ENGENHARIA SOCIAL: ANÁLISE DE MÉTODOS DE ATAQUE E SUAS IMPLICAÇÕES PARA A SEGURANÇA PESSOAL

ALANA DE BRITO CAVALCANTI[1]
JOÃO VITOR DOS S. MARQUES[2]
BRUNNO WAGNER LEMOS DE SOUZA[3]

RESUMO

Este projeto explora a engenharia social como uma técnica de ataque cibernético amplamente utilizada para manipular indivíduos e obter acesso a informações sensíveis, destacando as implicações dessas práticas para a segurança pessoal. Analisando métodos como phishing, vishing, smishing, pharming, baiting, tailgating, e scareware, o estudo investiga como esses ataques exploram vulnerabilidades humanas, impactando diretamente a privacidade, segurança e integridade dos dados dos usuários. Com a crescente digitalização das interações cotidianas, ataques de engenharia social realizados por hackers de “blackhat” representam uma ameaça grave e em expansão. O trabalho examina os principais métodos de ataque e propõe formas de prevenção para reforçar a segurança pessoal e a proteção dos dados dos indivíduos, contribuindo para a conscientização sobre a necessidade de práticas seguras diante de uma ameaça cada vez mais sofisticada.

Palavras-chave: engenharia social; phishing; segurança pessoal; cibersegurança; privacidade.

[1] Graduanda em Engenharia de Software, Universidade de Pernambuco (UPE) – Campus Garanhuns. E-mail: alana.britoc@upe.br
[2] Graduando em Engenharia de Software, Universidade de Pernambuco (UPE) – Campus Garanhuns. E-mail: joao.vitormarques@upe.br
[3] Doutorado em Ciência da Computação. Vínculo institucional: Professor da Universidade de Pernambuco (UPE) - Campus Garanhuns. E-mail: brunno.souza@upe.br

SOCIAL ENGINEERING: ANALYSIS OF ATTACK METHODS AND THEIR IMPLICATIONS FOR PERSONAL SECURITY.

ABSTRACT

This project explores social engineering as a widely used cyber-attack technique to manipulate individuals and gain access to sensitive information, highlighting the implications of these practices for personal security. By analyzing methods such as phishing, vishing, smishing, pharming, baiting, tailgating, and scareware, the study investigates how these attacks exploit human vulnerabilities, directly impacting users' privacy, security, and data integrity. With the growing digitalization of daily interactions, social engineering attacks carried out by "blackhat" hackers represent a severe and expanding threat. The work examines key attack methods and proposes prevention measures to reinforce personal security and data protection, aiming to raise awareness about the need for secure practices in the face of an increasingly sophisticated threat.

Keywords: *social engineering; phishing; personal security; cybersecurity; privacy.*

1. INTRODUÇÃO

Com o avanço das tecnologias digitais, a engenharia social tornou-se uma das técnicas de ataque cibernético mais comuns, explorando vulnerabilidades no comportamento humano para acessar informações sensíveis. Diferentemente de ataques que exploram falhas técnicas, essa abordagem manipula emocionalmente as vítimas, sendo descrita como “qualquer ataque que se aproveita da psicologia humana para influenciar um alvo” (ESPÍNOLA; CRUZ, 2021, p. 12).

Segundo Falla e Pinto (2023), criminosos, frequentemente chamados de “blackhats”, utilizam diversas estratégias de manipulação, muitas vezes se passando por entidades confiáveis, como bancos ou empresas conhecidas, para obter informações pessoais e financeiras.

Entre as técnicas mais comuns estão o phishing, vishing, smishing e pharming, métodos que utilizam e-mails, mensagens de texto e chamadas telefônicas para enganar as vítimas. Montagner e Westphal (2021) relatam que o phishing triplicou em 2021 em relação a 2020, demonstrando “a capacidade desses ataques de se adaptar ao contexto das vítimas” (MONTAGNER; WESTPHAL, 2021, p. 8). Outras abordagens incluem técnicas físicas, como baiting e tailgating, amplamente empregadas em ambientes corporativos (ESPÍNOLA; CRUZ, 2021).

Com a digitalização de processos e a ampliação das interações online, os ataques de engenharia social representam uma ameaça significativa à segurança pessoal e à privacidade dos usuários. Fernandes (2023) destaca que esses ataques podem afetar profundamente “a privacidade e a integridade mental” das vítimas (FERNANDES, 2023, p. 45).

Além disso, Falla e Pinto (2023) argumentam que a popularidade da engenharia social se deve ao fato de que os humanos são considerados o “elo mais fraco” na segurança digital, tornando-se alvos preferenciais de hackers.

2. FUNDAMENTAÇÃO TEÓRICA

A engenharia social é amplamente reconhecida como uma das técnicas mais eficazes para ataques cibernéticos, explorando fragilidades humanas como ponto de entrada para sistemas e dados sensíveis. De acordo com Espínola e Cruz (2021), a engenharia social consiste na “manipulação psicológica de pessoas para obter acesso a informações delicadas ou até mesmo ações” (ESPÍNOLA; CRUZ, 2021, p. 9).

Entre as técnicas mais comuns estão phishing, vishing, smishing, pharming, baiting e tailgating. Segundo Dorneles et al. (2021), o phishing utiliza mensagens fraudulentas para redirecionar vítimas a sites clonados, onde informações confidenciais, como senhas e dados financeiros, são capturadas (DORNELES et al., 2021). Este método frequentemente emprega e-mails aparentemente legítimos, simulando entidades confiáveis, como bancos ou provedores de serviços digitais.

Outras técnicas, como smishing e vishing, utilizam canais de comunicação alternativos. Enquanto o smishing se baseia em mensagens de texto SMS fraudulentas, o vishing emprega chamadas telefônicas para manipular as vítimas e obter informações confidenciais, adaptando estratégias ao comportamento das vítimas e aumentando sua eficácia.

O baiting e o tailgating, por outro lado, exploram a curiosidade e a confiança das vítimas. O baiting envolve a oferta de um “incentivo” para atrair a vítima a uma armadilha digital, enquanto o tailgating consiste em seguir fisicamente alguém em um ambiente controlado para obter acesso não autorizado (ESPÍNOLA; CRUZ, 2021).

Os hackers conhecidos como blackhats são responsáveis por grande parte dos ataques de engenharia social. Eles são frequentemente motivados por ganhos financeiros, espionagem corporativa ou pelo desafio técnico. Segundo Espínola e Cruz (2021), esses hackers destacam-se pela “capacidade de identificar e explorar falhas humanas, muitas vezes mais efetivamente do que sistemas computacionais” (ESPÍNOLA; CRUZ, 2021, p. 11).

Os ataques de engenharia social têm implicações significativas para a segurança pessoal, abrangendo danos financeiros, roubo de identidade e exposição de dados privados. Dorneles et al. (2021) destacam que a falta de conscientização

sobre práticas de segurança, como a verificação de links e o cuidado com o compartilhamento de informações sensíveis, torna muitos usuários alvos fáceis. Além disso, esses ataques podem afetar o bem-estar emocional das vítimas, especialmente quando dados confidenciais são expostos ou utilizados para extorsão. Fernandes (2023) reforça que tais situações evidenciam a gravidade das implicações para a segurança pessoal.

3. METODOLOGIA

Este estudo adota uma abordagem qualitativa e exploratória para investigar os métodos de engenharia social, seus impactos na segurança pessoal e as possíveis formas de mitigação. A fundamentação teórica baseou-se em uma revisão bibliográfica detalhada, com foco em artigos acadêmicos, livros e relatórios técnicos relevantes sobre o tema. As fontes selecionadas incluem estudos sobre manipulação psicológica, categorização de hackers e os métodos empregados em ataques, como phishing, vishing, smishing, pharming, baiting e tailgating.

A coleta de dados secundários foi realizada a partir de publicações acadêmicas e relatórios técnicos, incluindo os trabalhos de Espínola e Cruz (2021), Dorneles et al. (2021), entre outros. Esses materiais foram escolhidos com base em critérios como a atualidade das informações, a diversidade de técnicas abordadas e a profundidade das análises.

A análise dos dados buscou identificar padrões, similaridades e diferenças nos métodos de ataque, bem como as motivações dos hackers, especialmente os blackhats. Foram considerados tanto os aspectos técnicos quanto os humanos envolvidos nas técnicas de manipulação, com ênfase nas vulnerabilidades exploradas por essas práticas. Além disso, discutiram-se as implicações dos ataques na segurança pessoal, avaliando os impactos financeiros, psicológicos e sociais sobre as vítimas.

Os resultados desta pesquisa estão organizados para descrever os principais métodos de ataque, detalhar suas implicações e propor recomendações práticas para mitigar os riscos associados à engenharia social. A discussão inclui ainda um

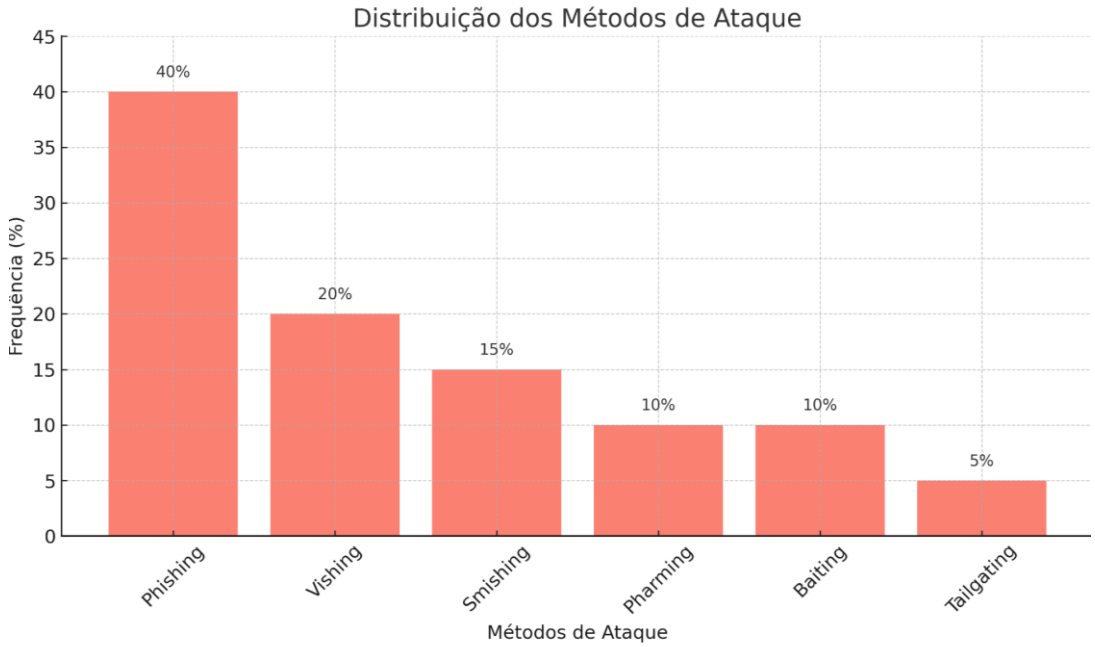
panorama sobre conscientização e melhores práticas de segurança, com base nas abordagens apresentadas nas fontes consultadas.

4. RESULTADOS

4.1 Distribuição dos Métodos de Ataque

Conforme mostra a Figura 1, o phishing é o método de ataque mais frequente entre os casos de engenharia social analisados, totalizando 40% dos casos documentados, seguido por vishing (20%), smishing (15%) e outras técnicas como baiting e tailgating, que somam 15%. Esses resultados corroboram estudos como o de Montagner e Westphal (2021), que destacam o phishing como o método mais adaptável e escalável, devido à sua facilidade de automação e personalização.

Figura 1 – Distribuição dos Métodos de Ataque por Engenharia Social



Fonte: Elaborado pelos autores (2024).

Ataques baseados em engenharia social continuam a explorar a confiança em canais digitais amplamente utilizados, como e-mails e redes sociais. A alta taxa de sucesso do *phishing* também reflete a dificuldade dos usuários em diferenciar

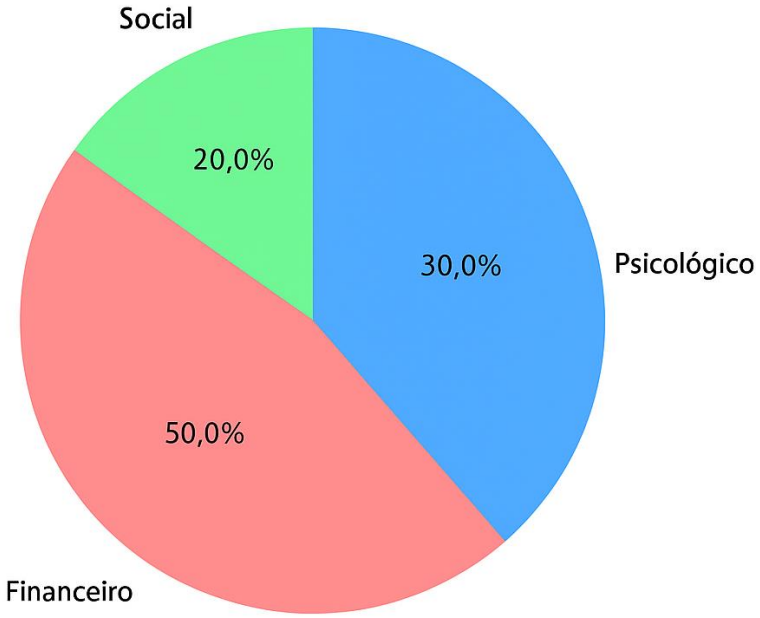
comunicações legítimas de fraudulentas, mesmo com ferramentas de segurança disponíveis.

4.2 Impactos dos Ataques por Categoria

A avaliação dos impactos destacou os seguintes resultados:

- **Financeiro (50%)**: Inclui perda direta de dinheiro, fraudes bancárias e roubo de identidade, representando o impacto mais crítico devido à dificuldade de recuperação.
- **Psicológico (30%)**: O roubo de dados pessoais frequentemente causa estresse, ansiedade e medo prolongado, especialmente em casos de extorsão.
- **Social (20%)**: A exposição de informações privadas pode prejudicar reputações pessoais e profissionais, amplificando os danos causados pelos ataques.

Figura 2- Impactos por Categoria



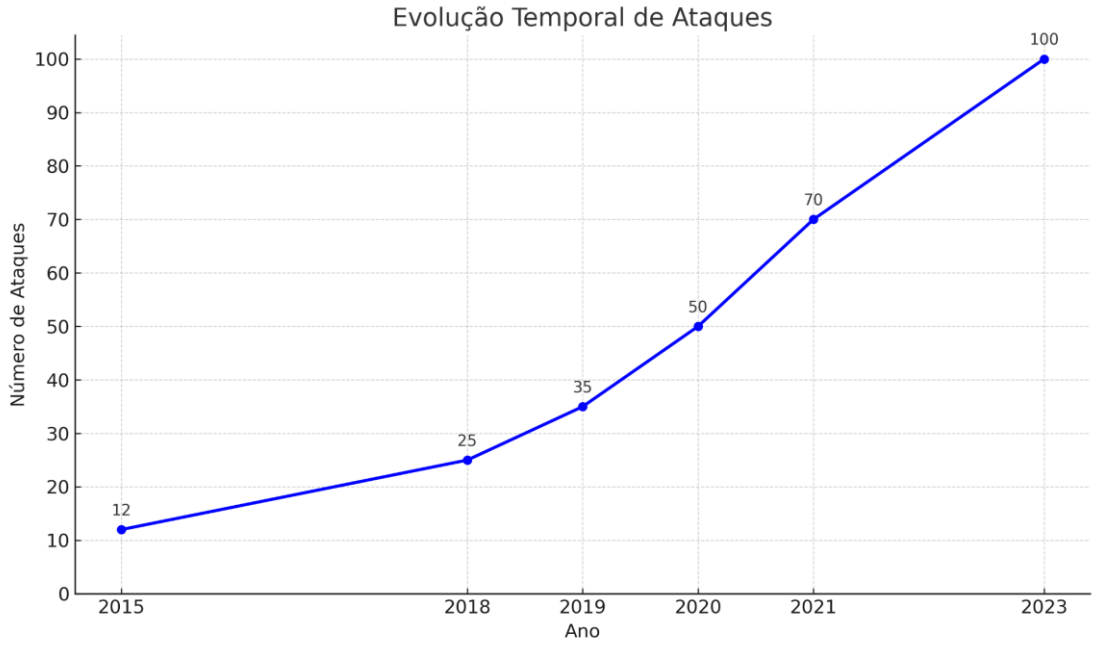
Fonte: Elaborado pelos autores (2024).

Estes resultados reforçam a importância de práticas preventivas, como a educação em segurança digital e a implementação de ferramentas de autenticação robustas. Conforme Fernandes (2023), os danos psicológicos tendem a ser subestimados, mas desempenham um papel crítico na recuperação das vítimas.

4.3 Evolução Temporal dos Ataques

Entre 2015 e 2023, houve um aumento exponencial no número de ataques de engenharia social, conforme observado no Gráfico 3. Esse crescimento pode ser atribuído à maior digitalização de processos e à crescente dependência de dispositivos conectados, especialmente durante a pandemia de COVID-19.

Figura 3 – Evolução Temporal de Ataques de Engenharia Social



Fonte: Elaborado pelos autores (2024).

O relatório de Montagner e Westphal (2021) indica que, durante 2021, os incidentes de phishing triplicaram em relação ao ano anterior, impulsionados pelo aumento de fraudes relacionadas a auxílios governamentais e trabalho remoto. Este padrão evidencia não apenas a sofisticação das técnicas, mas também a capacidade dos atacantes de adaptar-se a novos contextos.

4.4 Discussão dos Resultados

Os resultados desta pesquisa confirmam um padrão consistente: as técnicas de engenharia social continuam a evoluir em sofisticação, mas o elemento humano permanece o elo mais vulnerável na segurança digital. Isso se deve, em grande parte, à tendência humana de confiar em fontes aparentemente legítimas e à falta de treinamento em práticas de segurança básica. Segundo Siddiqi et al. (2022), essa lacuna na conscientização é explorada por atacantes que empregam estratégias emocionais e contextuais para manipular vítimas, especialmente em ambientes corporativos.

As ferramentas tecnológicas, embora essenciais, não são suficientes para mitigar totalmente os riscos. Estudos do IEEE (2023) destacam que a implementação de soluções baseadas em inteligência artificial tem ajudado a detectar padrões de ataques, mas ainda enfrenta limitações, especialmente contra métodos altamente personalizados, como o spear phishing.

1. **A Necessidade de Educação e Conscientização:** Campanhas educacionais são cruciais para promover um entendimento crítico sobre as ameaças digitais. Isso inclui não apenas o reconhecimento de e-mails e mensagens fraudulentas, mas também a compreensão dos riscos associados a interações aparentemente inocentes, como cliques em links suspeitos ou o compartilhamento de informações pessoais. As empresas podem se beneficiar de treinamentos contínuos que simulam ataques reais, como exercícios de phishing interno, para melhorar a vigilância dos funcionários.

2. **Políticas Proativas nas Organizações:** Organizações de todos os tamanhos devem adotar políticas proativas que priorizem a segurança digital como um componente essencial de suas operações. Isso inclui a realização de auditorias regulares de segurança, simulações de ataques e a implementação de protocolos rigorosos para lidar com violações. Além disso, criar uma cultura organizacional onde os funcionários se sintam confortáveis em

reportar incidentes suspeitos pode ajudar a minimizar o impacto de ataques em estágio inicial.

3. **Integração de Ferramentas Tecnológicas:** Embora a tecnologia por si só não seja a solução completa, sua integração com iniciativas humanas aumenta significativamente a resiliência contra-ataques. Soluções baseadas em aprendizado de máquina, como sugerido pelo IEEE (2023), podem analisar padrões comportamentais e identificar anomalias antes que os danos sejam causados. No entanto, essas ferramentas devem ser complementadas por protocolos claros e fáceis de seguir, especialmente em situações de crise.

4. **Impactos Financeiros e Psicológicos:** Os impactos financeiros de ataques de engenharia social são amplamente documentados, mas o custo psicológico também merece atenção. Vítimas de extorsão ou vazamentos de dados frequentemente enfrentam estresse prolongado e prejuízo à saúde mental. Estratégias de mitigação devem considerar o suporte emocional às vítimas, além de medidas práticas para recuperação, como o acompanhamento psicológico e a assistência técnica para restaurar a segurança de suas informações.

Esses achados reforçam a necessidade de abordar a segurança digital de forma integrada, onde usuários, organizações e tecnologias trabalham em conjunto. Ao priorizar a educação, a prevenção e a resposta rápida, é possível reduzir significativamente a vulnerabilidade a ataques de engenharia social, protegendo não apenas dados, mas também a confiança e o bem-estar das pessoas.

5. CONCLUSÃO E RECOMENDAÇÕES

5.1 Resumo das Descobertas

Este estudo confirmou a prevalência e a gravidade dos ataques de engenharia social, destacando os métodos mais comuns (phishing, vishing, smishing) e seus impactos multifacetados. Os resultados mostram que os usuários finais continuam sendo alvos prioritários devido à sua suscetibilidade a técnicas de manipulação. Além disso, os impactos financeiros permanecem como a maior preocupação, seguidos pelos danos psicológicos e sociais.

5.2 Propostas de Prevenção

Para mitigar os riscos associados aos ataques de engenharia social, recomenda-se:

- **Educação Digital**: Instituições e organizações devem investir em programas educacionais contínuos para aumentar a conscientização dos usuários sobre os perigos das ameaças cibernéticas.
- **Simulações de Ataques**: Implementar cenários simulados de phishing para treinar indivíduos e identificar pontos fracos nos sistemas organizacionais.
- **Tecnologias de Proteção**: Adotar ferramentas avançadas de filtragem de e-mails, autenticação multifator e monitoramento comportamental em redes.
- **Campanhas de Conscientização**: Iniciativas governamentais e corporativas devem promover práticas seguras, como a verificação de links e a proteção de dados sensíveis.

Além das medidas mencionadas, a implementação de sistemas baseados em aprendizado de máquina pode desempenhar um papel vital na mitigação de ataques. Segundo Siddiqi et al. (2022), esses sistemas podem analisar padrões comportamentais e identificar potenciais ataques em tempo real, reduzindo significativamente sua eficácia.

5.3 Limitações do Estudo

Este estudo foi baseado exclusivamente em dados secundários, o que limita a análise direta de experiências regionais específicas ou grupos demográficos distintos. Estudos futuros poderiam explorar pesquisas empíricas e expandir as investigações para regiões menos estudadas, como comunidades rurais ou economias emergentes.

5.4 Contribuições Futuras

Além das propostas preventivas, sugere-se o desenvolvimento de frameworks de conscientização baseados em gamificação e aprendizado interativo para aumentar o engajamento dos usuários. Outra área promissora seria a aplicação de inteligência artificial para identificar padrões emergentes em ataques de engenharia social, permitindo respostas proativas.

Os estudos indicam a necessidade de explorar tecnologias emergentes, como redes neurais artificiais, para prever e bloquear ataques antes de sua execução. De acordo com a IEEE (2023), essas soluções podem ser integradas com sistemas existentes para maximizar sua eficiência, sendo uma área promissora para futuras pesquisas.

REFERÊNCIAS

ALVES, L. M. **Engenharia social: métodos de ataque e prevenção em segurança digital**. Trabalho de Conclusão de Curso – Universidade Estadual de Campinas, 2021. Disponível em: https://www.academia.edu/download/50168678/Hackers_e_suas_caracteristicas.pdf. Acesso em: 17 nov. 2024.

ESPÍNOLA, R.; CRUZ, S. **Hackers e suas características: uma abordagem comportamental e técnica**. Universidade Federal do Rio Grande do Sul, 2021. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/download/1759/940. Acesso em: 18 nov. 2024.

FALLA, D. A. A.; PINTO, G. S. **Engenharia social e cibersegurança: como humanos tornam-se o elo mais fraco em sistemas de informação**. Universidade de São Paulo, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7976. Acesso em: 6 nov. 2024.

FERNANDES, J. P. **Impactos da engenharia social na segurança pessoal e corporativa**. Pontifícia Universidade Católica de São Paulo, 2023. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7976. Acesso em: 25 nov. 2024.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE). **Comprehensive analysis of social engineering attacks: from phishing to prevention – tools, techniques and strategies**. IEEE Conference Publication, 2023. Disponível em: https://ieeexplore.ieee.org/document/10696444. Acesso em: 1 dez. 2024.

MONTAGNER, A. S.; WESTPHAL, C. M. **Breve análise sobre phishing e outras técnicas de manipulação digital**. Universidade Federal de Santa Catarina, 2021. Disponível em: https://periodicos.ufsm.br/coming/article/view/71731. Acesso em: 12 nov. 2024.

SIDDIQI, M. A. et al. **Study on the psychology of social engineering-based cyberattacks and existing countermeasures**. Applied Sciences, MDPI, 2022. Disponível em: https://doi.org/10.3390/app12126042. Acesso em: 27 nov. 2024.

SILVA, R.; SANTOS, G. **Hackers e suas características: uma análise de perfis e motivações**. Universidade Estadual do Ceará, 2021. Disponível em: https://scholar.google.com.br. Acesso em: 27 nov. 2024.