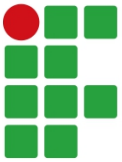


INSTITUTO FEDERAL
São Paulo
Campus Campinas

DANIELE ALVES DA COSTA

O IMPACTO DE ATAQUES DE ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO: IDENTIFICAÇÃO DE VULNERABILIDADES NA GESTÃO ORGANIZACIONAL

CAMPINAS
2025

DANIELE ALVES DA COSTA

O IMPACTO DE ATAQUES DE ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO: IDENTIFICAÇÃO DE VULNERABILIDADES NA GESTÃO ORGANIZACIONAL

Trabalho de Conclusão de Curso apresentado como parte dos requisitos para obtenção do diploma do Curso Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia Campus Campinas.

Orientador: José Américo dos Santos Mendonça

CAMPINAS

2025

FICHA CATALOGRÁFICA
Biblioteca IFSP – Campus Campinas
Tatiane Helena Borges de Salles
CRB8/8946

Costa, Daniele Alves da.

O impacto de ataques de engenharia social na segurança da informação : identificação de vulnerabilidades na gestão organizacional / Daniele Alves da Costa. – 2025.
68 f. il.

Trabalho de Conclusão de Curso (Graduação em Tecnologia em Análise e Desenvolvimento de Sistemas) – Instituto Federal de Educação, Ciência e Tecnologia do Estado de São Paulo, Campinas, SP, 2025 .

Orientador(a): José Américo dos Santos Mendonça.

1. Engenharia social. 2. Segurança da informação. 3. Conscientização. 4. Prevenção. . I. Orientador(a) José Américo dos Santos Mendonça. II. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. III. Título.

Ministério da Educação
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
Campus Campinas
FUC CURSO SUP TEC ADS

ATA N.º 19/2025 - TADS-CMP/DAE-CMP/DRG/CMP/IFSP

Ata de Defesa de Trabalho de Conclusão de Curso - Graduação

Na presente data, realizou-se a sessão pública de defesa do Trabalho de Conclusão de Curso intitulado O IMPACTO DE ATAQUES DE ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO: IDENTIFICAÇÃO DE VULNERABILIDADES NA GESTÃO ORGANIZACIONAL apresentado(a) pelo(a) aluno(a) Daniele Alves da Costa CP3020142 do Curso **SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS (Campus Campinas).** Os trabalhos foram iniciados às 19:00hs pelo(a) Professor(a) presidente da banca examinadora, constituída pelos seguintes membros:

Membros	IES	Presença (Sim/Não)
JOSÉ AMÉRICO S. MENDONÇA	IFSP	SIM
ZADY CASTAÑEDA SALAZAR	IFSP	SIM
FÁBIO FELICIANO DE OLIVEIRA	IFSP	SIM

Observações:

A banca examinadora, tendo terminado a apresentação do conteúdo da monografia, passou à arguição do(a) candidato(a). Em seguida, os examinadores reuniram-se para avaliação e deram o parecer final sobre o trabalho apresentado pelo(a) aluno(a), tendo sido atribuído o seguinte resultado:

[x] Aprovado(a)

[ ] Reprovado(a)

Proclamados os resultados pelo presidente da banca examinadora, foram encerrados os trabalhos e, para constar, eu lavrei a presente ata que assino juntamente com os demais membros da banca examinadora.

Campus Campinas, 24 de outubro de 2025

Documento assinado eletronicamente por:

- **Jose Americo dos Santos Mendonca**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 24/10/2025 18:11:06.
- **Fabio Feliciano de Oliveira**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 28/10/2025 21:25:23.
- **Zady Castaneda Salazar**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 29/10/2025 15:00:28.

Este documento foi emitido pelo SUAP em 24/10/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsp.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 1052832
Código de Autenticação: c8c8c0836e

DEDICATÓRIA

Dedico este trabalho à minha família, aos colegas, professores e servidores do Instituto que colaboraram em minha jornada formativa. Dedico, em especial, ao meu irmão Gabriel Costa, que sempre me apoiou e foi minha maior e mais próxima inspiração no universo acadêmico.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pela dádiva da vida, pela sabedoria concedida ao longo desta jornada, pela oportunidade de concluir mais uma etapa de minha experiência acadêmica e por ter me fortalecido nos momentos de dificuldade.

Agradeço aos meus queridos pais, Aparecida e Nelson, pelo amor e apoio incondicional. Ao meu querido irmão, Gabriel Costa, pelo incentivo, união e parceria em todos os momentos. E ao meu namorado, Gustavo, pelo carinho, paciência, pelo apoio, por acreditar em mim e por ser meu porto seguro durante toda essa trajetória. Agradeço imensamente por fazerem parte desse sonho e me ajudarem a torná-lo realidade.

Agradeço também à minha família e amigos pelo apoio incondicional e pelas palavras de incentivo.

Agradeço ao meu orientador pela paciência e pela dedicação ao longo da produção deste trabalho.

Agradeço a todos os professores e servidores do IFSP Campus Campinas, que contribuíram de maneira direta e indireta para a conclusão deste trabalho.

EPÍGRAFE

"Conhece-te a ti mesmo e conhecerás o universo e os deuses."

Sócrates

RESUMO

Este trabalho tem como tema o impacto dos ataques de engenharia social na segurança da informação, com ênfase na identificação de vulnerabilidades humanas exploradas por agentes maliciosos. O objetivo principal foi compreender como esses ataques ocorrem, destacando seus tipos mais comuns, além de apresentar estudos de caso exploratórios, estatísticas atualizadas e recomendações eficazes de prevenção. O estudo caracterizou-se como uma pesquisa bibliográfica e exploratória, desenvolvida a partir de revisão bibliográfica e documental. A análise evidenciou que os ataques de engenharia social continuam crescendo em frequência e sofisticação, sendo responsáveis por grande parte das violações de segurança registradas no mundo. O estudo apontou que o fator humano permanece sendo o elo mais vulnerável na cadeia da segurança da informação, o que reforça a necessidade de medidas preventivas. Verificou-se que, embora existam ferramentas e sistemas de proteção avançados, esses recursos não são suficientes para impedir ataques baseados em manipulação psicológica. Conclui-se que o enfrentamento da engenharia social exige uma abordagem voltada à conscientização, à capacitação dos usuários e ao fortalecimento da cultura de segurança, a fim de reduzir os impactos desses ataques no ambiente organizacional e social.

Palavras-chave: engenharia social; segurança da informação; fator humano; conscientização; prevenção.

ABSTRACT

This paper addresses the impact of social engineering attacks on information security, with an emphasis on identifying human vulnerabilities exploited by malicious actors. The main objective was to understand how these attacks occur, highlighting the most common types, as well as presenting case studies, updated statistics, and effective prevention methods. The study is characterized as qualitative and exploratory research, based on bibliographic and documentary review. The analysis showed that social engineering attacks continue to increase in frequency and sophistication, accounting for a significant portion of security breaches worldwide. The research indicated that the human factor remains the weakest link in the information security chain, reinforcing the need for preventive measures. It was found that although advanced protection tools and systems exist, they are not sufficient to prevent attacks based on psychological manipulation. It is concluded that addressing social engineering requires an approach focused on user awareness, training, and strengthening of the security culture in order to reduce the impacts of such attacks in organizational and social environments.

Keywords: social engineering; information security; human factor; awareness; prevention.

LISTA DE FIGURAS

Figura 1 - Tríade de requisitos de seguranças..... 24
Figura 2 - Fases que comumente um Engenheiro Social percorre..... 28
Figura 3 - Exemplo de Ataque de Phishing em massa..... 34
Figura 4 - Manchete do portal O TEMPO sobre hacker acusado de facilitar roubo ao BC..... 39
Figura 5 - Manchete do portal Security Report sobre tentativa de invasão ao Siafi.. 41
Figura 6 - Página “Fascículos” da Cartilha de Segurança para Internet..... 54
Figura 7 - Cartilha “Guia para Proteção de Conhecimentos Sensíveis”.....55
Figura 8 - Cartilha “Segurança da Informação para Agentes de Tratamento de Pequeno Porte”..... 56

LISTA DE GRÁFICOS

Gráfico 1: Elementos chave listados em violações..... 46
Gráfico 2: Principais incidentes de Engenharia Social..... 47
Gráfico 3: Incidentes de fraude reportados ao CERT.br.....50

LISTA DE QUADROS

Quadro 1: Violações envolvendo engenharia social..... 46
Quadro 2 - Incidência de incidentes em pequenas e médias organizações..... 48

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
BC	Banco Central
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CID	Confidencialidade, Integridade e Disponibilidade
CNN	Cable News Network
CSIRT	Computer Security Incident Response Team
DBIR	Data Breach Investigations Report ou Relatório de Investigações de Vazamento de Dados
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
E-MAIL	Messages electronically ou Correio Eletrônico
ETA	Education, Training and Awareness
FBI	Federal Bureau of Investigation
IA	Inteligência Artificial
IBM	International Business Machines Corporation
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission ou Organização Internacional de Padronização/Comissão Eletrotécnica Internacional
LGPD	Lei Geral de Proteção de Dados
MFA	Multi-Factor Authentication
NBR	Norma Brasileira
PIX	Sistema Brasileiro de Pagamentos e Transferências Instantâneas
PSTI	Provedor de Serviços de Tecnologia da Informação
QI	Quociente de Inteligência
QR Code	Quick Response Code ou Código de Resposta Rápida
SI	Segurança da Informação
SMS	Short Message Service ou Serviço de Mensagem Curta
SPF	Sender Policy Framework
TCU	Tribunal de Contas da União

TI	Tecnologia da Informação
WEF	World Economic Forum

SUMÁRIO

1 INTRODUÇÃO..... 16
2 OBJETIVOS..... 19
2.1 Objetivo Geral..... 19
2.2 Objetivos Específicos..... 19
3 FUNDAMENTAÇÃO TEÓRICA..... 20
3.1 Vulnerabilidade..... 20
3.2 Manipulação Psicológica..... 20
3.3 Engenharia Social..... 22
3.4 Segurança da Informação: Definição e sua importância..... 23
3.5 Pilares da Segurança da Informação..... 23
3.6 Lei Geral de Proteção de Dados Pessoais (LGPD)..... 25
3.7 Vulnerabilidades na Gestão Organizacional..... 25
3.8 Ataques de Engenharia Social - Um risco ainda subestimado..... 26
3.8.1 Os riscos do fator humano em segurança da informação..... 27
3.8.2 Etapas da Engenharia Social - Como os ataques acontecem?..... 28
3.8.3 Abordagem sobre o comportamento humano..... 28
3.8.4 Abordagem tecnológica..... 29
4 METODOLOGIA..... 32
4.1 Abordagem do Estudo..... 32
4.2 Procedimentos Metodológicos Planejados..... 32
4.3 Limitações do Estudo..... 33
5 TÉCNICAS DE ENGENHARIA SOCIAL..... 35
5.1 Subdivisões de ataques de phishing..... 35
5.2 Pretexting..... 37
5.3 Baiting..... 38
5.4 Quid Pro Quo..... 38
6 ESTUDOS DE CASO EXPLORATÓRIOS..... 39
6.1 Ataque ao sistema financeiro no Banco Central..... 39
6.2 Invasão ao Sistema Integrado de Administração Financeira do Governo Federal SIAFI..... 41
6.3 MGM Resorts (2023)..... 43
6.4 CDK Global (2024)..... 44
6.5 Arup (2024)..... 44
6.6 Ataque de Phishing e Lavagem de Dinheiro (2021)..... 45
7 ABORDAGEM ANALÍTICA E ESTATÍSTICA GERAL DE RELATÓRIOS..... 46
7.1 Perspectiva global de vazamento de dados..... 46
7.2 Panorama Brasileiro de Incidentes Cibernéticos..... 52
8 ESTRATÉGIAS DE PROTEÇÃO E PREVENÇÃO CONTRA ATAQUES DE ENGENHARIA SOCIAL..... 54

8.1 Educação, Treinamento e Conscientização (ETA)..... 54
8.2 Autenticação Multifator (MFA)..... 55
8.3 Filtragem de E-mails e Proteção de Domínios..... 55
8.4 Controles de Acesso e Princípio do Menor Privilégio.....56
8.5 Procedimentos de Relato e Resposta a Incidentes..... 56
8.6 Cartilha - Guia de Boas Práticas Individuais..... 57
10 CONCLUSÃO..... 61
11 REFERÊNCIAS..... 63

1 INTRODUÇÃO

A informação tornou-se um dos recursos mais importantes para os indivíduos e organizações na Era digital, no que diz respeito à segurança e estratégia (Sêmola, 2014). Antigamente, a informação era limitada e o conhecimento circulava lentamente, por outro lado, atualmente, observa-se o que Manuel Castells (1999) denominou como “sociedade em rede”, na qual o valor está na capacidade de acessar, processar e distribuir conhecimento em tempo real. Nesse novo paradigma, a informação se tornou não apenas um insumo, mas também uma mercadoria, uma moeda e um alvo.

Por meio da comparação com períodos anteriores, no modelo industrial fordista, por exemplo, a eficiência estava associada à repetição, ao controle de processos físicos e à hierarquia rígida. Em contrapartida, na era digital, a vantagem competitiva decorre da capacidade de captar, armazenar, analisar e proteger dados, especialmente os dados pessoais e comportamentais, cuja exploração alimenta desde campanhas de marketing até decisões políticas. A informação é conceituada como “dados contextualizados”, e seu valor está diretamente relacionado à maneira como é interpretada e utilizada (Davenport; Prusak, 1998). Isso implica que, além do simples acesso aos dados, é essencial garantir sua integridade, confiabilidade e segurança.

A transformação digital intensificou essa lógica. Em um cenário de big data, inteligência artificial e computação em nuvem, os fluxos informacionais se tornaram a espinha dorsal de empresas, governos e até mesmo de relações interpessoais. Sob essa perspectiva, a pesquisadora Shoshana Zuboff (2020, p. 18) argumenta que vivemos na era do “capitalismo de vigilância”, um modelo econômico baseado na coleta massiva de dados comportamentais para prever e moldar ações humanas. Nesse contexto, o controle da informação não é apenas uma questão operacional, mas uma disputa por poder. A informação, antes vista como suporte para decisões, tornou-se ela mesma o centro da estratégia.

Pode-se verificar que a segurança da informação tornou-se um dos pilares essenciais para a sustentabilidade das organizações em um mundo cada vez mais digitalizado, especialmente diante do aumento exponencial de ataques cibernéticos. Sob essa perspectiva, entre as diversas ameaças existentes, os ataques de engenharia social destacam-se por sua capacidade de explorar o fator humano

como um potencial risco, considerado o elo mais frágil na cadeia de segurança (Mitnick; Simon, 2002). Esses ataques não dependem apenas de vulnerabilidades técnicas, mas também da manipulação psicológica de indivíduos para obter acesso a informações confidenciais, causando prejuízos financeiros, danos à reputação e violações de conformidade, como as previstas na Lei Geral de Proteção de Dados (LGPD). A valorização da informação exige, portanto, uma nova cultura organizacional, baseada não apenas em tecnologias de proteção, mas também em educação, ética e responsabilidade.

De acordo com o Relatório de Riscos, publicado pelo Fórum Econômico Mundial (2022 *apud* ALVES *et al.,* 2024, p. 2),

> O relatório *The Global Risks Report* (*World Economic Forum* (WEF), 2022), publicado pelo Fórum Econômico Mundial, destaca a prevalência de problemas de cibersegurança relacionados a erros humanos, onde aproximadamente 95% dos problemas nesse domínio são atribuídos a falhas humanas, enquanto ameaças internas a empresas, sejam intencionais ou acidentais, contribuem para 43% de todas as violações.

Tendo isso em vista, métodos que visam abordar e explorar comportamentos humanos são frequentemente utilizados para burlar sistemas de segurança robustos, atacando diretamente o despreparo ou desatenção dos colaboradores. Assim, vale salientar que empresas de todos os portes estão sujeitas a esses riscos, mas muitas ainda negligenciam a implementação de políticas eficazes de conscientização e gestão de vulnerabilidades humanas (Schneier, 2020).

Nesse contexto, este trabalho estuda os ataques de engenharia social na segurança da informação, identificando as principais vulnerabilidades que facilitam essas ameaças, além de propor medidas que contribuam para mitigar o sucesso desses ataques. O trabalho busca responder a seguinte questão-problema: "Como os ataques de engenharia social exploram as vulnerabilidades humanas e quais medidas podem ser adotadas para mitigar esses riscos?"

Para isso, será realizada uma pesquisa qualitativa, criada a partir da revisão bibliográfica de artigos científicos, relatórios de segurança e estudos de caso de violações de dados causadas por engenharia social. Além disso, serão discutidas propostas de prevenção, como treinamentos de conscientização, políticas de acesso restrito e testes de *phishing*, que podem fortalecer a postura de segurança das empresas.

A relevância deste estudo está em contribuir para a compreensão dos riscos associados à engenharia social, oferecendo *insights* práticos para a gestão corporativa e a proteção de dados. Espera-se que os resultados possam auxiliar usuários e empresas a se conscientizarem dos principais ataques envolvendo engenharia social, da importância da segurança de dados e de se estruturar políticas de segurança de dados em uma organização, bem como retratar algumas soluções para ambos, a fim de proteger e desenvolver estratégias mais eficientes contra essas ameaças, alinhadas às melhores práticas de segurança da informação e à conformidade legal.

2 OBJETIVOS

2.1 Objetivo Geral

Compreender o impacto dos ataques de engenharia social na segurança da informação, por meio de uma revisão bibliográfica, visando verificar quais são os principais tipos de ciberataque de engenharia social e apontar dados estatísticos de relatórios de incidentes e vulnerabilidades.

2.2 Objetivos Específicos

- Identificar e descrever os ataques de engenharia social mais comuns;
- Relatar casos e notícias veiculadas na mídia especializada que evidenciam a ocorrência de ataques de engenharia social;
- Exibir análises estatísticas de relatórios reconhecidos na área de segurança da informação, como o DBIR Verizon 2025 e o CERT.br;
- Indicar medidas eficazes de prevenção contra ataques de engenharia social, com base em boas práticas de segurança cibernética.

3 FUNDAMENTAÇÃO TEÓRICA

Este capítulo aborda os conceitos e definições importantes e necessários para o entendimento do presente trabalho. A princípio serão introduzidos conceitos de vulnerabilidade, manipulação psicológica, engenharia social e segurança da informação, pilares da SI, LGPD, vulnerabilidades na gestão organizacional, bem como a manipulação em ataques de engenharia social.

3.1 Vulnerabilidade

A palavra "vulnerabilidade" surge do Latim "Vulnus", a qual significa ferida. De acordo com o Dicionário Aurélio “vulnerabilidade é estar pronto para ser atacado, ser alguém sem defesa, ser fraco”.

No âmbito da segurança da informação, a vulnerabilidade pode ser definida como qualquer fraqueza em um sistema, processo ou comportamento humano que possa ser explorada por ameaças para comprometer a confidencialidade, integridade ou disponibilidade dos ativos de informação (ISO/IEC 27001, 2013). Sob a ótica da gestão organizacional, as vulnerabilidades transcendem o aspecto técnico, englobando falhas organizacionais e humanas que criam brechas para violações de segurança.

3.2 Manipulação Psicológica

Estudos de Neurociência Cognitiva demonstram que decisões tomadas sob pressão emocional tendem a ignorar processos racionais de análise, explicando a eficácia desses ataques (Goleman, 1995). Ademais, o trabalho de Goleman retrata que a inteligência emocional não está ligada ao nível de QI da pessoa, mas à maneira que ela identifica e lida com as próprias emoções e as dos outros. Nesse sentido, indivíduos com alto nível de inteligência emocional podem utilizar essa habilidade para identificar pontos fracos em outras pessoas e manipulá-las para

atingir seus objetivos. Além disso, pessoas mal intencionadas frequentemente analisam o comportamento emocional de suas vítimas em busca de fragilidades que possam ser exploradas, uma vez que a vulnerabilidade psicológica é um fator determinante no sucesso de ataques de engenharia social (Hadnagy, 2018).

A engenharia social, enquanto prática maliciosa de manipulação psicológica, não é um fenômeno recente, mas sua sofisticação e disseminação cresceram exponencialmente com a digitalização das relações humanas e corporativas. Acerca disso, a essência desse tipo de ataque reside na capacidade de induzir indivíduos a tomarem decisões erradas com base em estímulos emocionais e contextuais cuidadosamente planejados. Kevin Mitnick (2002), reconhecido mundialmente por sua experiência prática como hacker e posteriormente como consultor de segurança, define a engenharia social como a habilidade de explorar a confiança humana para obter acesso a sistemas ou informações.

Para Mitnick, a tecnologia é apenas um meio, o verdadeiro vetor de ataque é a mente humana, ou seja, o elo mais sujeito a variáveis e falhas é o ser humano. Christopher Hadnagy (2018) complementa essa visão ao tratar da engenharia social como um processo que se ancora em princípios clássicos de persuasão, amplamente estudados pela psicologia, especialmente por autores como Robert Cialdini.

O psicólogo Cialdini (2006) identificou seis princípios de influência que ajudam a explicar por que a engenharia social funciona tão bem: reciprocidade, comprometimento e consistência, prova social, autoridade, escassez e simpatia. Esses mecanismos, amplamente utilizados em marketing e comunicação, são reaproveitados por agentes maliciosos para criar situações emocionalmente convincentes, levando as vítimas a agir impulsivamente. Além disso, autores como Daniel Goleman (1995) argumentam que o ser humano frequentemente toma decisões baseadas mais na emoção do que na razão, especialmente sob pressão ou em contextos de incerteza, o que se demonstra como uma condição típica dos ataques de engenharia social. É nesse entrelaçamento entre emoção e decisão que reside o sucesso desses golpes.

3.3 Engenharia Social

Hadnagy (2018) define engenharia social como "a arte de manipular pessoas para que realizem ações ou divulguem informações confidenciais". Diferente dos ataques baseados em vulnerabilidades técnicas, a engenharia social foca no fator humano, considerado o elo mais frágil na cadeia de segurança da informação (Schneier, 2020). Desta forma, a engenharia social ressalta o caráter interdisciplinar, de modo a combinar conhecimento tecnológico, técnicas de persuasão, psicologia social que explora a confiança, a curiosidade ou a autoridade para induzir indivíduos a divulgar informações confidenciais ou realizar ações que comprometam a segurança (Mitnick; Simon, 2002).

Dessarte, a engenharia social envolve habilidades, por exemplo, de manipulação psicológica, coerção, bem como meios de doutrinação. Esses métodos são usufruídos com o intuito de importunar ou até mesmo controlar os pensamentos e crenças de uma outra pessoa, ou seja, método de persuasão que impacta outro indivíduo a agir conforme desejado. Por meio de narrativas persuasivas, as pessoas são ludibriadas e induzidas ao erro. Além disso, os golpistas exploram emoções intrínsecas do homem, como o medo de perder uma oportunidade “única”, enfatizar um senso de urgência para resolver um problema, ou também, explorar afiliações políticas.

Atualmente, os ataques de engenharia social têm se disseminado de forma acelerada, retratando uma séria ameaça à cadeia de segurança cibernética. Ademais, a finalidade desses crimes se baseia na manipulação de indivíduos e organizações para que revelem informações sensíveis e valiosas, favorecendo, assim, ações de cibercriminosos. Tendo isso em vista, mesmo com investimentos em firewalls, criptografia e sistemas de detecção de intrusos, as organizações continuam vulneráveis quando os colaboradores não estão preparados para identificar e resistir a tentativas de manipulação (Hadnagy, 2018).

Pode-se dizer que isso ocorre porque os seres humanos, diferentemente das máquinas, tendem a confiar em outros indivíduos, o que os torna mais vulneráveis em meio a cadeia de segurança. Por meio da exploração de interações

humanas, agentes mal-intencionados podem exercer influência psicológica sobre suas vítimas, levando-as a compartilhar dados confidenciais ou a descumprir protocolos de segurança estabelecidos. Nesse sentido, os ataques de engenharia social se configuram como uma das principais ameaças à integridade dos sistemas tempoe redes computacionais, justamente por explorarem fatores humanos (Salahdine; Kaabouch, 2019).

3.4 Segurança da Informação: Definição e sua importância

A informação é crucial para os negócios de uma corporação e, consequentemente, por sua valorização, demanda ser preservada. Sobretudo na atualidade interconectada, onde esse ativo está em constante aumento, enquanto pode estar exposto a diversos riscos e vulnerabilidades. Assim, consoante a definição da Associação Brasileira de Normas Técnicas (ABNT) (ISO 27002), “Segurança da informação é a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Tendo isso em vista, a informação é um ativo estratégico e se faz competitivo em meio ao mercado. Portanto, vale ressaltar que a segurança da informação é necessária para o funcionamento da organização, seja no setor público, seja no setor privado, de modo a zelar pelas infraestruturas críticas.

3.5 Pilares da Segurança da Informação

A segurança da informação, por sua vez, baseia-se na tríade CID, ou também conhecida pelos três pilares fundamentais: confidencialidade, integridade e disponibilidade (ISO/IEC 27001, 2013).

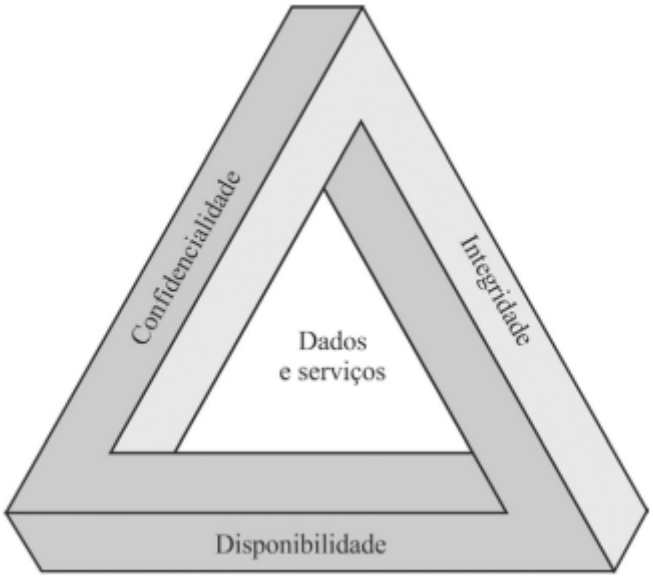
Confidencialidade: este pilar garante que as informações consideradas privadas ou confidenciais não estejam disponíveis e nem evidenciadas para sujeitos

não autorizados, de modo a proteger a privacidade pessoal e suas informações. Desse modo, a divulgação não autorizada desses dados se situa na perda de confidencialidade.

Integridade: este eixo assegura a irretratabilidade e a veracidade das informações, de modo a proteger contra a adulteração ou anulação indevida de informações. Assim sendo, a quebra de integridade implica na transformação ou eliminação não consentido de informações.

Disponibilidade: esta base certifica que o acesso aos sistemas, bem como o uso das informações seja seguro, realizado no tempo adequado e que não haja recusa de serviço a usuários autorizados. Dessa maneira, evidencia-se que a perda de disponibilidade corresponde ao rompimento do acesso a dados ou informações no sistema.

Figura 1 - Tríade de requisitos de seguranças



Fonte: (Stallings; Brown, 2014)

3.6 Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei nº 13.853, de 8 de julho de 2019, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece regras para o tratamento de dados pessoais, tanto no meio físico quanto no digital, por pessoas físicas ou jurídicas, públicas ou privadas. Seu principal objetivo é assegurar os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade dos indivíduos.

Essa legislação surgiu como resposta à crescente coleta e uso de informações pessoais, buscando garantir que os dados sejam tratados com transparência, segurança e responsabilidade. Entre os princípios que fundamentam a LGPD estão o respeito à privacidade, à autodeterminação informativa, à liberdade de expressão e à inviolabilidade da intimidade, honra e imagem das pessoas.

Com a entrada em vigor da LGPD, qualquer organização que realize o tratamento de dados pessoais deve adotar práticas que assegurem a proteção dessas informações, evitando seu uso indevido. Isso implica em obrigações legais tanto para empresas quanto para órgãos públicos, que devem implementar políticas internas de segurança e conscientização para garantir a conformidade com a lei.

3.7 Vulnerabilidades na Gestão Organizacional

As organizações frequentemente negligenciam riscos associados ao comportamento humano, tais como:

- Falta de treinamento em segurança: Colaboradores não reconhecem tentativas de golpes (ISO/IEC 27001, 2013).
- Políticas de acesso frágeis: Excesso de privilégios ou ausência de autenticação multifatorial (MFA) (Verizon Dbir, 2025).
- Cultura organizacional despreparada: Falta de conscientização sobre proteção de dados (LGPD, 2018).

Schneier (2020, p. 47) amplia essa definição em sua máxima que diz: "Vulnerabilidades corporativas são frequentemente sintomas de problemas gerenciais, políticas desatualizadas, treinamentos ineficazes ou culturas organizacionais que negligenciam o fator humano na segurança".

"Qualquer fraqueza identificável em processos, controles ou comportamentos organizacionais pode ser explorada por ataques de engenharia social" (ISO/IEC 27002, 2022, Seção 5.1).

Essas estratégias se tornam ainda mais eficazes quando encontram, nas organizações, ambientes propícios à sua disseminação. Falhas processuais, como a ausência de políticas atualizadas de segurança, canais ineficazes de comunicação e ausência de simulações periódicas de ataques, somam-se a fatores humanos, como falta de treinamento, sobrecarga de trabalho e baixa percepção de risco. Em muitos casos, colaboradores não reconhecem a importância de seu papel na cadeia de proteção de dados e tendem a minimizar alertas ou orientações por não entenderem o real impacto de suas ações.

Por conseguinte, essa combinação entre técnicas de manipulação emocional, falhas organizacionais e ausência de cultura de segurança cria o terreno fértil para o avanço da engenharia social. Assim sendo, compreender essa intersecção é fundamental para desenvolver estratégias que não se limitem ao campo tecnológico, mas que integrem psicologia, gestão e governança da informação (Hadnagy, 2018; Cialdini, 2006).

Em suma, a engenharia social representa uma ameaça crescente que se aproveita não apenas de falhas técnicas, mas principalmente de vulnerabilidades humanas e organizacionais. A compreensão profunda de seus mecanismos, aliada a planos educativo e gerencial, constitui passo essencial para a construção de uma cultura de segurança resiliente.

3.8 Ataques de Engenharia Social - Um risco ainda subestimado

Esta subseção tem foco em abordar uma problemática relacionada ao ser humano centralizado como um fator sujeito a manipulações de Engenharia social e, consequentemente, sofrer grandes impactos e perdas à organização quando as

empresas negligenciam as tendências e a evolução de ataques de engenharia social.

3.8.1 Os riscos do fator humano em segurança da informação

Nos dias atuais, as organizações de todas as magnitudes se preocupam mais com aspectos de segurança de dados e informações, de modo que elas investem fortemente no desenvolvimento das melhores medidas de segurança (Bhusal, 2021). Pode-se dizer que os dados e as informações são os bens mais valiosos para as corporações no mundo atual. Em uma corporação, o fator humano está como o alvo mais fácil e suscetível a falhas dentro do escopo de segurança da informação. Além disso, com o avanço da tecnologia e dos meios de comunicação, os seres humanos estão sofrendo ataques de “Engenharia Social”, de modo que acabam sendo vítimas da manipulação e fornecem informações confidenciais.

Essa prática é uma maneira empregada por cibercriminosos no qual exploram aspectos suscetíveis à psicologia das pessoas com desígnio de obter acessos privilegiados ou para divulgação dessas informações. Tendo isso em vista, esses golpes que utilizam técnicas de engenharia social tem uma alta taxa de sucessos quando se comparado a outros ataques cibernéticos, visto que explora o elo mais fraco da segurança da informação (Bhusal, 2021). Essa artimanha utilizada pelos atacantes conseguem ser quase imperceptíveis às máquinas e programas de segurança mais tecnológicos, uma vez que eles utilizam vertentes da psicologia e para suceder a manipulação humana e desviar dos sistemas de segurança implementados (Bhusal, 2021).

Outro aspecto relevante diz respeito ao desdém e a falta de iniciativas abordando o fator humano relacionado com a segurança da informação. Dessarte, é fundamental a divulgação da importância da tríade de requisitos de segurança e do ensinamento de novas tecnologias e o treinamento dos usuários para identificar possíveis ameaças cibernéticas. Logo, ataques de engenharia social podem ser vista como uma grave ameaça, visto que não se pode ser abordada por meios

convencionais de sistemas de identificação de intrusões como firewalls ou *softwares* antivírus (Greavu-Şerban, Constantin, 2022).

3.8.2 Etapas da Engenharia Social - Como os ataques acontecem?

Os engenheiros sociais podem atacar por intermédio de várias ferramentas como: emails, ligações de telefone, mídias sociais e comunicações pessoais, com desígnio de se aproximarem do alvo e adquirir dados para expor ou modificar os sistemas de informação de uma associação. Acerca disso, os ataques envolvem quatro etapas (GOV.BR, 2024):

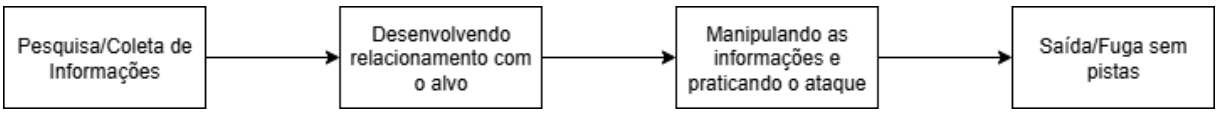
1- Investigação de informações sobre a vítima;

2 - Criação de relacionamento ou interação com a vítima;

3- Extorsão da vítima - adulterar as informações e realizar o ataque;

4 - Desassociação/saída - fugir sem deixar vestígios.

Figura 2 - Fases que comumente um Engenheiro Social percorre



Fonte: Bhusal, 2021

3.8.3 Abordagem sobre o comportamento humano

Bhusal (2021) retrata como cada etapa é construída e como os atacantes conseguem bem-suceder os ataques. Verifica-se que na fase inicial, ocorrem os estudos e coletas de informações acerca do alvo em questão, antes de qualquer

ataque real. Ademais, essa etapa determina as chances da efetivação do ataque, e para isso, os criminosos utilizam ferramentas que auxiliam na varredura de informações disponíveis na *internet*, como o Maltego, o qual contém dados de perfis e postagens em gráficos para melhor análise de conexão previamente desconhecidas. Os especialistas nesse ataque combinam informações de diferentes fontes (fotos, localização e informações de amigos), inclusive referências públicas (vestimentas, falta de dever moral, baixo nível de entendimento de engenharia social e ataques cibernéticos).

Em seguida, o atacante avalia as informações coletadas e trabalha em direção a um plano de ação para chegar na vítima. Depois, a comunicação entre o atacante e o alvo se inicia, com objetivo de criar um potencial vínculo com a vítima por meio de conversas supostamente inócuas. O principal intuito dessa interação é conquistar a confiança da vítima, e posteriormente, construir um contexto que dissimule as reais intenções e capture as fraquezas do alvo. Os manipuladores podem tentar se passar por pessoas conhecidas como amigos ou familiares, ou até mesmo, fingir ser um agente bancário ou governamental.

Posteriormente, o esquema se dá início e a vítima é manipulada baseado nas pesquisas reunidas nas etapas antecedentes a fim de afetar sistemas ou obter dados confidenciais. Além disso, as técnicas de manipulação utilizadas atingem emocionalmente o alvo para que o plano ocorra até que as informações importantes sejam coletadas e órgãos de segurança não sejam acionados pela vítima.

Por fim, o contato com o alvo se desvanece aos poucos ou de forma repentina, onde todo e qualquer vestígio ou evidência de crime são excluídos pelos atacantes sem ao menos que a vítima descubra.

3.8.4 Abordagem tecnológica

Por um lado, observou-se os aspectos comportamentais salientados pelos criminosos para que os crimes tenham sucesso, porém ainda, outra maneira que os atacantes abordam as vítimas é por meio de recursos tecnológicos. Diferentemente,

Greavu-Şerban e Constantin (2022) retratam o procedimento por um viés mais técnico que baseia-se na falsificação de um sistema de aplicação em que a vítima facilita informações confidenciais através de ataques de *phishing*, emails de *spam*, *pop-ups*, *spyware* ou *malware*. Tendo em vista essas maneiras, o usuário fica exposto a perceber uma janela de *pop-up*, por exemplo, a qual informa que o sistema rodando verificou certos erros que limitaram sua funcionalidade. A partir disso, é informado que para a aplicação ser restaurada, é necessário completar algumas informações confidenciais como campos de ID e senha e, logo, o fraudador consegue acessar o sistema computacional com essas credenciais.

Além disso, diversos e-mails de *spam* trazem anexos que escondem vírus, como trojans e outros programas maliciosos, capazes de afetar tanto computadores individuais quanto redes inteiras. Os efeitos desse tipo de ataque podem ir desde uma queda no desempenho da máquina até problemas mais graves, como a perda ou alteração de registros e até a manipulação da comunicação dentro da rede. Dentro desse cenário, o *phishing* é uma das práticas mais comuns utilizadas em ataques de engenharia social. Geralmente, a vítima é abordada por meio de e-mails falsos ou até mesmo por ligações telefônicas, sendo induzida a fornecer informações sigilosas.

Em alguns casos, o criminoso digital se aproveita de programas aparentemente legítimos, mas que vêm infectados com *malware*. Esse é um recurso amplamente utilizado pelos criminosos, o qual a terminologia se refere a qualquer software malicioso desenvolvido com o objetivo de comprometer sistemas, roubar informações ou fornecer acesso remoto não autorizado aos atacantes. Conforme ressaltam William Stallings e Lawrie Brown (2014), esses programas podem se disfarçar de aplicativos legítimos, induzindo o usuário a instalá-los com a falsa promessa de otimização ou segurança, quando, na verdade, servem para coleta de dados ou abertura de brechas no sistema para invasões futuras.

Dentro dessa categoria, destaca-se também o *ransomware*, um tipo específico de *malware* que, ao infectar o dispositivo, criptografa os arquivos da vítima e exige um pagamento, geralmente em criptomoeda, para liberar o acesso ao conteúdo sequestrado. De acordo com Kaspersky (2023), esse tipo de ataque não depende apenas de vulnerabilidades técnicas, mas explora principalmente a

confiança e a desatenção do usuário, que é levado a clicar em *links* ou baixar anexos maliciosos enviados por e-mail, mensagens instantâneas ou até sites comprometidos. Assim, o usuário acaba instalando o *software* acreditando que se trata de uma ferramenta útil para melhorar o desempenho do computador, quando na verdade está sendo enganado.

> O *ransomware* é um tipo de malware que criptografa os dados do sistema ou bloqueia o acesso aos arquivos de um usuário, exigindo o pagamento de um resgate em moeda virtual para restaurar o acesso aos dados. Esse tipo de ataque, amplamente estudado por especialistas em segurança cibernética, tornou-se uma das principais ameaças à segurança digital. Geralmente, o pagamento é solicitado em criptomoedas, como o Bitcoin, dificultando o rastreamento da identidade do autor do ataque (Silva Júnior, 2023, p. 15).

Assim, observa-se que, mesmo em ameaças tecnológicas, o elemento humano continua sendo o principal vetor para o sucesso da invasão.

4 METODOLOGIA

4.1 Abordagem do Estudo

Este estudo foi desenvolvido através de uma pesquisa qualitativa, de caráter exploratório-descritivo, baseado em pesquisa bibliográfica e documental. Tem como objetivo, compreender o impacto dos ataques de engenharia social na segurança da informação, identificando seus principais tipos, impactos e formas de prevenção (Gil, 2019).

A pesquisa é classificada como exploratória, conforme definido por Gil (2017), por ter como objetivo proporcionar maior familiaridade com o tema, permitindo sua exploração e compreensão a partir de diferentes fontes e perspectivas, além disso essa análise contém diversos aspectos, tal como fatos ou eventos estudados.

Com relação a procedimentos metodológicos, este trabalho é uma pesquisa bibliográfica realizada a partir de trabalhos anteriormente publicados, artigos científicos, livros, teses, relatórios, notícias veiculadas na mídia especializada, além de outros meios (Gil, 2017).

4.2 Procedimentos Metodológicos Planejados

A primeira etapa consiste em uma revisão bibliográfica abrangente, utilizando aplicações como Google Scholar, periódicos da CAPES, biblioteca virtual Pearson, entre outras. Além disso, a seleção dos materiais seguiu critérios de relevância temática e atualidade, priorizando publicações dos últimos cinco anos, com exceção de obras clássicas utilizadas para a fundamentação teórica. A divisão dos materiais ocorreu de maneira a distinguir os mais pertinentes sobre a temática.

Como destaca Gil (2019), essa abordagem permite mapear o conhecimento consolidado sobre o tema antes de avançar para análises mais específicas.

Na segunda etapa, foi realizado o levantamento dos principais tipos de ataques de engenharia social e como funcionam, com base na incidência em outros trabalhos do tema.

A terceira etapa envolveu o estudo de ataques de engenharia social em empresas. Esses casos serão analisados considerando três aspectos: (1) os vetores de ataque utilizados, (2) as medidas de resposta implementadas e (3) os resultados obtidos. Como sugere Yin (2015), a análise de casos múltiplos permite identificar padrões e extrair lições valiosas para a prática organizacional.

Na quarta etapa, são apresentados dados de análises dos relatórios de incidentes e vazamento de dados de organizações reconhecidas no campo da cibersegurança, como o Verizon *Data Breach Investigations Report* e o Centro Nacional Brasileiro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br). Esses documentos foram examinados através do método de análise de conteúdo proposto por Bardin (2016), com o objetivo de identificar padrões nos ataques de engenharia social. A análise destacou principalmente as técnicas de ataque mais frequentes e as vulnerabilidades organizacionais exploradas.

Por fim, com base nos resultados das etapas anteriores, o trabalho abrange um conjunto de recomendações práticas para prevenção e mitigação de ataques de engenharia social, consoante às cartilhas e políticas de proteção de dados.

4.3 Limitações do Estudo

A principal limitação está relacionada à disponibilidade de dados sigilosos ou técnicos sobre incidentes reais, tendo em vista a sensibilidade e confidencialidade dos dados, de forma a dificultar a obtenção de informações detalhadas de empresas. Nesse sentido, muitos ataques de engenharia social, especialmente em ambientes corporativos e financeiros, não são divulgados publicamente em detalhes,

seja por questões legais, estratégicas ou reputacionais. Dessa forma, a análise de casos reais se restringiu às informações veiculadas na imprensa e nos relatórios públicos, o que pode não refletir a totalidade do incidente ou de suas consequências.

Possíveis restrições sobre a atualidade dos dados:

- Rápida evolução das técnicas de engenharia social.
- Possível desatualização de relatórios durante a pesquisa.

5 TÉCNICAS DE ENGENHARIA SOCIAL

A engenharia social diferencia-se dos ataques tradicionais por explorar fatores psicológicos em vez de falhas técnicas. Nesse tipo de ação, o criminoso manipula emoções e comportamentos humanos para induzir a vítima a compartilhar informações confidenciais ou realizar ações que comprometem a segurança. Elementos como confiança, autoridade, senso de urgência e curiosidade são estrategicamente explorados para reduzir a desconfiança e facilitar o engano (Rajalim, 2025). Entre as diversas modalidades, destacam-se aquelas que atualmente aparecem com maior frequência nos incidentes de segurança cibernética, as quais serão descritas a seguir.

*Phishing***:** O termo *phishing* vem da palavra em inglês *fishing* (pescar). Consiste no envio de mensagens fraudulentas que se passam por fontes confiáveis, com desígnio a explorar e usufruir de técnicas psicológicas, como de cunho urgente, medo ou de recompensa, e assim, induzir a vítima a agir prontamente sem desconfiar do golpista (IBM, 2024). Além disso, os criminosos aprimoram essa técnica e aumentam ataques quando são mais personalizados e emocionalmente cativantes. Algumas dessas ramificações de ataques de *phishing* são abordadas abaixo:

5.1 Subdivisões de ataques de *phishing*

Phishing por e-mail em massa: os criminosos se passam por grandes entidades para trazer mais confiança ao golpe, e utilizam o correio eletrônico para realizar o ataque, de modo a enviar emails promiscuamente para a maior quantidade de pessoas possível esperando que uma parcela cliquem em *links* ou arquivos maliciosos e tenha dados confidenciais violados (IBM, 2024).

Figura 3 - Exemplo de Ataque de Phishing em massa.

Fonte: Usecure [s.d.]

Vishing (*Phishing* por voz): é o ataque de *phishing* por ligações telefônicas como intermédio de comunicação com as vítimas. Assim, o golpista tende a falsificar o identificador de chamadas, de modo a dissimular ser de uma organização legítima. Além disso, as abordagens são tendenciosas a assustar às vítimas como complicações com o cartão de crédito (IBM, 2024).

Smishing (*Phishing* por SMS): de acordo com a IBM, 2024 “o termo "*smishing*" é uma combinação de "SMS" ou "short message service", a tecnologia por trás das mensagens de texto, e *"phishing"*. Desse modo, os criminosos enviam mensagens fraudulentas com intuito de enganar as pessoas a clicarem em *links* carregados com *malware*, roubar dados confidenciais e manipular a vítima a transferir dinheiro (IBM, 2024).

Quishing: esse termo deriva-se da junção de *QR code* com *phishing*. Trata-se de um golpe que insere códigos QR maliciosos em e-mails, mensagens ou locais físicos. Ao escaneá-los, a vítima é redirecionada a sites fraudulentos que coletam dados pessoais, bancários ou realizam *downloads* de *malware* (IBM, 2024). Desse modo, o delito acontece quando a vítima escaneia o QR code acreditando se

tratar de uma fonte confiável, como bancos, órgãos públicos ou empresas conhecidas, e ao acessar o *link* oculto no código, ela fornece dados sem perceber o risco (IBM, 2024).

Spear Phishing: é o ataque de *phishing* direcionado para uma pessoa específica, geralmente que possua acesso a dados confidenciais ou um certo nível de autoridade (IBM, 2024).

Whale phishing ou *Whaling*: no contexto de ataque cibernético significa “pescar baleias”, ou seja, é um golpe de *phishing* que visa executivos de alto nível e líderes que podem autorizar pagamentos e transferências (IBM, 2024). Esse ataque faz parte da classificação de spear *phishing*, uma vez que é um ataque com alvo a um indivíduo específico.

Phishing e IA (Inteligência Artificial): Com o avanço da IA, os ataques de *phishing* tornaram-se mais sofisticados. Essa tecnologia facilita a automatização de tarefas repetitivas, geração de mensagens personalizadas e padronização de ataques que antes exigiam muito trabalho humano (MPMT, 2024). Ademais, pode ser usada para criar *deepfakes*, ou seja, vozes ou imagens falsificadas que simulam pessoas conhecidas, com objetivo de induzir confiança na vítima e aumentar a eficácia do golpe (TCE-ES, s.d.). Sob essa ótica, portanto, é possível verificar que a IA intensifica e amplifica o escopo em níveis de escalabilidade, personalização e realismo dos ataques, o que o torna mais difícil de ser detectado também.

5.2 *PRETEXTING*

Esse nome procede da palavra “pretexto”, na qual o engenheiro social cria um cenário falso ou identidade falsa e assume uma identidade confiável, como um executivo ou suporte técnico de TI solicitando acesso ao sistema, a fim de enganar ou manipular a vítima para extrair dados sensíveis (Mitnick, 2002). Desse modo, o principal objetivo do golpista nesse caso é ganhar a confiança do usuário para que ele compartilhe informações confidenciais e prejudique a organização alvo. Na

maioria dos casos, não é comum que os colaboradores questionem alguém relevante que teria acesso ao sistema do computador (Lira, 2020).

5.3 *Baiting*

Uso de iscas, isto é, utiliza um meio físico ou digital organizada de maneira atrativa com intuito de cativar a vítima, como pen drives que estão infectados com código malicioso ou ofertas salientes falsas, dessa forma, o alvo é induzido a instalação de malwares e o criminoso terá acesso aos dados alocados na máquina da vítima (Hadnagy, 2018). Além disso, os golpistas podem utilizar o *pretexting*, por exemplo, com a finalidade de manipular a isca, adaptando-a para torná-la ainda mais atrativa à vítima (IBM, 2024).

5.4 *Quid Pro Quo*

A expressão *quid pro quo* é uma frase em latim que significa “uma coisa em troca de outra”. Esse golpe aborda uma promessa ou oferta de benefícios em troca de informações, como falsos suportes técnicos, em troca de uma informação ou acesso que solicitam senhas (Schneier, 2020). Dessa maneira, a finalidade desse ataque está em obter acesso não autorizado ao sistema ou roubar informações confidenciais.

6 ESTUDOS DE CASO EXPLORATÓRIOS

A engenharia social tem se mantido como a técnica mais eficaz para contornar defesas que dependem exclusivamente de tecnologia (Breda F., Barbosa H., Morais T., 2023). A seguir, apresentam-se estudos de caso exploratórios selecionados, que evidenciam como a engenharia social foi empregada em ataques de alto impacto. Cada caso será analisado sob três perspectivas: (1) vetor e técnica de engenharia social utilizada; (2) sequência de eventos que permitiu a intrusão; e (3) consequências operacionais, financeiras e reputacionais. Essa abordagem visa demonstrar não apenas a variedade de artifícios psicológicos utilizados pelos atacantes, mas também padrões recorrentes que podem orientar ações preventivas e correções de processo em organizações de diferentes portes e setores (Rajalim, 2025).

6.1 Ataque ao sistema financeiro no Banco Central

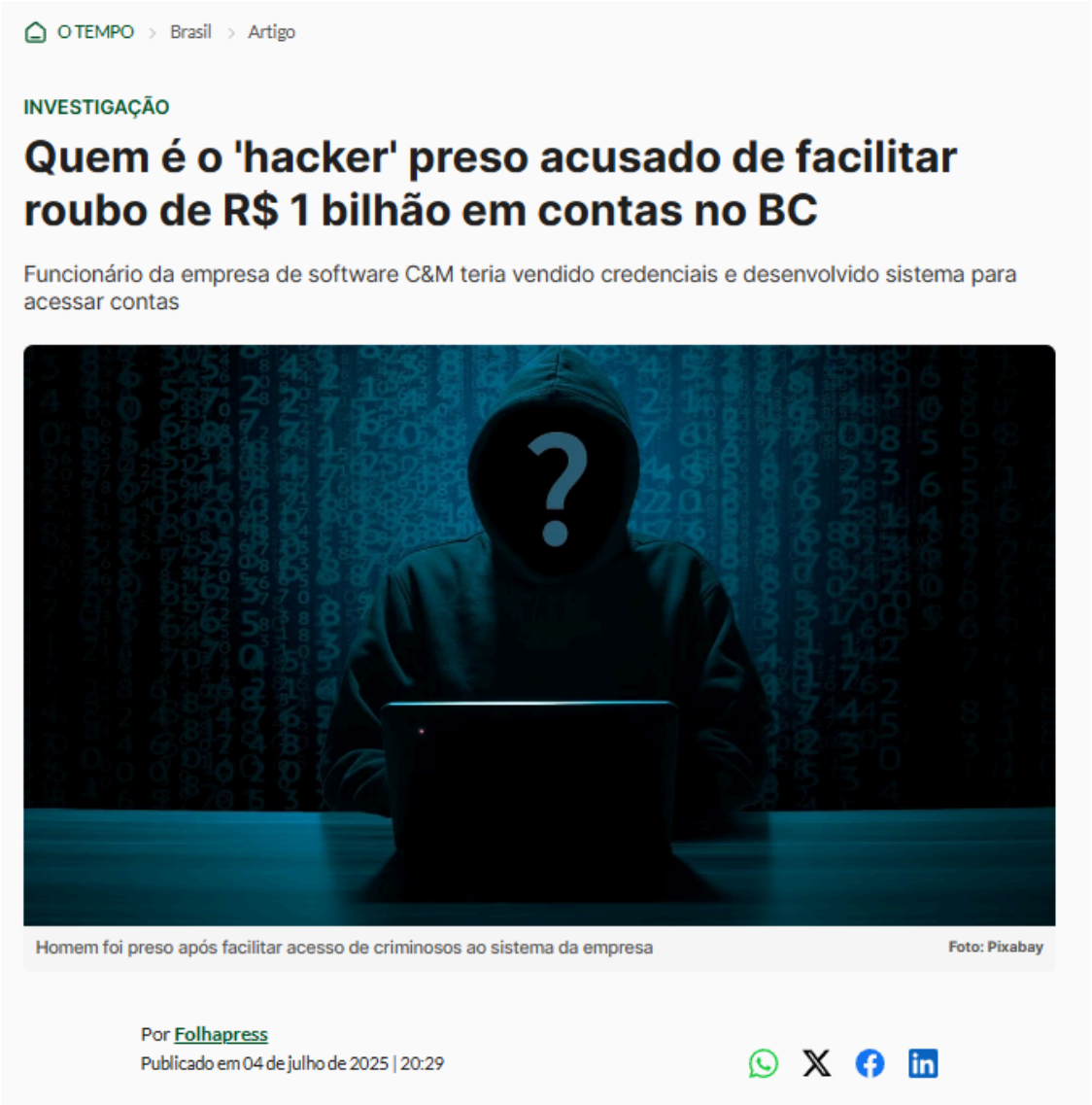
O caso que envolveu o Banco Central do Brasil em 2025 ilustra de forma marcante como a engenharia social pode superar barreiras tecnológicas e gerar prejuízos de proporções milionárias. O incidente ocorreu por meio da empresa intermediária C&M *Software*, atuando como Prestadora de Serviços de Tecnologia da Informação (PSTI), para instituições participantes do PIX, e que tinha acesso a sistemas críticos relacionados ao BC. O ponto central da ocorrência foi a atuação de um funcionário de tecnologia da informação da C&M, que teria aceitado colaborar com criminosos ao vender suas credenciais de acesso e facilitou transações fraudulentas (O TEMPO, 2025). Além disso, a C&M *Software* foi obrigada a ser desconectada do ambiente operacional de mensagens interbancárias por determinação do Banco Central, suspendendo temporariamente suas atividades críticas (CNN, 2025).

Esse episódio representa um ataque de engenharia social baseado em *quid pro quo*, o que caracteriza uma abordagem de troca direta de recursos em troca do

acesso aos sistemas críticos, em que o funcionário da C&M *Software* forneceu suas credenciais em troca de um benefício monetário**.** Dessa forma, não houve necessidade de exploração de falhas técnicas complexas, mas sim da vulnerabilidade de um indivíduo com acesso privilegiado. Ao manipular a confiança de um funcionário, os fraudadores conseguiram contornar barreiras de segurança que, do ponto de vista tecnológico, permaneciam intactas. Sob essa ótica, evidencia-se como a terceirização de serviços em setores críticos amplia a superfície de ataque, já que empresas parceiras muitas vezes não possuem os mesmos controles de segurança que a instituição principal (IPNEWS, 2025).

Por conseguinte, o impacto do caso não se restringe ao prejuízo financeiro direto, embora esse seja expressivo. Vale considerar também os custos com as medidas emergenciais de contingência, a perda de reputação perante a sociedade e o risco de desconfiança no sistema financeiro nacional (O TEMPO, 2025).

Figura 4 - Manchete do portal O TEMPO sobre hacker acusado de facilitar roubo ao BC



Fonte: O TEMPO, 2025

6.2 Invasão ao Sistema Integrado de Administração Financeira do Governo Federal SIAFI

No início de 2024, o governo federal identificou uma invasão ao Sistema Integrado de Administração Financeira do Governo Federal (SIAFI), sistema utilizado para registros e execução financeira da União, que gerou suspeitas sérias de desvio

de recursos. As investigações apontam que criminosos utilizaram credenciais válidas de servidores autorizados para emitir ordens de pagamento fraudulentas (Bracco, 2024).

Os criminosos utilizaram uma combinação de *phishing* e *pretexting*, enviando mensagens fraudulentas que, com dados pessoais das vítimas, as induziram a clicar em *links* maliciosos. Essas ações de engenharia social permitiram a coleta de senhas, que eram usadas para emitir ordens de pagamento fraudulentas. Consoante ao relatório do Tribunal de Contas da União (TCU), evidencia que o ambiente era propício para uma crise. O tribunal apontou "indícios de falhas sistêmicas", como controles de acesso insuficientes e a carência de mecanismos de autenticação fortes e a "necessidade urgente de aprimoramento" do SIAFI. Além disso, o TCU também destacou a necessidade de revisão de processos, o que inclui a forma como os servidores interagem com o sistema.

Este incidente evidencia que a segurança de sistemas complexos, como o SIAFI, depende de uma abordagem holística que abrange o treinamento de usuários, a implementação de autenticação multifator e o monitoramento de acessos. O caso destaca que o fator humano continua sendo o elo mais frágil da cadeia de segurança da informação.

Figura 5 - Manchete do portal Security Report sobre tentativa de invasão ao Siafi

Fonte: Security Report (2024).

6.3 MGM Resorts (2023)

O ataque contra a MGM Resorts em 2023 foi um exemplo notável de engenharia social de alto nível. O grupo de hackers *Scattered Spider* (também conhecido como UNC3944 e BlackCat/ALPHV) usou a técnica de vishing (*phishing* por voz) para enganar um funcionário do *help desk* de TI da empresa. Os invasores obtiveram informações sobre o perfil do funcionário na rede social LinkedIn e, a partir daí, passaram por ele em uma ligação para a central de suporte. Acreditando que estavam atendendo a um colega, os funcionários do help desk redefiniram as

credenciais de acesso, concedendo aos hackers uma entrada para a rede interna da MGM.

Uma vez dentro, os criminosos conseguiram escalar privilégios e implantar um *ransomware*, paralisando sistemas críticos em hotéis e cassinos da rede, incluindo reservas, caça-níqueis e sistemas de pagamento. O ataque causou interrupções generalizadas e resultou em um prejuízo estimado em mais de US$100 milhões. O incidente destacou a fragilidade das defesas corporativas contra ataques que visam o elo mais fraco: o ser humano.

6.4 CDK *Global* (2024)

O ataque contra a CDK *Global*, um dos maiores provedores de software para concessionárias de veículos nos Estados Unidos, afetou mais de 15 mil revendedoras de automóveis na América do Norte. O vetor inicial do ataque foi uma campanha de *phishing* massiva, direcionada a funcionários da empresa. Através de e-mails falsos, os invasores conseguiram roubar credenciais de acesso e obter uma entrada inicial na rede da CDK (IBM, 2024).

Essa invasão inicial permitiu que o grupo criminoso escalasse privilégios e implantasse um *ransomware*, causando a interrupção substancial de sistemas essenciais, como vendas, financiamento e agendamento de serviços. O ataque resultou em prejuízos na casa das dezenas de milhões de dólares e em um caos operacional em todo o setor. O caso da CDK reforça a importância de um treinamento constante sobre segurança para os funcionários, já que mesmo uma única falha de segurança humana pode levar a uma catástrofe financeira e operacional (REUTERS, 2024).

6.5 Arup (2024)

O caso da empresa de engenharia e consultoria Arup demonstra o uso de *deepfake* para criar um golpe de engenharia social altamente convincente. Nesse cenário, os golpistas utilizaram tecnologia de inteligência artificial para se passar, em uma videochamada, por diretores financeiros da Arup e de uma empresa parceira. O alvo foi um funcionário do departamento financeiro, que foi convencido a autorizar e realizar múltiplas transferências bancárias, somando aproximadamente £20 milhões.

A tecnologia de *deepfake* permitiu que os criminosos simulassem a aparência e a voz dos executivos, o que deu uma camada extra de credibilidade ao ataque. Nesse episódio, o elemento humano novamente foi explorado, mas com apoio de tecnologia de inteligência artificial que aumentou a credibilidade do golpe.

6.6 Ataque de *Phishing* e Lavagem de Dinheiro (2021)

Este estudo de caso, baseado em uma confissão do Departamento de Justiça dos EUA em 2024, analisa um ataque cibernético de 2021 contra uma empresa em São Francisco, focado na exploração da engenharia social. O ataque inicial utilizou uma campanha de *phishing* para obter acesso a um e-mail corporativo. Ao monitorar as comunicações, os criminosos interceptaram uma transação financeira legítima e, por meio do *Business Email Compromise* (BEC), redirecionaram um pagamento de cerca de US $922.445,34 para contas sob seu controle (FBI, 2024).

O caso ilustra a vulnerabilidade do fator humano, que, ao ser manipulado, permite que cibercriminosos contornem as defesas tecnológicas. Este incidente sublinha que a engenharia social, em suas formas mais sofisticadas como o BEC, representa uma ameaça sistêmica, expondo a necessidade de uma abordagem de segurança que combine tecnologia robusta com a conscientização e o treinamento contínuo dos funcionários.

7 ABORDAGEM ANALÍTICA E ESTATÍSTICA GERAL DE RELATÓRIOS

Inicialmente, é válido entender a diferença entre incidente e vulnerabilidades.

INCIDENTE: Um incidente de segurança é qualquer evento adverso, confirmado ou suspeito, que afeta a segurança dos sistemas computacionais ou das redes de computadores, comprometendo a integridade, confidencialidade ou disponibilidade de um ativo de informação (Verizon DBIR, 2025).

VULNERABILIDADES: São notificações preventivas que alertam os responsáveis pelos ativos sobre fragilidades nos sistemas computacionais, as quais podem ser exploradas por agentes maliciosos para causar danos ou comprometimento dos dados ou sistemas (Verizon DBIR, 2025).

Como proposto na metodologia, esse subtópico tem como finalidade complementar as análises realizadas consoante aos trabalhos bibliográficos referenciados por meio de relatórios de vazamento de dados e incidentes cibernéticos. A princípio, foram selecionadas duas fontes que promovem uma abordagem analítica e estatística, as quais contêm informações recentes e que revelam, principalmente, o crescimento dos ataques de engenharia social nas organizações. Assim, utilizou-se como referencial teórico para essa seção, a Verizon DBIR 2025 e o CERT 2025. Vale ressaltar, contudo, a dificuldade de acesso a detalhes de incidentes cibernéticos devido a confidencialidade e sensibilidade dos dados.

7.1 Perspectiva global de vazamento de dados

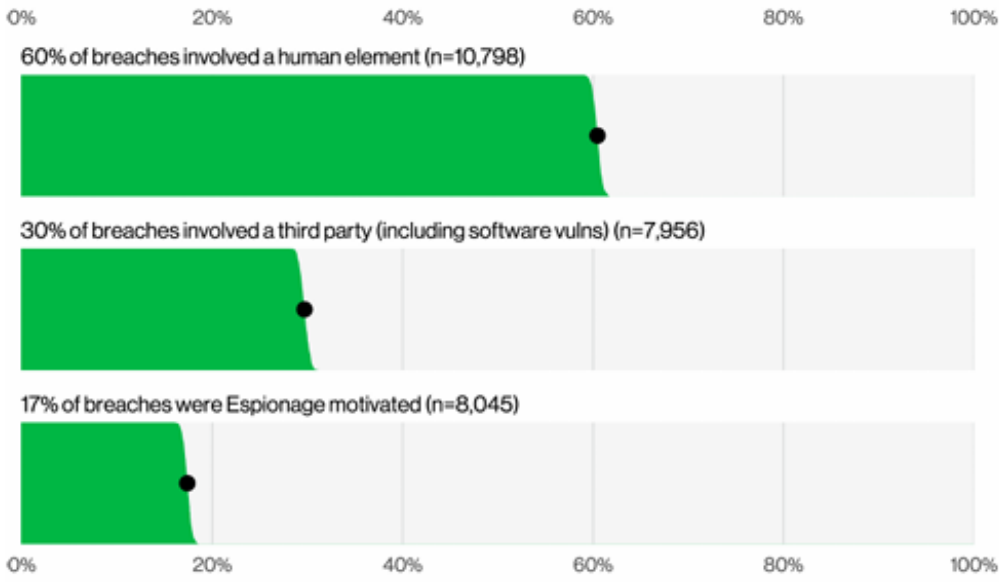
O Relatório de Investigações de Violação de Dados, Verizon (2025), contempla uma ampla variedade de incidentes, o que contribui para análises. Dessa forma, o DBIR utilizou 22.052 incidentes de segurança reais, dos quais foram

analisados 12.195 incidentes respectivos a violações de dados, além de constatar vítimas de ameaças em 139 países em torno do globo. Além disso, os incidentes avaliados correspondem ao período entre (01/11/2023 e 31/10/2024). Assim sendo, foi possível verificar alguns cenários semelhantes à edição anterior do relatório, além do aumento abrupto de casos em outros panoramas.

Desse modo, observou-se, com base nas análises do relatório, o gráfico 1 evidenciam os casos principais listados em violações, e inicialmente, percebe-se que as violações envolvendo pessoas foram responsáveis pela maioria dos casos. Sob essa perspectiva, das 10.798 brechas de segurança analisadas, verificou-se que 60% dessas violações envolvem o fator humano, correspondendo esse elemento, a maior parte do comprometimento de dados. Em seguida, considerou-se uma amostra de 7.956 casos em que se avaliou que em 30% dessas brechas, envolveram um terceiro externo, (incluindo falhas de *software* de terceiros), esse crescimento expressivo das brechas envolvendo terceiros alertou, pois passaram de 15% para 30% em apenas um ano, ou seja, dobraram. Ademais, uma amostra de 8.045 casos analisados retratou que 17% das violações foram motivadas por espionagem cibernética (Verizon DBIR, 2025).

> Também observamos um crescimento significativo nas violações motivadas por espionagem em nossa análise, que agora estão em 17%. Esse aumento foi, em parte, devido a mudanças na composição de nossos colaboradores. Essas violações exploraram a exploração de vulnerabilidades como um vetor de acesso inicial 70% das vezes, mostrando o risco de operar serviços sem correção. No entanto, também descobrimos que a espionagem não era a única coisa que os atores patrocinados pelo estado estavam interessados - aproximadamente 28% dos incidentes envolvendo esses atores tinham um motivo financeiro (VERIZON DBIR 2025, p. 11).

Gráfico 1: Elementos chave listados em violações



Fonte: DBIR Verizon 2025 (p. 11)

As violações de dados envolvendo engenharia social é um tópico bastante crucial, devido à rapidez que os atacantes agem, bem como a frequência que essas ameaças são realizadas. O quadro 1 ilustra 4.009 incidentes, dos quais 3.405 resultaram em divulgação de dados, sendo eles informações internas (68%), outras categorias de dados (58%) e segredos corporativos (53%) (DBIR Verizon, 2025).

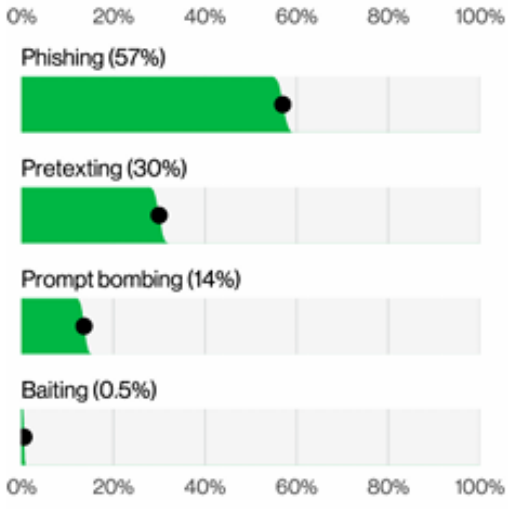
Quadro 1: Violações envolvendo engenharia social

Frequência	4.009 incidentes, 3.405 divulgação de dados confirmada
Atores de ameaças	Externos (100%) (violações)
Motivos dos atores	Financeiro (55%), Espionagem (52%) (violações)
Dados comprometidos	Internos (68%), Outros (58%), Segredos (53%) (violações)

Fonte: DBIR Verizon, 2025 (p. 46)

Inclusive, o gráfico 2 retrata o *phishing* e o *pretexting* como principais técnicas utilizadas em ataques de engenharia social, com base na análise de 3.208 incidentes do relatório de violação de dados da Verizon (2025). Dentre as categorias avaliadas, o *phishing* permanece como o método mais recorrente, representando 57% dos casos. Em seguida, destaca-se o *pretexting* (30%). Também aparecem técnicas mais recentes, como o *prompt bombing* (14%), que explora o cansaço e a desatenção do usuário ao bombardear com solicitações de autenticação, e o *baiting* (0,5%). Assim, esses dados reforçam a importância de treinar continuamente os usuários para reconhecer e resistir a esses ataques, uma vez que a engenharia social continua sendo uma das formas mais eficazes de violar sistemas, independentemente da tecnologia empregada.

Gráfico 2: Principais incidentes de Engenharia Social



Fonte: DBIR Verizon, 2025 (p. 47)

Ademais, foram evidenciados também, ataques de engenharia social presentes no setor financeiro e de seguros, sendo os principais padrões: o sistema de intrusão, a engenharia social e ataques básicos e aplicações web. Sob essa ótica, foi retratado 74% de violações de uma frequência de 3.336 incidentes e 927 com divulgação de dados confirmados (DBIR Verizon, 2025, p. 75).

Em seguida, outro aspecto relevante para este trabalho diz respeito à violação de dados de organizações, o qual fora também abordado no DBIR 2025. O estudo abordou que a “Engenharia Social” faz parte dos principais padrões em pequenas empresas, além de “Intrusão de sistema” e “Ataques Básicos a Aplicações Web", os três representam 96% das violações, como mostra o quadro 2.

> A primeira coisa que é prontamente aparente é que há quase quatro vezes mais vítimas de PMEs do que grandes organizações. Essa diferença aumentada faz sentido, em parte, devido ao simples fato de que há mais PMEs fazendo negócios do que grandes organizações (VERIZON DBIR 2025, p. 86).

Quadro 2 - Incidência de incidentes em pequenas e médias organizações

Organização	Frequência	Principais padrões	Atores de ameaça	Motivos do ator	Dados comprometidos
Pequenas empresas (menos de 1.000 funcionários)	3.049 incidentes, 2.842 com divulgação de dados confirmada	Intrusão de Sistema, Engenharia Social e Ataques Básicos a Aplicações Web representam 96% das violações	Externo (98%), Interno (2%), Parceiro (1%) (violações)	Financeiro (99%) (violações)	Interno (83%), Credenciais (34%), Outros (6%), Pessoal (4%) (vazamentos)
Grandes empresas (mais que 1.000 funcionários)	982 incidentes, 751 com dados de divulgação confirmados	Intrusão de Sistema, Ataques Básicos a Aplicações Web e Erros Diversos representam 79% das violações	Externo (75%), Interno (25%), Parceiro (1%), Múltiplo (1%) (violação)	Financeira (95%), Espionagem (3%), Ideologia (1%) (violação)	Pessoal (50%), Outros (36%), Credenciais (29%), Interno (29%) (violação)

Fonte: DBIR Verizon 2025 (p. 85)

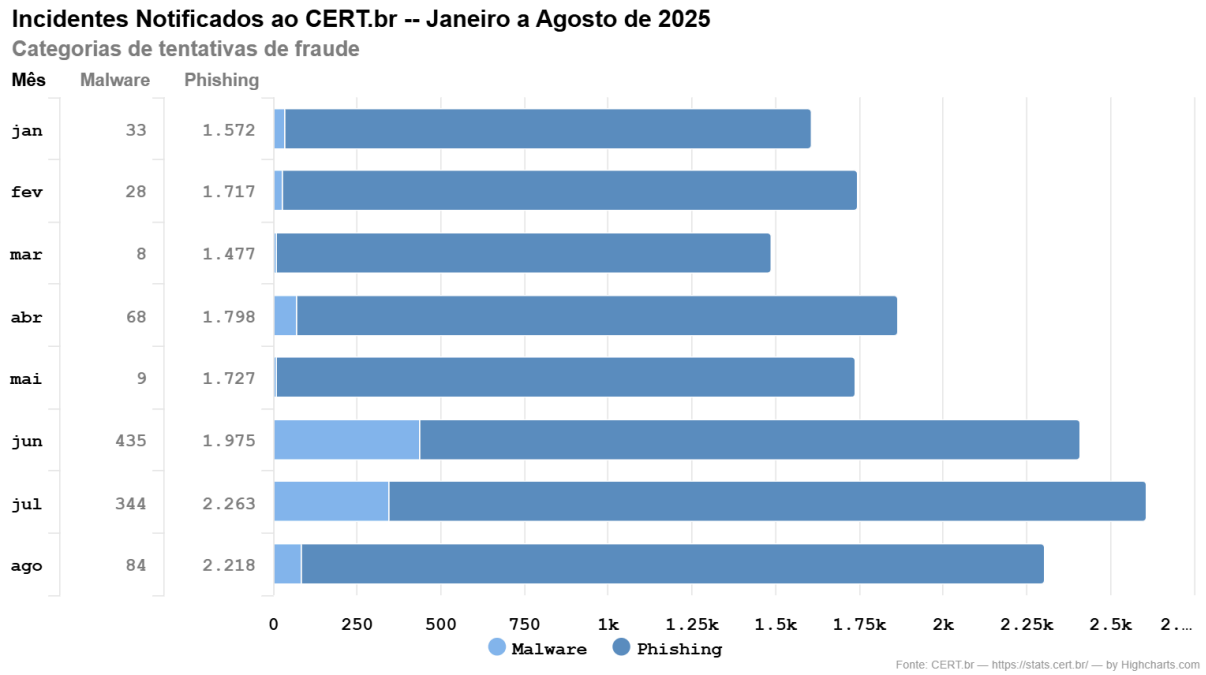
Portanto, com base na análise dos incidentes apresentados no relatório, fica evidente que a engenharia social continua sendo uma das técnicas mais exploradas por atacantes, reforçando a importância do fator humano na segurança da informação. Nesse sentido, o dado de que 60% das brechas envolveram elementos humanos demonstra que organizações de todos os tamanhos permanecem vulneráveis a essa natureza de abordagem, seja por meio de *phishing*, manipulação psicológica ou erro operacional. No entanto, esse cenário também destaca uma oportunidade clara de mitigação: a conscientização e o treinamento contínuo em segurança da informação. Assim, investir em programas educativos para colaboradores pode reduzir significativamente a exposição a esses riscos, tornando as pessoas uma linha de defesa eficaz contra ameaças cibernéticas e não uma fragilidade.

7.2 Panorama Brasileiro de Incidentes Cibernéticos

> O CERT.br é um CSIRT Nacional de Último Recurso (National CSIRT of Last Resort), que atua para facilitar a comunicação entre profissionais, especialistas e outras equipes, no país e no exterior, que possam auxiliar no tratamento de um incidente de segurança. O Centro também atua como ponto de contato nacional de último recurso para notificação de incidentes de segurança, principalmente quando um contato mais específico não é conhecido, de forma a auxiliar na análise e encaminhar para os contatos corretos (CERT.br, 2025).

Dados recentes divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) reforçam a criticidade de ameaças, o qual a engenharia social explora, a vulnerabilidade humana. Por meio da imagem 4, verifica-se que de janeiro a agosto de 2025, foram registradas milhares de notificações de tentativas de fraude, com destaque para as subcategorias de *phishing* e *malware*. Acerca disso, o dicionário Houaiss define a palavra fraude como "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". O *phishing*, que representa a forma mais recorrente de engenharia social, acumulou números superiores a 2.000 notificações mensais nos últimos três meses do período analisado, evidenciando sua prevalência e sofisticação crescente. Já os ataques por *malware*, muitos deles também associados a campanhas de engenharia social, apresentaram um aumento expressivo nos meses de junho e julho, sugerindo campanhas coordenadas de disseminação (CERT.br, 2025).

Gráfico 3: Incidentes de fraude reportados ao CERT.br



Fonte: CERT.br (2025).

Vale ressaltar que as notificações recebidas pelo CERT.br são voluntárias, enviadas por CSIRTs (Computer Security Incident Response Teams - grupos de resposta a incidentes), administradores de redes e usuários de Internet. Dessa forma, isso indica que os números apresentados não refletem a totalidade dos incidentes ocorridos no país, mas sim aqueles reportados espontaneamente, o que torna o cenário potencialmente ainda mais alarmante.

Neste contexto, problematiza-se a necessidade urgente de se fortalecer a cultura de segurança da informação nas organizações, especialmente no que tange à conscientização e capacitação dos colaboradores. Ferramentas técnicas são essenciais, mas insuficientes diante de ataques que exploram o comportamento humano. Simulações de *phishing*, treinamentos recorrentes e políticas claras de segurança são algumas das estratégias que podem ser adotadas para mitigar os riscos associados à engenharia social.

8 ESTRATÉGIAS DE PROTEÇÃO E PREVENÇÃO CONTRA ATAQUES DE ENGENHARIA SOCIAL

Os ataques de engenharia social exploram a vulnerabilidade humana, tornando sua detecção e prevenção um dos maiores desafios da segurança da informação. Segundo Bhusal (2021), mesmo com ferramentas avançadas, é extremamente difícil identificar e conter ataques sofisticados. Nesse sentido, a principal linha de defesa contra esse tipo de ameaça está no equilíbrio entre conscientização humana, políticas organizacionais e uso de tecnologias de proteção. Tendo isso em vista, vale ressalvar que o princípio da prevenção de ataques de engenharia social parte da exigência de o indivíduo se manter atento e desconfiado de qualquer interação incomum ou suspeita, visando a segurança tanto individual, quanto digital. Assim, este capítulo tem a finalidade de exibir algumas estratégias de prevenção de ataques de engenharia social.

8.1 Educação, Treinamento e Conscientização (ETA)

Segundo Bhusal (2021), a base de toda prevenção é a Educação, Treinamento e Conscientização (ETA), que busca preparar os indivíduos para reconhecer tentativas de manipulação, adotar comportamentos seguros no tratamento de informações e reagir de forma adequada diante de situações suspeitas. Sob essa ótica, por meio dessa metodologia, os cenários de simulação auxiliam na exposição de possíveis eventos criminosos, por exemplo, ataques de *phishing* por e-mail. Desse modo, o indivíduo que está sendo treinado analisa e aprende com as simulações. Além disso, existem empresas de consultoria que prestam serviços de treinamento direcionado para simulações de ataques de engenharia social, como Hoxhunt, Knowbe4 e Proofpoint.

Esses programas e campanhas recorrentes são de suma importância visto que podem reduzir significativamente a taxa de sucesso de ataques de engenharia social, uma vez que a pessoa pode identificar rapidamente e estará consciente

sobre como lidar com tais ocorrências, em adição, essas ações contribuem para a construção de uma cultura organizacional de segurança (Bhusal, 2021).

8.2 Autenticação Multifator (MFA)

Embora senhas fortes ainda sejam essenciais, criminosos frequentemente conseguem obter credenciais por meio de manipulação psicológica. Nesse contexto, a autenticação multifator (MFA) atua como uma camada extra de proteção, exigindo que o usuário valide sua identidade por outro método, como aplicativo autenticador, biometria ou token físico (Bhusal, 2021). Assim, em conformidade ao Leonardo Alves (2022), “Método de Prevenção ao *Phishing*”, “Essa medida de segurança é altamente eficaz na prevenção da perda de acesso à conta em caso de um ataque bem-sucedido. Mesmo que o usuário caia em um golpe de *phishing* e divulgue seus dados de login, o invasor ainda encontrará uma barreira adicional”, de forma que mesmo que as credenciais sejam comprometidas, o acesso não autorizado pode ser evitado.

8.3 Filtragem de E-mails e Proteção de Domínios

O correio eletrônico permanece sendo o vetor mais explorado em ataques de engenharia social, principalmente por meio do *phishing* e de suas variações. A grande quantidade de informações trocadas por e-mail torna esse canal um alvo altamente atrativo para criminosos. Para mitigar riscos, é essencial a implementação de filtros de segurança avançados, capazes de identificar mensagens suspeitas, bloquear anexos maliciosos e analisar *links* fraudulentos antes de chegarem à caixa de entrada do usuário.

Além disso, protocolos de autenticação de e-mails, como SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e DMARC (*Domain-based*

Message Authentication, Reporting, and Conformance), desempenham papel crucial na prevenção. Esses mecanismos ajudam a verificar a legitimidade do remetente, dificultando a falsificação de domínios confiáveis e elevando a barreira contra ataques de *phishing*. Quando combinados, esses recursos aumentam significativamente a proteção contra mensagens fraudulentas que buscam induzir o usuário ao erro (Alves, 2022).

8.4 Controles de Acesso e Princípio do Menor Privilégio

Outro método fundamental na prevenção de ataques de engenharia social é a aplicação do princípio do menor privilégio, segundo o qual os colaboradores devem possuir apenas o nível de acesso estritamente necessário para desempenhar suas funções. Essa prática reduz a superfície de ataque e limita os danos potenciais em caso de comprometimento de credenciais.

Por exemplo, um funcionário de nível operacional não deve ter acesso a informações estratégicas da empresa ou a sistemas administrativos de alto impacto. Se suas credenciais forem comprometidas, o atacante encontrará barreiras adicionais para avançar no sistema. Conforme preconizado pela NBR ISO/IEC 17799 (ABNT, 2005), auditorias de acesso devem ser realizadas periodicamente para identificar contas inativas, permissões excessivas e potenciais pontos de vulnerabilidade.

8.5 Procedimentos de Relato e Resposta a Incidentes

A resposta rápida a incidentes é essencial para reduzir o impacto de ataques, visto que um ataque de engenharia social pode causar grandes danos em questão de minutos, razão pela qual as organizações precisam adotar planos claros de resposta. Dessa maneira, os funcionários devem ter clareza sobre como e onde

relatar comportamentos suspeitos, seja por e-mail corporativo, portal interno ou linha telefônica dedicada.

Conforme a Agência Brasileira de Inteligência (2022), é fundamental que as organizações disponibilizem canais acessíveis e simples de denúncia que atuem com agilidade na contenção, bloqueio de acessos e investigação do incidente, ao passo que aumenta a possibilidade de identificação dos ataques, precocemente. Ademais, a existência de uma equipe de resposta a incidentes (Incident Response Team) garante que cada notificação seja devidamente investigada, reduzindo o impacto de ataques bem-sucedidos.

8.6 Cartilha - Guia de Boas Práticas Individuais

Além das medidas institucionais, cada indivíduo deve adotar práticas básicas de proteção e seguras. Por isso, em sua “Cartilha de Segurança para Internet”, a CERT.br disponibiliza diversos conteúdos chamados de fascículos, a respeito de segurança da informação, visando conscientizar os usuários acerca dos perigos no ambiente virtual e como se proteger, como golpes à privacidade e segurança em dispositivos móveis, vazamento de dados, entre outros, e não se expor a incidentes de segurança, uma vez que foi criado para educar a respeito de boas práticas nesse meio.

Figura 6 - Página “Fascículos” da Cartilha de Segurança para Internet

Fonte: CERT.br, 2025.

Nesse sentido, inclusive, outros órgãos como a Agência Brasileira de Inteligência (ABIN) e a Autoridade Nacional de Proteção de Dados (ANPD) disponibilizam de forma gratuita também, cartilhas sobre “Guia para Proteção de Conhecimentos Sensíveis” e “Segurança da Informação para Agentes de Tratamento de Pequeno Porte”, respectivamente.

Figura 7 - Cartilha “Guia para Proteção de Conhecimentos Sensíveis”

Fonte: Agência Brasileira de Inteligência (ABIN).

Dessa forma, a ABIN orienta os indivíduos, em seu documento, sobre como se proteger contra ataques de engenharia social. Além disso, o documento da ANPD fornece diversas recomendações de boas práticas e diretrizes para a implementação de normas de proteção, especialmente voltadas para agentes de tratamento de dados de pequeno porte, conforme a LGPD. Essas recomendações são cruciais, pois muitas dessas organizações não dispõem de especialistas na área de proteção de dados pessoais, o que dificulta o cumprimento das exigências de conformidade com a legislação.

Figura 8 - Cartilha “Segurança da Informação para Agentes de Tratamento de Pequeno Porte”

Fonte: Autoridade Nacional de Proteção de Dados (ANPD).

Assim, as cartilhas de segurança promovem uma função importante na conscientização e aprendizado dos usuários no que diz respeito às boas práticas de segurança cibernética, oferecendo uma maneira efetiva na proteção de eventuais crimes cibernéticos.

10 CONCLUSÃO

Esse trabalho de pesquisa buscou responder a seguinte questão: Como os ataques de engenharia social exploram as vulnerabilidades humanas e quais medidas podem ser adotadas para mitigar esses riscos?

O estudo visou compreender o impacto dos ataques de engenharia social na segurança da informação, identificando seus principais tipos, exibindo casos reais noticiados, apresentando estatísticas de relatórios especializados e apontando propostas de prevenção. Além disso, vale ressaltar que o estudo evidenciou obstáculos em encontrar dados concretos das organizações, visto que se referem a dados sensíveis e sigilosos.

O projeto concluiu que há diversos ataques de engenharia social como: *phishing*, *vishing*, *smishing*, *quishing*, *spear phishing, whaling*, *pretexting*, *baiting* e *quid pro quo*. Ao passo que com o avanço da tecnologia, os ataques de engenharia social são cada vez mais vistos e a evolução desses métodos está cada vez mais sofisticada, tendo potencial de provocar impactos financeiros, operacionais e reputacionais severos.

Desse modo, pode-se assumir que os ataques cibernéticos envolvendo engenharia social estão aumentando e tendem a continuar se intensificando, evidenciando a centralidade do fator humano na segurança cibernética.

Compreendeu-se que os sistemas de proteção de segurança modernos não são suficientes para conter ameaças baseadas na manipulação humana, uma vez que, além de empresas, os clientes, colaboradores e indivíduos são alvos de ataques dos engenheiros sociais, explorando brechas de comportamento, falta de conhecimento e falhas de comunicação.

Conclui-se, portanto, que o fator humano continua sendo o elo mais frágil da cadeia de segurança e que a segurança da informação não depende apenas de soluções tecnológicas, mas, principalmente, da conscientização e do preparo das pessoas que interagem com sistemas e dados sensíveis, revelando a importância de uma cultura organizacional voltada à segurança da informação, que inclua treinamentos regulares, simulações de ataques, canais de denúncia e políticas de resposta a incidentes.

Dessarte, como prosseguimento desse estudo sugere-se um trabalho que visa abordar o guia de melhores práticas, bem como o desenvolvimento de um site de tais recomendações, o qual contenha links de instituições oficiais e que contemple orientações do Brasil e no exterior.

11 REFERÊNCIAS

ALVES, Ângela Rayne Nogueira et al. Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital. **Texto Livre**, Belo Horizonte, v. 17, n. 51184, p. 1-17, ago. 2024. Disponível em: https://www.researchgate.net/publication/384163812_Fator_humano_na_seguranca_da_informacao_um_mapeamento_dos_comportamentos_de_risco_no_ambiente_digital. Acesso em: 15 jul. 2025.

ALVES, Leonardo de Moura. **Engenharia Social: Estudo de Ataques e Métodos de Prevenção**. 2024. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Pontifícia Universidade Católica de Goiás, Goiânia, 2024. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/7976/1/TCC%202%20-%20Leonardo%20de%20Moura%20Alves.pdf. Acesso em: 12 ago. 2025.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Engenharia social:** guia para proteção de conhecimentos sensíveis. Brasília: ABIN, 2021. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 21 set. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 17799:** tecnologia da informação – código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. Disponível em: https://www.facom.ufu.br/~william/Disciplinas%202013-1/BSI%20-%20GSI035%20-%20Auditoria%20e%20Seguranca%20da%20Informacao/Materiais%20Auxiliares/NBR%20ISO-IEC%2017799-2005-NORMA.pdf. Acesso em: 19 set. 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022**: Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. 3. ed., versão corrigida em 31 mar. 2023. Rio de Janeiro: ABNT, 2022. Disponível em: https://intranetcomunix.com/wp-content/uploads/2024/07/ABNT_ISO_27001.pdf. Acesso em: 21 set. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo:** segurança da informação para agentes de tratamento de pequeno porte. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf. Acesso em: 20 set. 2025.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2016. Disponível em: https://madmunifacs.wordpress.com/wp-content/uploads/2016/08/anc3a1lise-de-contec3bado-laurence-bardin.pdf. Acesso em: 14 maio 2025.

BHUSAL, C. S. ***Systematic Review on Social Engineering: Hacking by Manipulating Humans***. Journal of Information Security, v. 12, p. 104–114, 2021. DOI: 10.4236/jis.2021.121005.

BRACCO, Matheus. **Sistema financeiro do governo é alvo de invasão cibernética**. *Security Leaders*, 24 abr. 2024. Disponível em: https://securityleaders.com.br/invasao-ao-siafi-tentou-roubar-r-9-milhoes-do-ministerio-da-gestao-e-inovacao. Acesso em: 12 set. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 mar. 2025.

BREDA, F.; BARBOSA, H.; MORAIS, T. ***Social engineering and cyber security***. 2023. Trabalho de Conclusão de Curso (Graduação em Segurança da Informação), São Paulo, 2023 https://doi.org/10.21125/INTED.2017.1008.

CASTELLS, Manuel. **A Sociedade em Rede**. 6. ed. São Paulo: Paz e Terra, 2002. v. 1. Disponível em: https://globalizacaoeintegracaoregionalufabc.wordpress.com/wp-content/uploads/2014/10/castells-m-a-sociedade-em-rede.pdf. Acesso em: 06 mar. 2025.
CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Fascículos da Cartilha de Segurança para Internet**. CERT.br, 2023. Disponível em: https://cartilha.cert.br/fasciculos. Acesso em: 20 set. 2025.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Incidentes notificados ao CERT.br:** incidentes notificados voluntariamente ao CERT.br por CSIRTs, administradores de redes e usuários finais. CERT.br, 2025. Disponível em: https://stats.cert.br/incidentes. Acesso em: 20 set. 2025.

CFO DIVE. ***Scammers siphon $25M from engineering firm Arup in deepfake 'CFO' scam***. 16 maio 2024. Disponível em: https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501. Acesso em: 13 set. 2025.

CIALDINI, Robert B.. **INFLUENCE**: the psychology of persuasion. New York: HyperCollins, 1984. 279 p. Disponível em: https://ia800203.us.archive.org/33/items/ThePsychologyOfPersuasion/The%20Psychology%20of%20Persuasion.pdf. Acesso em: 04 abr. 2025.

CNN BRASIL. **Entenda ataque hacker milionário em prestadora de serviços financeiros**. Disponível em: https://www.cnnbrasil.com.br/nacional/centro-oeste/df/entenda-ataque-hacker-milionario-em-prestadora-de-servicos-financeiros. Acesso em: 15 set. 2025.

CNN. ***British multinational design and engineering firm Arup says it was tricked into paying out $25 million to fraudsters after an elaborate deepfake scam***. 16 maio 2024. Disponível em: <https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk#:~:text=A%20British%20multinational%20design%20and,out%20%2425%20million%20to%20fraudsters.>. Acesso em: 13 set. 2025.

CNN. **MGM diz que ataque cibernético custou US$100 milhões para a empresa**. 5 out. 2023. Disponível em: https://edition.cnn.com/2023/10/05/business/mgm-100-million-hit-data-breach. Acesso em: 12 set. 2025.

DAVENPORT, Thomas; PRUSAK, Laurence. **Conhecimento empresarial**: como as organizações gerenciam seu capital intelectual. 9. ed. Rio de Janeiro: Elsevier, 2003. 237 p. Tradução: Lenke Peres.

FERREIRA, Aurélio Buarque de Holanda. Informação. In: FERREIRA, Aurélio Buarque de Holanda. Miniaurélio: o minidicionário da língua portuguesa dicionário. 7 ed. Curitiba:Positivo, 2008, p. 478.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008. 220 p. Disponível em: https://ayanrafael.com/wp-content/uploads/2011/08/gil-a-c-mc3a9todos-e-tc3a9cnicas-de-pesquisa-social.pdf. Acesso em: 16 abr. 2025.

GOLEMAN, Daniel. **Inteligência emocional**: a teoria revolucionária que redefine o que é ser inteligente. Rio de Janeiro: Objetiva, 2011. 420 p. Tradução: Fabiano Morais. Disponível em: https://ceaf.mpac.mp.br/wp-content/uploads/10-Inteligencia-Emocional-Daniel-Goleman.pdf. Acesso em: 21 maio 2025.

GOVERNO DO BRASIL. **Engenharia social:** como aspectos psicológicos podem se relacionar com golpes e fraudes. GOV, 2024. Disponível em: https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1. Acesso em: 23 set. 2025.

HADNAGY, Christopher. **Social Engineering**: The Science of Human Hacking. 2. ed. Indianapolis: Wiley, 2018. 362 p. Disponível em: http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf. Acesso em: 20 maio 2025.

IBM. **Hackers estão visando cada vez mais concessionárias de automóveis**. 11 jul. 2024. Disponível em: https://www.ibm.com/think/news/hackers-increasingly-targeting-auto-dealers. Acesso em: 12 set. 2025.

IBM. ***O que é phishing?*** IBM Think. São Paulo: IBM, 17 maio 2024. Disponível em: https://www.ibm.com/br-pt/think/topics/phishing. Acesso em: 21 set 2025.

IBM. **Pretexting: o que é e como se proteger**. Disponível em: https://www.ibm.com/br-pt/topics/pretexting. Acesso em: 02 maio 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27002:2022:** Information security, cybersecurity and privacy protection — Information security controls. 3rd ed. Geneva: ISO, 2022. Disponível em: https://www.educacao.pr.gov.br/sites/default/arquivos_restritos/files/documento/2025-08/sd_iso_27002_controles_seguranca_informacao.pdf. Acesso em: 21 nov. 2025.

IPNEWS. **Engenharia social causa trilhões de prejuízos no mundo e avança no Brasil**. 2025. Disponível em: https://ipnews.com.br/engenharia-social-causa-trilhoes-em-prejuizos-no-mundo-e-avanca-no-brasil. Acesso em: 12 set. 2025.

KASPERSKY. ***Ransomware*: o que é e como se proteger**. 2023. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 15 set. 2025.

MITNICK, K. D.; SIMON, W. L. ***The Art of Deception:*** *Controlling the Human Element of Security.* Indianapolis: Wiley, 2002.
MPMT. **Uso de IA aumenta ataques de *phishing***. Cuiabá: Ministério Público do Estado de Mato Grosso, 8 fev. 2024. Disponível em: https://mpmt.mp.br/portalcao/news/1217/135249/uso-de-ia-aumenta-ataques-de-phishing. Acesso em: 21 set. 2025.

O TEMPO. ***Quem é o hacker preso acusado de facilitar roubo de R$1 bilhão em contas no BC***. 4 jul. 2025. Disponível em: https://www.otempo.com.br/brasil/2025/7/4/quem-e-o-hacker-preso-acusado-de-facilitar-roubo-de-r-1-bilhao-em-contas-no-bc. Acesso em: 12 set. 2025.

RAJALIM, S. *Understanding Human Vulnerabilities: A Study on Social Engineering Techniques in Cybersecurity*. **IJRASET**, v. 13, n. 6, p. 1660–1666, 2025. DOI: https://doi.org/10.22214/ijraset.2025.72502.

REUTERS. ***CDK Global cyber outage hits US auto dealers for second day in a row****.* 20 jun. 2024. Disponível em: https://www.reuters.com/technology/cybersecurity/cdks-cyber-outage-hits-us-auto-dealers-second-day-row-2024-06-20. Acesso em: 13 set. 2025.

SALAHDINE, Fatima; KAABOUCH, Naima. *Social engineering attacks: A survey.* ***Future Internet***, Basel, v. 11, n. 4, p. 89, 2019. DOI: https://www.mdpi.com/1999-5903/11/4/89. Acesso em: 25 mar. 2025.

SCHNEIER, Bruce. **Click Here to Kill Everybody**: Security and Survival in a Hyper-connected World. New York: W. W. Norton & Company, 2018. 331 p. Disponível em: https://pt.scribd.com/document/753921128/Click-Here-to-Kill-Everybody-Security-and-Survival-in-a-Hyper-Connected-World. Acesso em: 20 maio. 2025.

SÊMOLA, Marcos. **Gestão da Segurança da informação:** uma visão executiva. 2ª. Ed. Rio de Janeiro: Elsevier, 2014. 171p.

SILVA JÚNIOR, Luiz Carlos. ***Ransomware:*** **análise técnica e prevenção.** 2023. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Universidade Federal de Ouro Preto, Instituto de Ciências Exatas e Aplicadas, João Monlevade, 2023. Disponível em: https://monografias.ufop.br/bitstream/35400000/6049/11/MONOGRAFIA_RansomwareAn%C3%A1liseT%C3%A9cnica.pdf. Acesso em: 14 set. 2025.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores**: princípios e práticas. 2. ed. Rio de Janeiro: Elsevier, 2014. 728 p. Tradução: Arlete Simille Marques. Disponível em: https://www.kufunda.net/publicdocs/Segurança%20de%20Computadores%20(WILLIAM%20STALLINGS).pdf. Acesso em: 21 maio 2025.

TRIBUNAL DE CONTAS DO ESTADO DO ESPÍRITO SANTO. ***Deepfakes*** **e a IA para manipulação digital**. Portal de Ajuda TCE-ES. Disponível em: https://www.tcees.tc.br/ajuda/deepfakes-e-a-ia-para-manipulacao-digital/. Acesso em: 23 set. 2025.

UOL Economia. **TCU:** Há indícios de falhas sistêmicas no SIAFI e necessidade urgente de aprimoramento. 31 jul. 2024. Disponível em: https://economia.uol.com.br/noticias/estadao-conteudo/2024/07/31/tcu-ha-indicios-de-falhas-sistemicas-no-siafi-e-necessidade-urgente-de-aprimoramento.htm. Acesso em: 12 set. 2025.

U*.S. ATTORNEY'S OFFICE FOR THE NORTHERN DISTRICT OF CALIFORNIA.* ***Two Men Plead Guilty to Money Laundering in Connection with Phishing Scams that Targeted SF-Based Company****.* 2024. Disponível em: https://www.justice.gov/usao-ndca/pr/two-men-plead-guilty-money-laundering-connection-phishing-scams-targeted-sf-based. Acesso em: 15 set. 2025.

USECURE. Os exemplos mais comuns de um e-mail de phishing. **Blog USECURE**, [s.d.]. Disponível em: https://blog.usecure.io/pt/the-most-common-examples-of-a-phishing-email. Acesso em: 4 nov. 2025.

VERIZON. **2025** ***Data Breach Investigations Report*** **(DBIR).** New York: Verizon Enterprise, 2025. Disponível em: http://verizon.com/dbir. Acesso em: 28 mar. 2025.

YIN, R. K. **Estudo de caso**: planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015. Disponível em: http://maratavarespsictics.pbworks.com/w/file/fetch/74304716/3-YIN-planejamento_metodologia.pdf. Acesso em: 14 maio 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020. Cap. 1, p. 18. Tradução de George Schlesinger. Disponível em: https://www.intrinseca.com.br/upload/livros/1ºCap-AEraDoCapitalismoDeVigilancia.pdf. Acesso em: 01 maio 2025.