oferecer uma fonte de consulta para profissionais da área, gestores, estudantes e demais interessados no tema.

O presente estudo trata-se de uma pesquisa de natureza básica, pois busca ampliar o conhecimento teórico sobre a conscientização em segurança da informação e o combate à engenharia social, sem procurar uma aplicação prática de imediato.

Está sendo utilizada a pesquisa descritiva, visando analisar e revelar as características relacionadas à conscientização em segurança da informação. Além disso, este trabalho possui abordagem qualitativa, pois não se foca na medição de dados, mas na análise e no entendimento de conceitos, práticas e estratégias relacionadas à segurança da informação.

Diante disso, a pesquisa foi realizada por meio da revisão bibliográfica. Conforme definem Marconi e Lakatos (2017, p.57), a pesquisa bibliográfica “é um tipo específico de produção científica: é feita com base em textos, como livros, artigos científicos, ensaios críticos, dicionários, enciclopédias, jornais, revistas, resenhas, resumos”.

O Google Acadêmico foi a principal base de dados utilizada para o levantamento dos trabalhos acadêmicos. A busca se deu por critérios de inclusão, publicações no período de 2022 a 2024, no idioma português, e com relação direta com os temas de segurança da informação, engenharia social, conscientização de usuários ou ataques de phishing. Os trabalhos que não atendiam a esses requisitos foram excluídos automaticamente.

Utilizando os unitermos “Segurança da Informação”, “Engenharia Social”, “Conscientização” e “Phishing”, presentes no conteúdo dos artigos encontrados, combinados, resultou em 277 trabalhos.

Desses, foram pré-selecionados 14 trabalhos conforme a relevância do título. Por fim, após a leitura do resumo e conclusão, foram selecionados 4 artigos para análise final (quadro 1), sendo excluídos os trabalhos que não apresentavam contribuições ou foco do tema definido.

Quadro 1 -Trabalhos selecionados para análise.

Título	Autor/Ano	Foco Principal
Engenharia Social e Técnicas de Defesas: uma abordagem no nível de conhecimento e de conscientização de usuários de dispositivos de Internet das Coisas	Maiara de Castro Santos (2022)	Estudo sobre vulnerabilidades em IoT e proposta de ferramenta informativa para conscientização de usuários contra ataques de engenharia social.
Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira: um estudo de caso	Érica de Souza Pires (2023)	Estudo de caso sobre a eficácia da plataforma KnowBe4 na conscientização de colaboradores de uma cooperativa de crédito.
APSEA: Um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social	Waldson Rodrigues Cardoso (2024)	Desenvolvimento e validação de um sistema especialista para prevenção e conscientização contra ataques de engenharia social.
Saphish: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo Phishing	Victor Wohlers Cardoso (2024)	Desenvolvimento de um aplicativo gamificado para conscientização e treinamento de usuários contra ataques de phishing.

Fonte: Elaborado pelo autor (2025).

Além dos trabalhos acadêmicos, foram consultados livros, relatórios, estatísticas e materiais sobre iniciativas como as ações do CERT.br, Escola Virtual de Governo (EV.G), KnowBe4, entre outras, realizadas por meio de busca na internet de forma geral.

O estudo adota o método hipotético-dedutivo, partindo da premissa de que a educação contínua em segurança da informação é determinante para mitigar a eficácia dos ataques de engenharia social nas organizações.

5 ANÁLISE DE RESULTADOS

Na presente seção, serão apresentados os resultados obtidos visando atender ao objetivo da pesquisa. A partir da análise dos quatro trabalhos selecionados na revisão bibliográfica. A análise dos dados levantados nesta revisão bibliográfica permite uma interpretação crítica sobre como diversas metodologias de conscientização impactam a segurança da informação. Ao comparar os estudos selecionados, notamos que a vulnerabilidade humana frente à engenharia social não é uma constante, mas sim uma variável que pode ser gerenciada por meio de uma educação estruturada.

Assim, a discussão a seguir vai além de simplesmente expor os resultados de cada autor, ela busca integrar seus achados para compreender como as ferramentas tecnológicas e abordagens pedagógicas se combinam para fortalecer o fator humano.

No âmbito corporativo, a eficácia de programas de treinamento contínuo é reforçada pelas evidências trazidas por Pires (2023). Análise desta intervenção em uma cooperativa de crédito demonstra que a exposição frequente a conteúdos de segurança altera significativamente a cultura organizacional. 99,4% dos colaboradores relataram maior segurança no manuseio de dados após o uso da plataforma KnowBe4, sugere que o conhecimento técnico contribui para reduzir a insegurança e aumenta a assertividade na tomada de decisão.

Mais do que a percepção aparente, a mudança comportamental é tangível, a redução drástica no compartilhamento de senhas, apenas 1,7% mantiveram a prática e a recusa em aceitar acessos remotos não verificados, 93,7% indicam que o treinamento cria reflexos defensivos. Isso valida a teoria de que a educação formal transforma o colaborador de um alvo passivo em um agente ativo de defesa.

Entretanto, a literatura analisada aponta que a redução do engajamento em treinamentos tradicionais é um desafio real. Nesse ponto, o trabalho de Cardoso, V. (2024) dialoga diretamente com as limitações dos métodos tradicionais ao introduzir a gamificação. A comparação entre os achados sugere que, enquanto o treinamento corporativo foca na conformidade, a gamificação foca no engajamento.

Com alta adesão ao aplicativo Saphish, impulsionada por sistemas de ranking com 89% de engajamento, revela que mecanismos lúdicos são essenciais para manter a atenção do usuário a longo prazo. Análise desse estudo indica que a interatividade não apenas atrai, mas facilita a retenção cognitiva, 100% dos usuários

afirmaram que os tópicos teóricos gamificados foram fundamentais para resolver os desafios práticos de phishing. Portanto, a gamificação surge não como substituta, mas como um complemento necessário no aprendizado.

A discussão se aprofunda ao considerarmos a personalização da defesa, o estudo de Cardoso, W. (2024), introduz uma evolução na abordagem, o uso de Sistemas Especialistas para diagnóstico. Diferente de treinamentos massivos, a análise via Inteligência Artificial permitiu segmentar o risco humano, identificando que 22,31% dos usuários ainda possuíam vulnerabilidade considerada alta. Com a interpretação deste dado é crucial, demonstra que, mesmo em ambientes controlados, existe uma parcela de usuários que exige atenção diferenciada.

A validação técnica da ferramenta APSEA, com nota máxima em confiabilidade, sugere que a tendência para a redução de engenharia social reside em sistemas adaptativos, capazes de simular o raciocínio de um especialista para corrigir falhas comportamentais específicas de cada indivíduo.

Por fim, a análise estende-se ao contexto da Internet das Coisas (IoT), onde Santos (2022), evidencia uma discrepância entre o conhecimento teórico e a prática segura. Sua pesquisa revela que, embora 87% dos usuários conheçam o termo Engenharia Social, muitos ainda negligenciam configurações básicas de segurança em dispositivos domésticos.

Desse modo, sugere que a conscientização no ambiente de trabalho nem sempre se traduz para a vida pessoal, criando brechas para ataque em home office. O portal proposto pela autora para intervenção educativa, foi bem avaliada com 90% pelos usuários, onde acreditam que o curso oferecido pelo portal influencia de alguma forma na conscientização. Portanto, reforça que a conscientização deve ser onipresente, cobrindo não apenas computadores corporativos, mas todo o ecossistema digital do usuário.

Em síntese, a interpretação conjunta dessas obras permite afirmar que a conscientização é uma ferramenta importante para a redução de ataque humano. As evidências indicam que a combinação de métodos, a formalidade dos processos corporativos, a atratividade da gamificação e a precisão dos sistemas inteligentes cria uma defesa em profundidade. O usuário consciente deixa de ser o elo mais fraco e torna-se a primeira linha de defesa, capaz de identificar irregularidades que escapam muitas vezes aos filtros tecnológicos.

6 CONSIDERAÇÕES FINAIS

Ao longo desta pesquisa, foi possível apresentar um breve panorama de como a conscientização em segurança da informação é essencial no combate à engenharia social, por meio de uma revisão bibliográfica. A partir da interpretação crítica dos estudos selecionados, foi possível confirmar a hipótese inicial de que a educação contínua e estruturada é fundamental para mitigar as vulnerabilidades humanas, que continuam sendo o principal vetor de ataques cibernéticos.

A discussão dos resultados permitiu concluir que não existe uma solução tecnológica isolada para resolver o problema da engenharia social. Portanto, a segurança da informação depende fundamentalmente do comportamento do usuário. Ficou evidenciado que treinamentos corporativos eficazes alteram a cultura de segurança, reduzindo práticas de risco como o compartilhamento de senhas.

Simultaneamente, identificou-se que a eficácia desses treinamentos é potencializada quando se utilizam metodologias ativas, como a gamificação, que combatem o desinteresse e aumentam a retenção do conhecimento através da interatividade e competição saudável.

Além disso, a pesquisa destacou a importância da tecnologia como aliada no processo educativo. O uso de Sistemas Especialistas e Inteligência Artificial para diagnosticar níveis de vulnerabilidade individual mostrou-se uma abordagem promissora, permitindo que as organizações direcionem esforços para os colaboradores mais expostos a risco. Concluiu-se que a conscientização deve ultrapassar as fronteiras do ambiente corporativo, alcançando o contexto doméstico e dispositivos de IoT, visto que a segurança pessoal e organizacional estão cada vez mais entrelaçadas.

Como limitação deste estudo, reconhece-se que a análise se restringiu a dados secundários da literatura, não tendo sido realizada uma aplicação prática inédita pelo autor em um ambiente controlado. Para pesquisas futuras, recomenda-se, a investigação do impacto das novas ferramentas de Inteligência Artificial Generativa como deepfakes de voz e vídeo nas táticas de engenharia social e como os programas de conscientização devem evoluir para preparar os usuários para identificar essas ameaças hiper-realistas. Sugere-se também a realização de estudos de longo prazo para medir se a mudança comportamental adquirida através da gamificação se mantém consistente ao decorrer do tempo.

REFERÊNCIAS

BAIARDI, Leonardo. Fator humano é responsável por 74% dos ataques cibernéticos de 2023. **Security Leaders**, 2024. Disponível em: https://securityleaders.com.br/fator-humano-e-responsavel-por-74-dos-ataques-ciberneticos-de-2023/. Acesso em: 15 jul. 2025.

BUXTON, Oliver. **O que é um ataque de pretexting e como evitá-lo?** Disponível em: https://www.avast.com/pt-br/c-what-is-pretexting. Acesso em: 11 dez. 2025.

CARDOSO, Victor Wohlers. **Saphish**: um aplicativo gamificado para conscientização e treinamento contra ataques cibernéticos do tipo Phishing. 2024.

CARDOSO, Waldson Rodrigues. **APSEA**: um sistema especialista como ferramenta de conscientização e prevenção contra ataques de engenharia social. 2024.

CERT.BR. **Cartilha de Segurança para Internet**: fascículos. Disponível em: https://cartilha.cert.br/fasciculos/. Acesso em: 4 out. 2025.

CIALDINI, Robert B. **As armas da persuasão**. Tradução de Ivo Korytowski. Rio de Janeiro: Sextante, 2012. E-book.

CLAVIS. **Treinamento e conscientização em segurança da informação**. Disponível em: https://clavis.com.br/servicos/treinamento-e-conscientizacao-em-seguranca-da-informacao/. Acesso em: 4 out. 2025.

ESCOLA VIRTUAL GOV. **Plataforma de capacitação a distância para o serviço público brasileiro**. Disponível em: https://www.escolavirtual.gov.br/. Acesso em: 4 out. 2025.

FATTORI. **A importância da conscientização em segurança da informação**. 22 out. 2024. Disponível em: https://fattori.com.br/2024/10/22/a-importancia-da-conscientizacao-em-seguranca-da-informacao/. Acesso em: 15 jul. 2025.

FONTES, Edison Luiz G. **Segurança da informação**. Rio de Janeiro: Saraiva, 2012. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502122185/. Acesso em: 14 jul. 2025.

HADNAGY, Christopher. **Social engineering**: the art of human hacking. Indianapolis: Wiley Publishing, 2011.

IBSEC. **Fundamentos em cibersegurança na prática**. Disponível em: https://conteudo.ibsec.com.br/curso-fundamentos-em-ciberseguranca-na-pratica. Acesso em: 4 out. 2025.

KASPERSKY. **Treinamento de conscientização sobre segurança da informação**. Disponível em: https://www.kaspersky.com.br/enterprise-security/security-awareness. Acesso em: 4 out. 2025.

KNOWBE4: **treinamento de conscientização em segurança cibernética.** Disponível em: https://solonetwork.com.br/cybersecurity/KnowBe4. Acesso em: 4 out. 2025.

KOSINSKI, Matthew. **O que é phishing? | IBM**. Disponível em: https://www.ibm.com/br-pt/think/topics/phishing. Acesso em: 11 jul. 2025.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MARTINS, Maura. **O que é engenharia social e como evitar cair nesse golpe?** Disponível em: https://www.tecmundo.com.br/seguranca/403858-o-que-e-engenharia-social-e-como-evitar-cair-nesse-golpe.htm. Acesso em: 11 dez. 2025.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar**. Tradução de Pearson Education. São Paulo: Pearson Education do Brasil, 2003.

MYERS, David G. **Psicologia**. 9. ed. Rio de Janeiro: LTC, 2012.

MYERS, David G. **Psicologia social**. 10. ed. Porto Alegre: AMGH, 2014.

PIRES, Érica de Souza et al. **Análise do uso da plataforma KnowBe4 para conscientização da segurança da informação em uma instituição financeira**: um estudo de caso. 2023.

PONCE, Silvana. **ISO 27001:2013/ISO 27701:2020 – Sistema de Gestão da Segurança da Informação / Sistema de Gestão da Informação Privada**: panorama geral. São Paulo: QMS Brasil, 2021. Disponível em: https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf. Acesso em: 13 jul. 2025.

SANTOS, Maiara de Castro. **Engenharia social e técnicas de defesas**: uma abordagem no nível de conhecimento e de conscientização de usuários de dispositivos de Internet das Coisas. 2022.

SEABRA, David Bacelar Costa. **A exposição demasiada das informações em redes sociais digitais e o crescimento do phishing**. 2025. 127 f. Dissertação (Mestrado em Modelagem e Simulação de Biossistemas) – Universidade do Estado da Bahia, Alagoinhas, 2025.

SOUZA, Ramon. **Baiting: o que é este golpe de engenharia social**. Disponível em: https://conteudo.eskive.com/pt-br/baiting-o-que-eeste-golpe-de-engenharia-social. Acesso em: 11 jul. 2025.

TURBAN, Efraim; VOLONINO, Linda. **Tecnologia da informação para gestão**. 8. ed. Porto Alegre: Bookman, 2013. E-book. p.211. ISBN 9788582600160. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788582600160/. Acesso em: 10 dez. 2025.

UNIVERSIDADE DO ESTADO DA BAHIA - UNEB
DEPARTAMENTO DE CIÊNCIAS EXATAS E DA TERRA – CAMPUS II
CURSO: BACHARELADO DE SISTEMAS DE INFORMAÇÃO
COMPONENTE CURRICULAR: TRABALHO DE CONCLUSÃO DE CURSO

ATA DA SESSÃO DE DEFESA PÚBLICA DE TRABALHO DE CONCLUSÃO DE CURSO, DO CURSO DE BACHARELADO DE SISTEMAS DE INFORMAÇÃO DO SEGUNDO SEMESTRE 2025

No dia **três de dezembro de dois mil e vinte cinco**, às **dez horas e trinta minutos**, no auditório do Pôs Critica – Campus II, Universidade Estado da Bahia - UNEB, reuniu-se a Banca Examinadora composta pelo(a) professor(a) **Elaine Garrido** (professora convidada), professor (a) **José Roberto de Araújo Fontoura** (presidente da banca e professor orientador) e professor(a) **Bruno Cardoso** (professor convidado), para avaliar o Trabalho de Conclusão de Curso (artigo acadêmico), do(a) discente **Clevison da Silva Ferreira** intitulado **"Conscientização em Segurança da Informação no Combate a Engenharia Social"**. O presidente da Banca Examinadora abriu a sessão com os cumprimentos ao(a) candidato(a), aos demais membros da banca, esclarecendo, também, o caráter do evento e respectivas normas. A seguir, foi concedida a palavra ao autor do trabalho para apresentação por vinte minutos. Após esta exposição, os membros da Banca Examinadora realizaram suas considerações emitindo sugestões ao trabalho apresentado e em seguida à palavra foi devolvida ao(a) candidato(a). Após as necessárias considerações ao trabalho, a banca examinadora reuniu-se e os (as) professores(as) atribuíram nota **8,1**. Para registro e finalidades legais, eu **Prof. Fabricio Santos de Faro**, professor da disciplina TCC, lavrei a presente Ata.

Alagoinhas, 03 de dezembro de 2025.

Profº. Fabrício Santos de Faro
Professor de TCC