UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

DEMIS DOUGLAS GOMES SANTOS

Framework de Contrainteligência em Engenharia Social: Mitigando Efeitos e Aprimorando Defesa

João Pessoa/PB
2024

DEMIS DOUGLAS GOMES SANTOS

Framework de Contrainteligência em Engenharia Social: Mitigando Efeitos e Aprimorando Defesa

Dissertação apresentada ao Centro de Informática - CI da Universidade Federal da Paraíba - UFPB para a obtenção do título de Mestre em Informática pelo Programa de Pós-Graduação em Informática - PPGI.

Área de concentração: Ciências da Computação
Linha de Pesquisa: Sistemas de Computação

Orientador: Prof. Dr. Gustavo Henrique Matos Bezerra Motta

Coorientador: Prof. Dr. Rubens Elias Duarte Nogueira

João Pessoa/PB

2024

Catalogação na publicação
Seção de Catalogação e Classificação

S237f Santos, Demis Douglas Gomes.
Framework de contrainteligência em engenharia social : mitigando efeitos e aprimorando defesa / Demis Douglas Gomes Santos. - João Pessoa, 2024.
119 f. : il.

Orientação: Gustavo Henrique Matos Bezerra Motta.
Coorientação: Rubens Elias Duarte Nogueira.
Dissertação (Mestrado) - UFPB/CI.

1. Segurança digital. 2. Engenharia social. 3. Contrainteligência. 4. Vulnerabilidades humanas. 5. Cibersegurança. I. Motta, Gustavo Henrique Matos Bezerra. II. Nogueira, Rubens Elias Duarte. III. Título.

UFPB/BC CDU 004.056(043)

Elaborado por Walqueline da Silva Araújo - CRB-15/514

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

Ata da Sessão Pública de Defesa de Dissertação de Mestrado de Demis Douglas Gomes Santos, candidato ao título de Mestre em Informática na área de Sistemas de Computação, realizada em 30 de janeiro de 2025.

Aos trinta dias do mês de janeiro do ano de dois mil e vinte e cinco, às quatorze horas, no Centro de Informática da Universidade Federal da Paraíba, reuniram-se os membros da Banca Examinadora constituída para julgar o Trabalho Final do discente Demis Douglas Gomes Santos, vinculado a esta Universidade sob a matrícula nº 20221014810, candidato ao grau de Mestre em Informática, na área de *"Sistemas de Computação"*, na linha de pesquisa *"Sistemas de Computação"*, do Programa de Pós-Graduação em Informática. A comissão examinadora foi composta pelos professores: Gustavo Henrique Matos Bezerra Motta, Orientador e Presidente da banca; Gledson Elias da Silveira, Examinador Interno; Ozonias de Oliveira Brito Junior, Examinador Externo à Instituição. Dando início aos trabalhos, o Presidente da Banca cumprimentou os presentes, comunicou a finalidade da reunião e passou a palavra ao candidato para que ele fizesse a exposição oral do trabalho de dissertação intitulado "**Framework de Contrainteligência em Engenharia Social: Mitigando Efeitos e Aprimorando Defesa**". Concluída a exposição, o candidato foi arguido pela Banca Examinadora que emitiu o seguinte parecer: "***aprovado***". Do ocorrido, eu, Gilberto Farias de Sousa Filho, coordenador do Programa de Pós-Graduação em Informática, lavrei a presente ata que vai assinada por mim e pelos membros da Banca Examinadora. João Pessoa, 30 de janeiro de 2025.

gov.br Documento assinado digitalmente
GILBERTO FARIAS DE SOUSA FILHO
Data: 12/02/2025 10:46:31-0300
Verifique em https://validar.iti.gov.br

Gilberto Farias de Sousa Filho
Coordenador do Programa de Pós-Graduação em Informática

gov.br Documento assinado digitalmente
GUSTAVO HENRIQUE MATOS BEZERRA MOTTA
Data: 03/02/2025 12:38:44-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Gustavo Henrique M. Bezerra Motta
Orientador (PPGI-UFPB)

gov.br Documento assinado digitalmente
GLEDSON ELIAS DA SILVEIRA
Data: 04/02/2025 14:55:59-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Gledson Elias da Silveira
Examinador Interno (PPGI-UFPB)

gov.br Documento assinado digitalmente
OZONIAS DE OLIVEIRA BRITO JUNIOR
Data: 11/02/2025 15:32:32-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Ozonias de Oliveira Brito Junior
Examinador Externo à Instituição (UFPI)

Dedico este trabalho à minha filha, Cecília; à minha saudosa mãe, Dona Lia (in memoriam); de forma especial, ao meu orientador, Gustavo Motta; aos professores do PPGI; e aos colegas e amigos, cujas contribuições foram inestimáveis ao longo da minha jornada.

À minha mãe (in memoriam), cuja amizade, companheirismo, esforço e amor foram fundamentais em minha formação pessoal e intelectual. A ela devo o ensinamento de pensar de forma crítica, agir com responsabilidade, analisar a vida com profundidade e valorizar cada momento. Sua orientação também me ensinou a não me manter inerte diante de injustiças, sejam elas cometidas contra mim ou contra terceiros.

À minha filha, Cecília Brunnet, expresso minha mais profunda gratidão por sua paciência e compreensão durante minha ausência, especialmente em uma fase tão importante de sua vida.

Ao professor Gustavo Henrique Matos Bezerra Motta, minha eterna gratidão por sua confiança e por sua orientação precisa e inestimável. Desde nosso primeiro encontro, sua dedicação e sabedoria foram essenciais não apenas para a execução deste trabalho, mas também para meu desenvolvimento pessoal e acadêmico. Seu apoio incansável foi um guia que me permitiu enfrentar desafios e evoluir continuamente, tanto como estudante quanto como ser humano.

Aos amigos do judô e do jiu-jitsu, agradeço pela compreensão em relação às minhas ausências nos tatames.

Aos professores do PPGI, especialmente ao Prof. Dr. Alisson Vasconcelos de Brito. Ao Prof. Dr. Clauirton de Albuquerque Siebra, pela condução competente da coordenação do PPGI, juntamente com o Prof. Dr. Gilberto Farias de Sousa Filho. Ao Prof. Dr. Fernando Menezes Matos, coordenador do PPGI em meu primeiro ano, e ao vice-coordenador, Prof. Dr. Iguatemi Eduardo da Fonseca, que me receberam com grande acolhimento no programa. Ao Prof. Dr. Gledson Elias da Silveira, que, durante a banca de qualificação, ofereceu contribuições valiosas, abrindo meus olhos para aspectos antes não considerados. Ao Prof. Dr. Guido Lemos de Souza Filho, pela sua postura firme na defesa do acesso à educação de qualidade. Ao Prof. Dr. Leandro Carlos de Souza, por suas orientações em momentos difíceis ao longo deste ciclo acadêmico. À Profª Dra. Liliane dos Santos Machado, por sua incansável dedicação na busca de palestrantes de renome durante a disciplina de seminários. Ao Prof. Dr. Lucídio dos Anjos Formiga Cabral, por sua valiosa contribuição à minha formação. À Profª Dra. Natasha Correia Queiroz Lino, por sua dedicação exemplar, que, mesmo em tempos de pandemia e com duas filhas pequenas, sempre esteve presente em suas aulas, sem atrasos ou ausências. Ao Prof. Dr. Tiago Pereira do Nascimento, que foi o segundo docente que mais contribuiu para o desenvolvimento desta pesquisa, meus sinceros agradecimentos.

Aos técnicos administrativos do PPGI, Maria Alice Ferreira Bezerra e Gean Paulo Barros, pela prestativa assistência nos momentos de dúvidas quanto aos trâmites administrativos.

Aos colegas do PPGI — Ana Maria Pinto da Silva Nascimento, Antonio Teixeira Neto, Elvis Silva de Souza, Erikson Carlos Ramos, Frederico Augusto Santos Brasil, Gabriel da Silva Belarmino, Jaqueline Donin Noleto, José Edson de Souto, Larrysa Mirelly Rosendo Figueiredo, Matheus Lira Sartor, Natália dos Santos Costa Neves, Victor Fellipe dos Santos Gomes — pela criação de um ambiente colaborativo e descontraído, propício à troca de ideias e ao desenvolvimento criativo.

Aos amigos do IEEE, em especial aos colegas do departamento de Cibersegurança, que esteve sob minha liderança durante este período. A colaboração e o compromisso de cada um de vocês foram fundamentais para o sucesso de nossos projetos. Agradeço profundamente pela parceria, pelo empenho e pelas valiosas contribuições, que não apenas aprimoraram nossas habilidades técnicas, mas também fortaleceram nossos laços de amizade e profissionalismo. Sinto-me honrado por ter trabalhado com uma equipe tão talentosa e dedicada. Obrigado a todos por essa jornada enriquecedora.

À Universidade Federal da Paraíba, pelos recursos disponibilizados em apoio a esta pesquisa.

À CAPES, pelo financiamento que tornou este trabalho possível.

A todos os que, de alguma forma, contribuíram para a realização deste trabalho, deixo meu mais sincero agradecimento.

Muito obrigado!

"Ninguém tende a uma determinada coisa pelo desejo e pelo estudo, se tal coisa não lhe for previamente conhecida."

(São Tomás de Aquino – Santo e Doutor da Igreja, rogai por nós!)

Resumo

DEMIS, DOUGLAS GOMES SANTOS. Framework de Contrainteligência em Engenharia Social: Mitigando Efeitos e Aprimorando Defesa. 2024. 120 f. Dissertação de Mestrado em Informática – Centro de Informática - CI, Universidade Federal da Paraíba - UFPB, João Pessoa/PB, 2024.

A segurança digital tornou-se um tema sensível e central na atual sociedade, na qual as interações humanas e tecnológicas são cada vez mais frequentes e complexas. Dentre os riscos emergentes, destaca-se a engenharia social, técnica que se baseia na manipulação psicológica de indivíduos para obter acesso indevido a informações ou sistemas computacionais. Essa prática, que explora vulnerabilidades humanas, possui ampla aplicabilidade tanto no ambiente digital quanto no físico, sendo utilizada em diversos contextos com o objetivo de obter vantagens ilícitas. Como contramedida, surge a contrainteligência, um conjunto de estratégias e práticas voltadas à mitigação dos danos provocados por ações de engenharia social, buscando proteger indivíduos e organizações da exploração de suas fragilidades comportamentais. A presente pesquisa tem como principal objetivo investigar a gênese da engenharia social e sua forma de aplicação, bem como avaliar se a contrainteligência é efetiva na mitigação dos seus efeitos. Para isso, o estudo parte de uma análise do estado da arte sobre o tema, propondo um conjunto de contramedidas organizadas em um framework conceitul, com base em fontes primárias e secundárias. As fontes primárias incluem trabalhos acadêmicos relevantes na área de segurança da informação e psicologia social, enquanto as fontes secundárias são reportagens e matérias veiculadas em meios de comunicação com credibilidade social, que retratam casos reais de ataques baseados em engenharia social. A metodologia adotada é de natureza exploratória e qualitativa, com foco na análise de estudos de caso envolvendo pessoas físicas e jurídicas que tenham sido alvo de ataques de engenharia social, sejam eles bem-sucedidos ou não. Por meio desses casos, busca-se compreender os mecanismos utilizados pelos atacantes, os fatores humanos explorados e a eficácia das respostas adotadas. A partir dessa análise, os frameworks propostos são testados e ajustados para refletir a realidade dos desafios enfrentados na proteção contra esse tipo de ameaça. Os resultados obtidos permitirão identificar padrões de comportamento explorados nas vítimas, bem como pontos vulneráveis nas práticas de segurança de organizações e indivíduos. Com isso, será possível avaliar a efetividade das medidas de contrainteligência sugeridas, contribuindo para o desenvolvimento de estratégias mais robustas de prevenção e resposta a ataques de engenharia social. Conclui-se que, diante da crescente sofisticação das ameaças baseadas na exploração do fator humano, é fundamental desenvolver e adotar práticas de contrainteligência como ferramenta estratégica de defesa. A pesquisa pretende, assim, oferecer uma contribuição relevante tanto para o meio acadêmico quanto para profissionais da área de segurança da informação, fortalecendo o debate e a aplicação de medidas preventivas eficazes no contexto da segurança digital contemporânea.

Palavras-chaves: Engenharia Social. Contrainteligência. Segurança Digital. Vulnerabilidades Humanas. Estratégias de Cibersegurança.

Abstract

DEMIS, DOUGLAS GOMES SANTOS. **Counterintelligence in Social Engineering: Mitigating Effects and Improving Defense.** 2024. 120 p. Master's Dissertation in Informatics - Informatics Center - IC, Federal University of Paraíba - FUPB, João Pessoa/PB, 2024.

Digital security has become a sensitive and central issue in today's society, where human and technological interactions are increasingly frequent and complex. Among the emerging risks, social engineering stands out as a technique based on the psychological manipulation of individuals to gain unauthorized access to information or computer systems. This practice, which exploits human vulnerabilities, is widely applicable in both digital and physical environments and is used in various contexts to obtain illicit advantages. As a countermeasure, counterintelligence emerges—a set of strategies and practices aimed at mitigating the damage caused by social engineering actions, seeking to protect individuals and organizations from the exploitation of their behavioral weaknesses. This research aims to investigate the origins of social engineering and how it is applied, as well as to assess whether counterintelligence is effective in mitigating its effects. To achieve this, the study is grounded in a state-of-the-art analysis on the subject and proposes a set of countermeasures organized into conceptual frameworks, based on primary and secondary sources. Primary sources include academic works relevant to the fields of information security and social psychology, while secondary sources consist of news reports and articles from reputable media outlets that describe real cases of social engineering attacks. The methodology adopted is exploratory and qualitative in nature, focusing on case studies involving individuals and organizations that have been targeted by social engineering attacks, whether successful or not. Through these cases, the study seeks to understand the mechanisms used by attackers, the human factors exploited, and the effectiveness of the responses implemented. Based on this analysis, the proposed frameworks are tested and adjusted to reflect the real-world challenges of protecting against such threats. The results are expected to identify behavioral patterns exploited in victims, as well as vulnerabilities in the security practices of individuals and organizations. This will allow for an evaluation of the effectiveness of the suggested counterintelligence measures, contributing to the development of more robust prevention and response strategies against social engineering attacks. It is concluded that, given the increasing sophistication of threats based on the exploitation of the human factor, it is essential to develop and adopt counterintelligence practices as a strategic defense tool. This research thus aims to offer a relevant contribution to both academia and information security professionals, strengthening the debate and application of effective preventive measures in the context of contemporary digital security.

Keywords: Social Engineering. Counterintelligence. Digital Security. Human Vulnerabilities. Cybersecurity Strategies.

Lista de figuras

Sumário

1 Introdução

Este capítulo está estruturado de forma lógica e progressiva, com o objetivo de proporcionar ao leitor uma compreensão clara do tema e do caminho seguido ao longo da dissertação. Na Seção 1.1, apresenta-se a definição do tema principal do estudo, com uma abordagem abrangente que busca contextualizar e introduzir os conceitos centrais relacionados à Engenharia Social e à Contrainteligência. Essa introdução tem o intuito de oferecer uma visão holística sobre o objeto de estudo, destacando sua relevância no cenário atual da segurança digital. A Seção 1.2 dedica-se a explicitar a motivação que impulsionou a realização deste trabalho. Aqui são apresentados os fatores práticos, acadêmicos e sociais que justificam a escolha do tema, além das lacunas percebidas na literatura e na prática profissional. Em seguida, a Seção 1.3 delineia de forma clara o objetivo geral da dissertação, bem como os objetivos específicos, que juntos guiam o desenvolvimento da pesquisa e a construção das propostas apresentadas. Por fim, a Seção 1.4 descreve a estrutura dos capítulos da dissertação, explicando brevemente o conteúdo de cada um e como eles se inter-relacionam para compor uma análise coesa e aprofundada sobre o tema.

1.1 Definição do tema

A Engenharia Social é um problema clássico de acordo com Zheng *et al.* (2019a), com larga aplicação no atual mundo moderno e digital, visto que os mais avançados sistemas de segurança não conseguem realizar uma defesa eficaz contra este tipo de técnica em virtude de sua atuação ocorrer através de uma ação direta contra o humano e seus frágeis sentimentos. Nesse contexto, o uso de contrainteligência a fim de obter a segurança da informação é uma das habilidades sociais que pode promover a redução dos danos causados em decorrência do uso ofensivo de engenharia social. Como definição, tem-se que "Resumidamente, a engenharia social é um tipo de ataque em que o atacante explora a vulnerabilidade humana através das redes sociais de interação para violar a segurança do ciberespaço. " (WANG; ZHU; SUN, 2021).

A contrainteligência segundo (PAICU, 2023), foi definida em seu trabalho como um conjunto de atividades e medidas realizadas por uma organização, como uma agência de

inteligência ou um governo, para identificar, neutralizar e prevenir ameaças ou atividades de inteligência adversárias. Os autores Zheng *et al.* (2019a), tentam trazer um outro prisma, alegando que a contrainteligência é o ramo da inteligência que se concentra em proteger as informações e operações próprias de uma organização contra espionagem, sabotagem, infiltração e outros tipos de atividades hostis conduzidas por agências de inteligência estrangeiras, grupos terroristas, criminosos cibernéticos e outros atores maliciosos. A contrainteligência envolve a coleta de informações sobre as atividades desses adversários, bem como a implementação de medidas de segurança para mitigar riscos e proteger os interesses da organização.

Tendo como referência a Agência Brasileira de Inteligência ABIN (2020), a qual define que a Contrainteligência tem como atribuições a produção de conhecimentos e a realização de ações voltadas para a proteção de dados, conhecimentos, infraestruturas críticas, comunicações, transportes, tecnologias de informação, além outros ativos sensíveis e sigilosos de interesse do Estado e da sociedade, ainda segundo a ABIN (2020), o trabalho desenvolvido pela Contrainteligência tem foco na defesa contra ameaças como a espionagem, a sabotagem, o vazamento de informações e o terrorismo as quais podem ser patrocinadas por instituições, grupos ou governos estrangeiros, esta, é uma outra definição trazida em ambito nacional para o mesmo tema. No Brasil a atuação da Contrainteligência ultrapassa os limites da ABIN e do SISBIN, passando a contribuir para a salvaguarda do patrimônio nacional sob a responsabilidade de instituições das mais diversas áreas, consideradas de interesse estratégico para a segurança e para o desenvolvimento nacional.

Em outras palavras, de um lado a parte atacante se utiliza da engenharia social para obter informações ou realizar ações comprometedoras por via interposta no intuito de romper o perímetro de segurança físico ou digital e fazer uso malicioso com finalidades diversas e, por outro lado, a parte oposta diz respeito a quem tenta se defender utilizando-se de contrainteligência para reduzir os riscos a exposição desse tipo de atuação ofensiva.

Na comunidade de segurança da informação, pesquisadores como Sirigiri *et al.* (2023), Tyagi *et al.* (2023) e Oveh e Aziken (2022) apontam que a engenharia social é uma das técnicas de ataque mais aplicadas e é um ataque popular desde a década de 1970. Em comparação ao ataque de força bruta, que é um ataque clássico a computadores com o intuito de quebra de senha por força bruta e software de exploração de vulnerabilidades,

ataques de engenharia social concentram-se em explorar vulnerabilidades nos sentimentos humanos para que se possa transpor uma barreira de segurança, sem ter que travar uma luta contra o firewalls ou antivírus por codificação maliciosa.

Isso exposto, é importante destacar que nenhum sistema computacional opera de forma totalmente independente da supervisão ou interação humana. Até o momento da escrita deste trabalho, todos os sistemas existentes dependem, em maior ou menor grau, de algum nível de intervenção humana. Como afirmam Martínez (2019), tratam-se de sistemas sociotécnicos, ou seja, compostos pela interação entre componentes técnicos e sociais.

Essa característica os torna suscetíveis a falhas humanas, sobretudo quando sentimentos e fatores comportamentais são explorados por atacantes por meio da engenharia social. A natureza vulnerável desses fatores humanos faz da engenharia social uma ameaça constante e universal à cibersegurança.

Em muitos casos, os ataques são simples em sua execução, como uma ligação telefônica em que o atacante se passa por um agente bancário para obter informações sigilosas da vítima. No entanto, com o avanço das tecnologias e a transformação do ambiente digital, a aplicação da engenharia social tornou-se ainda mais preocupante.

O estudo de Hoque *et al.* (2021) reforça essa gravidade ao apontar que os Sites de Redes Sociais (SRSs), a comunicação móvel, a Internet Industrial e a Internet das Coisas (IoT) não apenas produzem vastas quantidades de informações sobre pessoas e dispositivos, como também ampliam as possibilidades e caminhos para a realização de ataques.

Complementando essa visão, Alqarni, Algarni e Xu (2016) e Ansari *et al.* (2022) convergem na ideia de que é necessário adotar um comportamento proativo de proteção, ainda que sob uma perspectiva distinta da usual. Eles enfatizam que a mitigação da eficácia da engenharia social depende do modo como as informações, especialmente aquelas disponíveis em redes sociais, são geridas e protegidas.

Esse comportamento desejado alinha-se ao conceito de contrainteligência, que, segundo Ariyo e Zheng (2022), configura-se como uma conduta emergente e essencial para neutralizar os riscos associados à engenharia social.

1.2 Motivação

A motivação deste trabalho nasce da crescente eficácia — cada vez mais acentuada a cada ano — do uso da engenharia social como técnica para obtenção de vantagens indevidas ou acesso a informações sensíveis e confidenciais. Essa realidade é evidenciada por diversos estudos, como apontam (WANG; ZHU; SUN, 2021), (QIN *et al.*, 2017), (KIM; PAN; PARK, 2020) e (LEE *et al.*, 2021).

No contexto brasileiro, tais informações são também definidas juridicamente. A Lei Federal nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), descreve no artigo quinto, item dois, que dado pessoal sensível é aquele que trata da origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dados relativos à saúde, à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural (BRASIL, 2018). Em outras palavras, dados sensíveis correspondem a informações pessoais e privadas que, quando mal utilizadas ou expostas, podem gerar sérios prejuízos à privacidade e à segurança dos indivíduos.

Apesar da crescente sofisticação das ameaças, nota-se que a fragilidade dos sistemas informáticos, sobretudo na interface entre humanos e máquinas, permanece pouco explorada pela pesquisa científica. A dimensão emocional envolvida nessas interações, conforme discutido por Hijji e Alam (2021), ainda não recebe a devida atenção dentro do campo da segurança da informação. Essa observação está alinhada com os apontamentos de Wang, Zhu e Sun (2021) e Raja *et al.* (2022), os quais afirmam que a gênese da engenharia social ainda não constitui um campo de pesquisa plenamente consolidado.

Para Williams, Bleiman e Rege (2022), a relevância do tema é tamanha que a engenharia social deveria integrar o currículo de todos os cursos de computação. Já Hossain

et al. (2022) destaca que o letramento digital representa um dos caminhos mais promissores para garantir um ambiente digital mais seguro e confiável. Em síntese, os autores citados convergem na ideia de que o conhecimento aprofundado sobre táticas de engenharia social é essencial para o desenvolvimento de estratégias de contrainteligência eficazes e eficientes.

Diante disso, torna-se evidente a importância de ampliar os estudos sobre engenharia social e seus desdobramentos, especialmente no que diz respeito ao papel estratégico da contrainteligência. Compreender a origem, os mecanismos e os impactos dessa técnica é essencial não apenas para o meio acadêmico, mas também para a sociedade como um todo, considerando os prejuízos sociais e econômicos que ataques baseados em engenharia social podem causar a indivíduos, instituições e organizações.

1.3 Objetivo

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é delinear um framework de contrainteligencia com o objetivo de mitigar os ataques de engenharia social com base no framework da literatura que apresenta a genese dos ataques de engenharia social no prisma do atacante.

1.3.2 Objetivos Específico

Os objetivos específicos referentes ao presente estudo estão listados adiante:

- a) Realizar um levantamento sobre o estado da arte do tema estudado.
- b) Identificar a partir da literatura um framework conceitual em sua aplicação e que carregue consigo a gênese da engenharia social e a exploração do fator humano.
- c) Propor a ideia de um framework conceitual de contrainteligência com o intuito de mitigar os danos causados por engenharia social, tendo base todo o arcabouço teórico do estado da arte no momento.

- d) Propor recomendações pontuais com o objetivo de mitigar os danos causados por engenharia social.

1.4 Estrutura da Dissertação

A presente dissertação está organizada de forma a conduzir o leitor por uma trajetória lógica e progressiva, que favoreça a compreensão aprofundada do tema e de suas implicações no campo da segurança da informação. A seguir, apresenta-se a estrutura adotada para os capítulos que compõem este trabalho:

- O **Capítulo 1** é dedicado à *Introdução*. Nele, são apresentados o contexto da pesquisa, a delimitação do problema, os objetivos geral e específicos, a justificativa do estudo e a descrição da estrutura adotada para a dissertação.

- No **Capítulo 2**, é realizada a *Fundamentação Teórica*. Esta seção contempla uma análise bibliográfica abrangente sobre os conceitos de engenharia social, contrainteligência e suas aplicações práticas. O capítulo visa fornecer um arcabouço conceitual sólido que sustenta a proposta desenvolvida nesta pesquisa.

- O **Capítulo 3** trata do delineamento do *Framework de Contrainteligência em Engenharia Social*. Nele, são apresentados tanto os fundamentos teóricos quanto os aspectos práticos que embasam a construção do framework proposto. Essa seção representa o núcleo conceitual do trabalho, conectando teoria e aplicação.

- No **Capítulo 4**, descreve-se em detalhes a *Metodologia* adotada para a condução da pesquisa. A abordagem utilizada é de natureza qualitativa e exploratória, com base em entrevistas individuais. Este capítulo apresenta os procedimentos de coleta, análise e tratamento dos dados, além de explicar os critérios de seleção dos participantes e os instrumentos utilizados.

- O **Capítulo 5** é voltado à *Discussão e Análise dos Resultados*. Com base nas entrevistas realizadas, é feita uma interpretação crítica dos dados obtidos, com destaque para

os principais *insights* revelados pelos participantes. Esta análise busca aprofundar a compreensão sobre o fenômeno estudado e validar a aplicação do framework proposto.

- O **Capítulo 6** apresenta os *Resultados Finais*. Aqui, são consolidadas as descobertas obtidas ao longo da pesquisa, relacionando-as diretamente aos objetivos definidos na introdução. O capítulo oferece uma visão ampla e integrada dos resultados alcançados, contribuindo para a avaliação da eficácia do framework frente ao problema investigado.

- Por fim, no **Capítulo 7**, são expostas as *Considerações Finais*. Essa seção propõe uma síntese dos principais achados da pesquisa, destaca suas contribuições teóricas e práticas e aponta caminhos possíveis para investigações futuras. Também são discutidas as limitações do estudo e reflexões críticas sobre os resultados obtidos, com o intuito de enriquecer o debate acadêmico sobre o tema.

2 Fundamentação Teórica

Tendo como base as questões levantadas na problematização apontadas na definição do tema e motivação deste trabalho e as direções apontadas nos objetivos do capítulo anterior, esta pesquisa exibe um arcabouço teórico baseado em dois temas principais. O primeiro e maior deles é uma visão holística da técnica de engenharia social e seus meandros. O segundo tema, a contrainteligência, situa-se de forma antagônica ao primeiro, como meio para mitigar os efeitos da engenharia social.

A estrutura deste referencial teórico discute, inicialmente, na seção 2.1, o conceito de engenharia social, que é primordial à compreensão deste trabalho, colocando um prisma e situando o ambiente desta pesquisa. Na subseção 2.1.1, separamos as fases da execução conceitual da técnica de engenharia social, estabelecendo assim, um passo a passo sobre seu funcionamento. Na subseção 2.1.2, são apresentados os dez principais tipos de ataques de engenharia social com suas técnicas combinadas. Na subseção 2.1.3, explicita-se a interdisciplinariedade da engenharia social para o bom emprego da técnica. Na subseção 2.1.4, é demonstrado como a engenharia social atua com diversas conexões com sociológicas, psicológicas, e até mesmo com a neurociência e comportamento humano, utilizando-se de meios digitais e físicos.

Na seção 2.2, coloca-se o conceito de contrainteligência conforme o estado da arte na altura da escrita deste trabalho, no qual, desde já, aponta-se a escassez de trabalhos acadêmicos sobre o tema. Tratamos de forma análoga os frameworks (MICE+G, RASCLS), abordados na pesquisa Burkett (2013), encontrados na literatura para trazer a esta pesquisa.

Por fim, na última seção em 2.3, colocamos algumas considerações finais acerca do arcabouço teórico trazido a esta pesquisa.

2.1 Engenharia Social

A engenharia social é uma forma de ataque que compreende a aplicação de técnicas que visam manipular e explorar a psicologia humana para obter informações, influenciar

comportamentos ou obter acesso não autorizado a sistemas e recursos (GRBIC; DUJLOVIC, 2023). Baseia-se na interação e manipulação das pessoas, ao invés de explorar diretamente vulnerabilidades técnicas (EFTIMIE; MOINESCU; RACUCIU, 2022).

Os engenheiros sociais, geralmente, atacam utilizando táticas de persuasão, manipulação emocional, intimidação ou engano para convencer pessoas a realizar ações específicas (WANG; ZHU; SUN, 2021). Essas ações podem incluir a divulgação de senhas, acesso a sistemas protegidos, revelação de informações pessoais ou corporativas sensíveis (DAVIS; GRANT, 2023). Desse modo, pode-se ter como referência o uso variado da engenharia social, desde ataques direcionados a indivíduos ou organizações específicas até campanhas mais amplas, como *phishing* em massa ou fraudes por telefone. Ela explora a confiança e a tendência natural das pessoas em seguir instruções ou fornecer informações quando solicitadas por uma fonte aparentemente legítima (SANCHEZ-PANIAGUA; FERNANDEZ, 2022).

Entretanto, isso não significa que atacar via engenharia social seja um trabalho fácil, pois implica o atacante possuir habilidades sociais de manipulação e ludíbrio para obter informações ou realizar ações através de suas vítimas. Tais atacantes devem ser hábeis em manipular suas vítimas, como mágicos, atuando para obter informações sensíveis (UPLENCHWAR *et al.*, 2022). Em geral, as técnicas de manipulação visam obter a confiança da vítima, por exemplo, com a personificação de uma boa pessoa, para ter acesso a dados, etc. De acordo com (HOSSAIN *et al.*, 2022), a maioria das ameaças de ataques cibernéticos é resultado de engenharia social que, embora exija menos conhecimento técnico, é um método eficaz e não deve ser subestimado. Apenas 3% dos *malwares* tentam explorar aspectos exclusivamente técnicos, os outros 97% visam os usuários por meio de engenharia social (DAVIS; GRANT, 2023). Para (GONG, 2023), a maioria dos atacantes são hábeis nos testes de vulnerabilidades em sistemas complexos e seguros e possuem alta probabilidade de sucesso em suas incursões, nas quais conseguem encontrar pontos fracos em sistemas, redes, servidores, etc. Esses dois trabalhos apontam que a união de conhecimentos técnicos em explorar vulnerabilidades com a engenharia social potencializa o sucesso da investida ofensiva.

A Figura 1 ilustra sucintamente o framework conceitual proposto por (WANG; ZHU; SUN, 2021) para explicar como ocorrem ataques de engenharia social. Visando alcançar um objetivo, um atacante emprega um método de ataque que tem por base

Figura 1 – **Framework conceitual para explicar a ocorrência ataques de engenharia social. Fonte: (WANG; ZHU; SUN, 2021).**

um mecanismo de ação que explora alguma vulnerabilidade da vítima, que resulta em consequências (e.g., revelação de informações sensíveis, realização de ações críticas para segurança) que, direta ou indiretamente, permitem ao atacante realizar o objetivo pretendido.

De forma complementar, a Figura 1, apresenta dois prismas, o primeiro sendo o prisma do atacante e o prisma da vítima. Sob o prisma do atacante, podemos dizer que ele cria e executa o ataque com o objetivo de alcançar seu propósito, utilizando um método que concretiza essa intenção. Sob o prisma da vítima, suas vulnerabilidades humanas contribuem para as consequências do ataque. O autor sugere que a própria vítima, ao ser manipulada, pode ser responsável pelo sucesso do ataque. Por fim, o mecanismo de ação que opera em ambos os prismas, consolidando o objetivo do ataque, consiste em um método que explora diretamente as vulnerabilidades humanas específicas, resultando nas consequências do ataque.

2.1.1 Funcionamento da Engenharia Social

Como discutido acima, o método de engenharia social não utiliza algoritmos complexos e ferramentas de exploração de vulnerabilidades para cometer ataques e crimes, em vez disso, tira proveito de técnicas de manipulação das vítimas, colocando-o-as em uma falsa percepção da realidade, levando-as a entregar as informações necessárias ao ato antijurídico. Os ataques de engenharia social para Mambina, Ndibwile e Michael (2022), compreendem os seguintes estágios:

a) **Preparação:** O ato de preparação é o principal passo na engenharia social e este se divide em oito partes de igual importância.

1 **A coleta de informações** na qual, os atacantes pesquisam e coletam informações sobre a vítima ou a organização que desejam atingir. Eles podem usar fontes abertas, como redes sociais, sites públicos e até mesmo informações disponíveis em páginas de funcionários das empresas.

2 Em sequência, tem-se **criação de personas falsas**, com a criação de perfis fictícios em redes sociais e fóruns para estabelecer confiança com suas vítimas. Essas personas podem se passar por colegas de trabalho, amigos ou profissionais de confiança.

3 No terceiro passo, é realizado o **estudo do alvo**, os atacantes podem estudar o comportamento, os interesses e as atividades do alvo para personalizar o ataque e torná-lo mais convincente e eficaz.

4 No passo quatro, é realizada a **identificação de pontos fracos**, na qual os atacantes procuram identificar vulnerabilidades na organização ou nos indivíduos visados, como funcionários com acesso a informações confidenciais ou falhas em sistemas de segurança.

5 Para o passo cinco, tem-se **engenharia de confiança**, segundo a qual os atacantes tentam estabelecer uma relação de confiança com a vítima, seja por meio de interações amigáveis ou fornecendo informações aparentemente úteis e

relevantes.

6 No passo seis, é proposta a **utilização de pretextos**, ou seja, os atacantes criam subterfúgios convincentes para obter informações ou acesso. Isso pode incluir fingir ser um colega de trabalho que precisa de ajuda ou um técnico de suporte que requer credenciais para resolver um problema.

7 No penúltimo passo, **exploração de autoridade**, os atacantes se passam por figuras de autoridade, como gerentes, para coagir funcionários a fornecerem informações confidenciais.

8 No último passo, tem-se **uso de manipulação emocional**, na qual os atacantes podem aproveitar emoções como medo, urgência ou curiosidade para induzir as vítimas a tomar ações precipitadas.

b) **Infiltração:** A infiltração representa uma etapa avançada de um ataque de engenharia social, no qual o agressor procura penetrar fisicamente em ambientes restritos, como edifícios ou áreas protegidas, com a finalidade de obter informações confidenciais ou conduzir ações maliciosas. Esse tipo de ataque pode ser especialmente preocupante, pois o atacante entra diretamente no espaço alvo, podendo evitar algumas das medidas de segurança digital. Este ato se divide em seis passos:

1 **Disfarces:** O atacante pode se disfarçar como funcionário, entregador, técnico de suporte ou qualquer outra pessoa que tenha permissão de acesso ao local. Um uniforme falso, distintivo ou adesivo com o logotipo de uma empresa real podem ser usados para parecer mais autêntico.

2 **Falsificação de identidade:** O atacante pode utilizar documentos falsos, cartões de acesso ou até mesmo crachás roubados para se passar por um funcionário legítimo.

3 **Engenharia social presencial:** O atacante pode interagir pessoalmente com funcionários ou outros ocupantes do espaço alvo, usando técnicas de manipulação psicológica para convencê-los a fornecer acesso ou informações sensíveis.

4 **Aproveitamento de eventos ou distrações:** O atacante pode se aproveitar de eventos especiais, reuniões, festas ou situações de distração, nas quais os protocolos de segurança podem ser mais flexíveis.

5 **Acesso físico não autorizado:** O atacante pode usar técnicas de arrombamento, invasão ou uso de dispositivos eletrônicos para burlar sistemas de controle de acesso, como fechaduras eletrônicas ou alarmes.

6 **Cumplicidade interna:** Em alguns casos, o atacante pode ter a ajuda de alguém interno, seja por meio de suborno, chantagem ou coerção.

c) **Ataque**: O ataque de engenharia social explora a manipulação psicológica das pessoas para obter informações confidenciais, acesso a sistemas protegidos ou induzi-las a tomar ações indesejadas. Em geral, o funcionamento do ataque de engenharia social segue estes seis passos, unidos aos passos anteriores:

1 **Coleta de informações:** O atacante pesquisa e coleta informações sobre a vítima ou organização-alvo. Isso pode incluir detalhes pessoais, atividades online, afiliações profissionais, entre outros.

2 **Criação de pretextos:** Com base nas informações coletadas, o atacante cria um pretexto convincente para estabelecer contato com a vítima, como se passar por um colega de trabalho, representante de suporte técnico ou amigo.

3 **Estabelecimento de confiança:** O atacante tenta estabelecer uma relação de confiança com a vítima ao longo do tempo. Isso é feito através de conversas amigáveis, fornecimento de informações úteis ou até mesmo elogios.

4 **Exploração emocional:** Os atacantes podem explorar emoções como medo, urgência, compaixão ou curiosidade para manipular a vítima a agir impulsivamente, como fornecer informações confidenciais ou clicar em links maliciosos.

5 **Solicitação de informações sensíveis:** Uma vez que a confiança foi estabelecida, o atacante pode começar a solicitar informações confidenciais, como senhas, dados de acesso ou informações pessoais.

6 **Execução do ataque:** Com as informações obtidas, o atacante pode utilizar as credenciais para acessar sistemas ou realizar atividades maliciosas, como roubo de identidade, acesso a contas bancárias, divulgação de informações confidenciais, entre outros.

d) **Evasão:** Após ter realizado um ataque de engenharia social e logrado êxito, a evasão é a etapa em que o atacante busca sair do cenário do crime ou disfarçar suas atividades para evitar a detecção e evitar ser identificado. A evasão é uma parte crucial do processo para que o atacante não seja rastreado e possa continuar a explorar as informações obtidas ou planejar novos ataques. A forma como a evasão é realizada pode variar, dependendo da natureza do ataque e dos objetivos do atacante, sendo típicas as formas descritas a seguir:

1 **Encobrir rastros:** O atacante pode tentar eliminar ou mascarar quaisquer evidências de sua presença ou atividades, como logs de acesso, histórico de chamadas ou registros de transações.

2 **Uso de proxy e VPNs:** O atacante pode redirecionar o tráfego da Internet por meio de servidores proxy ou redes virtuais privadas (VPNs) para ocultar sua localização real e dificultar o rastreamento.

3 **Utilização de identidades falsas:** Se o atacante usou identidades falsas durante o ataque, ele pode abandonar essas personas para evitar ser associado

a qualquer atividade suspeita.

4 **Utilização de técnicas de ofuscação:** Técnicas de ofuscação podem ser empregadas para tornar os rastros digitais menos identificáveis, como uso de ferramentas de criptografia, esteganografia ou fragmentação de dados.

5 **Uso de redes anônimas:** O atacante pode utilizar redes anônimas, como a dark web, para esconder suas atividades e comunicações.

6 **Saída do local físico:** Se a engenharia social envolveu infiltração física em instalações restritas, o atacante pode simplesmente sair do local sem levantar suspeitas.

2.1.2 Framework da Engenharia Social

Nesta subseção, tem-se o framework da engenharia social proposto na literatura por Wang, Zhu e Sun (2021), já é um framework consolidado e referênciado há 4 anos, o trabalho disponibiliza junto ao estado da arte em engenharia social um framework abordando a relação entre os efeito externo (Mecanismo de Efeito), efeito interno (Vulnerabilidade Humana) e técnicas de ataques cibernéticos (Método de Ataque).

O artigo o dos pesquisadores Wang, Zhu e Sun (2021), propõe um modelo conceitual que fornece uma perspectiva integrativa e estrutural para descrever o funcionamento dos ataques de engenharia social. O trabalho norteador desta dissertação, classifica o funcionamento da engenharia social em três eixos principais (mecanismo de efeito, vulnerabilidade humana e método de ataque), são identificados para ajudar a compreender como os ataques de engenharia social ocorrem e seus efeitos.

Na Figura 1, apresentamos de forma adaptada as perspectivas de ambos os lados, atacante e vítima. Já na figura 2, trazemos a este trabalho todos os pontos relatados pelos pesquisadores Wang, Zhu e Sun (2021), na construção de sua tese.

A Figura 2, apresenta de forma detalhada as várias vulnerabilidades humanas em diversas situações, as quais são combinadas, segundo Wang, Zhu e Sun (2021), com os 'mecanismos de efeito', representando efeitos externos e alheios à vontade da vítima. Além de explorar os efeitos desses mecanismos e das vulnerabilidades humanas destacadas, o autor aprofunda a análise ao abordar os métodos de ataques, os quais combinam as vulnerabilidades humanas identificadas com os mecanismos de efeitos externos destacados.

Na Figura 1, o funcionamento deste framework é visualmente demonstrado. A fim de ilustrar de maneira vívida, são delineados, em lados opostos, os papéis do atacante e da vítima, revelando suas perspectivas, ou seja, as percepções individuais durante um ataque de engenharia social. Na ótica do atacante, o fluxo segue a seguinte sequência: primeiramente, o atacante concebe o método de ataque com base em seu objetivo e, esta etapa pode ser fundida a uma técnica cibernetica, em seguida, explora as vulnerabilidades humanas da vítima alvo. Por outro lado, na perspectiva da vítima, esta possui vulnerabilidades humanas que desencadeiam o ataque; este ponto de vista surge quando o atacante aproveita oportunamente as vulnerabilidades humanas identificadas.

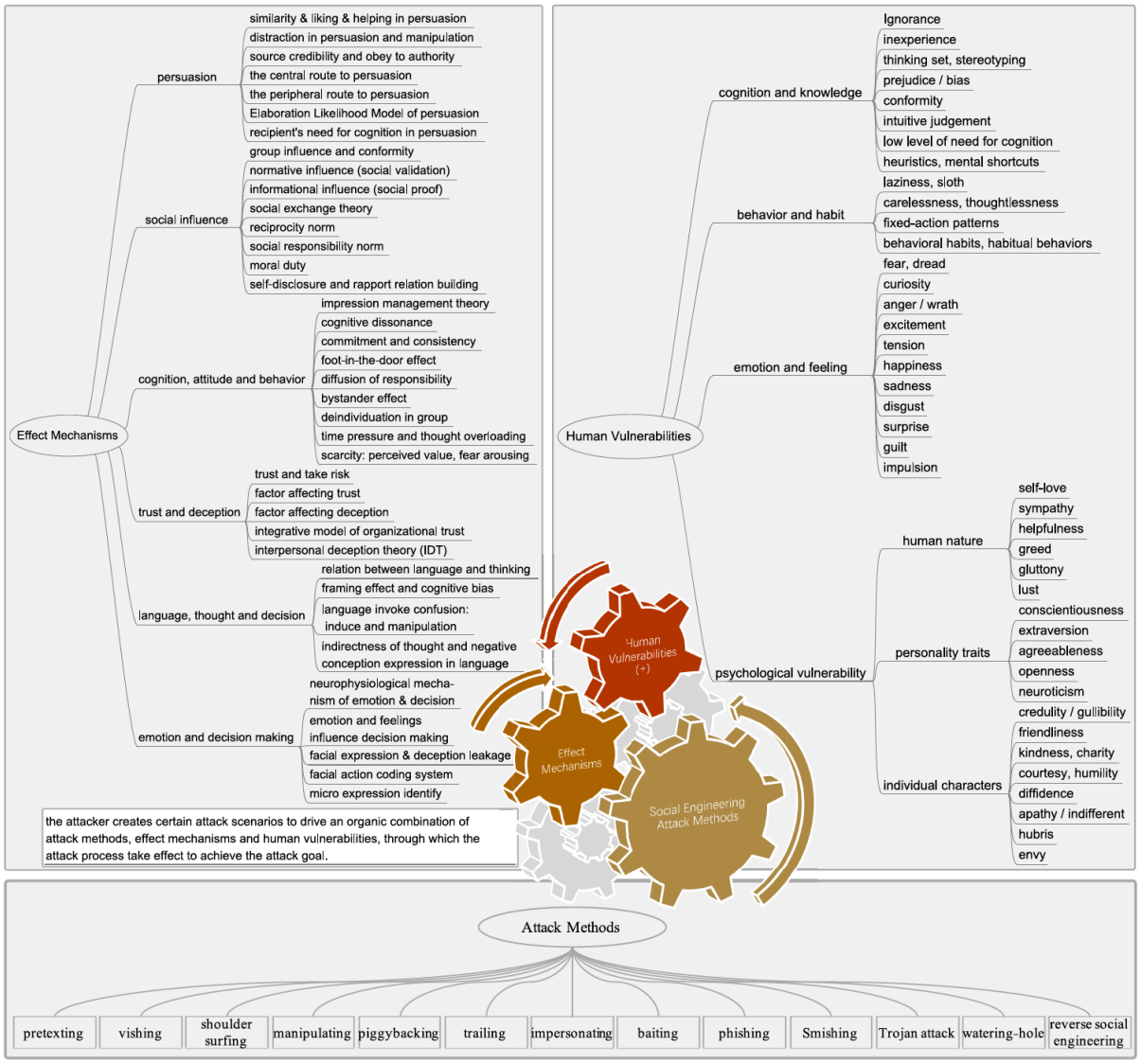

Figura 2 – Framework de Engenharia Social.(WANG; ZHU; SUN, 2021)

2.1.3 Tipos de Ataques de Engenharia Social

Até agora, comentou-se sobre o que são ataques de engenharia social. Mas, apartir deste ponto, serão apresentados os principais tipos de ataques de engenharia social, aqueles e considerados por Zambrano *et al.* (2019), como de maior incidência.

1) Ataques de *phishing*: O trabalho Khonji, Iraqi e Jones (2013), os define como tentativas fraudulentas de obter informações confidenciais, como senhas e detalhes bancários, por meio de mensagens ou sites falsos que se passam por entidades legítimas.

2) *Spam phishing*: Para Awad *et al.* (2022), esta técnica é definida como um ataque que dispara e-mails não solicitados e enganosos, para obter informações pessoais, como senhas e dados financeiros, através da falsa representação de entidades confiáveis.

3) *Spear phishing*: Segundo Qin *et al.* (2017), é um tipo de ataque de *phishing* que visa uma pessoa específica, seja um indivíduo ou uma organização. Para Zieni, Massari e Calzarossa (2023), essas pessoas podem ser um CEO de uma empresa, etc. Destaca-se que ambos os autores apontam que a ideia é alcançar as pessoas que têm acesso a muitos sistemas, como sistemas de informações de funcionários, sistemas de gerenciamento de redes, por exemplo. Esse tipo de *phishing* é perigoso porque os invasores podem obter acesso à maioria das informações de uma empresa apenas obtendo acesso a computadores e informações de funcionários de nível superior.

4) *phishing* em mecanismos de pesquisa: Segundo Abri *et al.* (2022), é realizado adicionando ou colocando sites falsos no topo dos resultados da pesquisa. Os autores afirmam ainda que os invasores usam algumas técnicas para colocar seu falso site malicioso no topo dos resultados de pesquisa para fazer com que seu site pareça seguro.

5) Ataques de isca: É apontado por Nicholls, Kuppa e Le-Khac (2021) como aquele que tira aproveito dos pontos fracos das vítimas para comprometer seus dados. Colocam ainda que unidades USB deixadas em anexos públicos ou de e-mail, incluindo detalhes sobre ofertas gratuitas ou software gratuito por tempo limitado para *download*, são tipos

de ataques de isca. Em outras palavras a maioria das pessoas pode ser atraída facilmente quando vê ofertas em *flash* ou palavras-chave gratuitas.

6) Ataques de Violação Física: São pouco evitados e envolve o atacante aparecendo pessoalmente durante o ataque. Para Tromblay (2023), os ataques de engenharia social de forma presencial visam violar a integridade física de um ambiente. Em virtude dos sentimentos humanos, apontados também por (WANG; ZHU; SUN, 2021), torna-se um ataque com uma chance alta de sucesso. Para Alturki, Alshwihi e Algarni (2020), os atacantes geralmente se apresentam como representantes de uma empresa respeitável e este tipo de hacker é formado principalmente por ex-trabalhadores que conhecem o sistema atual, as políticas e a conexão de rede da empresa. A recompensa do resultado é alta se o ataque for bem-sucedido, mas também tem riscos porque os atacantes devem comparecer pessoalmente.

7) Quid Attacks Pro Attacks: Esta nomenclatura definida por Wang, Sun e Zhu (2020) significa "um favor por um favor", em outras palavras, algum tipo de benefício mútuo entre os dois lados. Quid Attacks Pro Attacks oferece ofertas especiais ou brindes gratuitamente em troca de obter informações de uma vítima especifica, ou vitimas aleatórias. Sharmeen *et al.* (2020) colocam que é uma técnica de engenharia social comum e de fácil execução em virtude de não exigir do praticante conhecimentos técnicas avançados.

8) Falsificação de DNS: Se uma vítima estiver infectada com falsificação de DNS, sempre que inserir um URL legítimo, ela será redirecionada para um site malicioso que se assemelha ao site do URL legítimo. A vítima poderá ter uma certa dificuldade para diferenciar o site malicioso do legítimo porque são muito semelhantes. Uma vez ocorrido o ataque, a única maneira de se livrar da falsificação de DNS é limpar o roteamento de dados do sistema conforme apontam de forma convergente os trabalhos (BHATTACHARYA *et al.*, 2023; MAMBINA; NDIBWILE; MICHAEL, 2022) e (BHATTACHARYA *et al.*, 2023).

9) Ataques de Scareware: Visam assustar a vítima para que tome uma ação rápida, aponta Mambina, Ndibwile e Michael (2022). Por exemplo, um e-mail informando que uma nova tentativa de login suspeita foi detectada, redefina sua senha caso contrário, você perderá sua conta etc. Esse tipo de mensagem envolve ameaçar usuários e forçá-los a

realizar as tarefas e ações desejadas em um curto tempo.

10) Distribuição de malware por e-mail: Trata-se de e-mails disparados em massa com um arquivo duplamente nomeados em suas extensões finais. Por exemplo, "foto.jpeg.exe", "foto.png.bat". O estudo de Bhattacharya *et al.* (2023), coloca que essa dupla extensão é um estratégia muito eficaz. Este tipo de ataque tem o intuito de infectar diversas máquinas e abrir um canal entre o invasor e as vítimas para os mais diversos objetivos, desde BotNet's até roteamento durante o cometimento de um crime.

2.1.4 Interdisciplinariedade em Engenharia Social

A técnica de engenharia social é equivalente a uma cebola, para cada camada, se faz necessário uma habilidade especifica para que o atacante tenha sucesso. É preciso conhecimentos diversos e em diversas áreas para que se considere um engenheiro social eficaz (SINKó; BESENYő, 2023).

Os estudiosos Long e Mitnick (2011b) afirmam que a engenharia social é um campo interdisciplinar que envolve várias áreas de estudo, como psicologia, sociologia, antropologia, ciência política, ciência da computação e outras. Como resultado desta afirmação, há uma variedade de pesquisas científicas em engenharia social que abordam diferentes aspectos do tema e aqui vamos colocar alguns experimentos sociais que investigaram formas de manipulação.

Trazemos como referencial teórico alguns experimentos, dentre eles o estudo influente realizado por Asch (1940), conhecido como "experimentos de conformidade". Esse tipo de experimento é projetado para testar a disposição das pessoas em conformar-se com a opinião da maioria, mesmo que essa opinião seja claramente errada. De igual importância, o Psicólogo Festinger (1989) postula uma nova tese dentro da "teoria da dissonância cognitiva", tornando-se uma referência considerável quando se trata de manipulação da mente humana. Essa teoria propõe que, quando as pessoas enfrentam uma discrepância entre suas crenças ou valores e seus comportamentos, elas experimentam um estado de tensão psicológica conhecido como dissonância cognitiva. Por fim, porém

não menos importante, colocamos aqui como material, um dos maiores estudos sociais de manipulação humana, o estudo de Milgram (1963), denominado de "Teoria da autoridade". Essa teoria examina como as pessoas respondem à autoridade e às figuras de autoridade. O psicólogo social Stanley Milgram conduziu uma série de experimentos notórios no ano de 1960, conhecidos também como "Experimentos de Milgram", para testar a disposição das pessoas em obedecer a uma figura de autoridade, mesmo que isso significasse infligir dor em outra pessoa.

Para Almousa e Anwar (2023), origem da engenharia social remonta a tempos antigos, quando líderes militares e políticos usavam táticas de persuasão para obter vantagem em batalhas e negociações. Zheng *et al.* (2019b) exemplificam que na Grécia antiga os filósofos ensinavam retórica como uma habilidade essencial para a persuasão, enquanto Tzu e Pin (2015) afirmam em seu livro "A Arte da Guerra", sobre a importância de conhecer as emoções e motivações dos inimigos para vencê-los.

Com a evolução da sociedade, a engenharia social passou a ser aplicada em diversas áreas, como marketing, vendas, publicidade, política e, mais recentemente, em cibersegurança. Segundo Asiri *et al.* (2023), que discorreu sobre a compreensão das necessidades, desejos e comportamentos das pessoas, os profissionais destas áreas podem criar campanhas publicitárias, políticas e outras iniciativas que influenciem positivamente o comportamento do público.

No entanto, o estudo de Marchand-Nino e Fonseca (2019) aponta que a engenharia social também é frequentemente usada para fins maliciosos, como a manipulação de pessoas para obter informações confidenciais, roubar identidades ou cometer fraudes financeiras. No seu trabalho, Rueda (1999) afirma que os criminosos utilizam técnicas de engenharia social para se passar por pessoas confiáveis ou instituições legítimas, de forma a obter a confiança de suas vítimas e levá-las a realizar ações prejudiciais a si mesmas.

Com o avanço da tecnologia, a engenharia social também se expandiu para o mundo digital, criminosos cibernéticos utilizam táticas cada vez mais sofisticadas para enganar suas vítimas (HANCOCK, 1999). Isso inclui a criação de falsos sites e e-mails de *phishing*, nos quais usuários são induzidos a fornecer informações confidenciais, além do uso de

engenharia social em redes sociais e aplicativos de mensagens para se passar por amigos e familiares e obter acesso a informações pessoais.

No trabalho Wang, Zhu e Sun (2021), os pesquisadores apontam que é nítida a evolução dos sistemas de informação e embora a engenharia social tenha evoluído ao longo do tempo, seu objetivo principal continua sendo o mesmo: manipular as emoções e o comportamento humano para atingir seus próprios objetivos, sejam eles benignos ou malignos. E Hsieh, Leu e Takada (2022) colocam, que é importante estar atento a essas táticas e estar ciente de que qualquer pessoa pode ser uma vítima em potencial da engenharia social.

2.1.5 Interconexões em Engenharia Social

Assim como a engenharia social é interdisciplinar, ela também possui a peculiaridade de contar com interconexões entre os meios fisico e digitais. Por exemplo para Orbach (2023), um bom engenheiro social é aquele que consegue unir todas as ferramentas que estão ao seu alcance para lograr êxito em seus ataques. Para o autor, emprega-se na engenharia social, meios físicos e meios digitais e até mesmo por via interposta, agindo em um terceiro para atacar um quarto, com o objetivo de conseguir informações do primeiro e segundo, por exemplo.

Engenharia social em cibersegurança, segundo (LONG; MITNICK, 2011a), estuda como os criminosos usam técnicas de engenharia social para se infiltrar em sistemas de computador e obter informações confidenciais. Os pesquisadores (MIFTARI; LUMA-OSMANI; IDRIZI, 2022) têm investigado maneiras de identificar e mitigar essas ameaças, incluindo a análise de padrões de comportamento do usuário e a educação dos usuários sobre práticas de segurança cibernética, conforme destaca (WANG; ZHU; SUN, 2021).

Os ataques de engenharia social foram responsáveis por algumas das maiores e mais prejudiciais violações de segurança da história recente, trazidos a sociedade através do jornal The Guardian (THEGUARDIAN, 2013a), (THEGUARDIAN, 2016), (THEGUARDIAN, 2017) e (THEGUARDIAN, 2013b):

- A violação da Target: em 2013, a Target, uma das maiores varejistas dos Estados Unidos, sofreu uma grande violação de dados que afetou mais de 110 milhões de clientes. Os invasores usaram um e-mail de *phishing* para roubar credenciais de um fornecedor terceirizado, que usaram para obter acesso aos sistemas da Target.(THEGUARDIAN, 2013a)

- As violações de dados do Yahoo: O Yahoo sofreu uma série de violações de dados entre 2013 e 2014 que afetaram todos os três bilhões de contas de usuários. Os invasores usaram e-mails de *spear phishing* para induzir os funcionários do Yahoo a revelar suas credenciais, que eles usaram para acessar os sistemas da empresa. (THEGUARDIAN, 2016)

- A violação da Equifax: em 2017, a Equifax, uma das maiores agências de relatórios de crédito do mundo, sofreu uma violação maciça de dados que afetou mais de 143 milhões de clientes. Os invasores usaram uma vulnerabilidade no aplicativo da Web da Equifax para obter acesso a dados confidenciais do cliente.(THEGUARDIAN, 2017)

- O Twitter Bitcoin Scam: Em julho de 2020, os hackers usaram táticas de engenharia social para obter acesso às contas do Twitter de indivíduos proeminentes, incluindo Barack Obama, Elon Musk e Bill Gates. Os invasores usaram essas contas para promover um golpe de Bitcoin, que rendeu mais de US 100.000 em questão de horas.(THEGUARDIAN, 2013b)

2.2 Contrainteligência

Para Falkov (2023), Shpiro (2023) e Awad *et al.* (2022), a contrainteligência é uma atividade que visa identificar, prevenir e neutralizar as ações de serviços de inteligência adversário, organizações criminosas ou outros atores hostis que possam representar uma ameaça à segurança de um determinado ente, seja pais, sistema computacional, organizações ou até mesmo um indivíduo específico.

A Agência Brasileira de Inteligência (ABIN) e do Sistema Brasileiro de Inteligência (SISBIN) de acordo com a fonte oficial do governo federal em ABIN (2020), atuam no Brasil com foco em promover a defesa contra ameaças como a espionagem, a sabotagem, o vazamento de informações e o terrorismo, os quais podem ser patrocinadas por instituições, grupos ou governos estrangeiros.

Em outros termos, a contrainteligência está relacionada ao campo da inteligência, que envolve a coleta de informações para fins de segurança nacional, defesa ou proteção de interesses estratégicos. No entanto, Huang H. Tan J. (2009), explicam que enquanto a inteligência se concentra na obtenção de informações, a contrainteligência tem como objetivo proteger essas informações e os recursos vitais contra atividades de espionagem, sabotagem ou subversão. Com o foco na guerra fria, Murphy (2023) coloca que as atividades de contrainteligência podem incluir a identificação e monitoramento de agentes estrangeiros ou infiltrados, a análise de ameaças de segurança, a proteção de informações sensíveis, a implementação de medidas de segurança, a condução de investigações internas para identificar vazamentos de informações, entre outras tarefas. Para Shpiro (2023), essas atividades de contrainteligência são realizadas por agências de inteligência, forças de segurança ou departamentos especializados dentro de uma organização ou governo.

Segundo Paicu (2023) e Fischer (2023), a contrainteligência é fundamental para garantir a integridade e a segurança das informações e recursos essenciais de um país ou organização, bem como para prevenir possíveis danos causados por atividades hostis a exemplo da prática de engenharia social.

Na doutrina tradicional de contrainteligência atualizada por Plekhanov (2023), os atos de traição e deslealdade são motivados por dinheiro, ideologia, coerção ou compromisso, ego e ressentimento. Tendo ainda sido acrescentada pelo autor, a ganância, vindo assim ser denominado em sua sigla em inglês (MICE+G), o qual faz referência aos termos: *money, ideology, coercion or compromise, ego or excitement, ganance*. Mais recentemente, a estrutura de reciprocidade, autoridade, escassez, consistência, gosto e provas sociais, e em inglês *reciprocation, authority, scarcity, commitment and consistency, liking, social proof*, vindo a compor a sigla em (RASCLS), foi usada para identificar potenciais inimigos, traidores e criminosos cibernéticos, tais argumentos são encontrados também na literatura oportunizada por Burkett (2013). O trabalho de Burkett (2013), argumenta que as estruturas MICE+G e RASCLS podem ajudar a educar e treinar membros dos setores público e privado para detectar, defender e derrotar ataques cibernéticos.

Os mesmos métodos psicológicos que os oficiais de inteligência usam para recrutar espiões se aplicam à engenharia social no domínio cibernético (HUGHES-WILSON, 2016) e (HUANG H. TAN J., 2009). Os autores relacionados anteriormente, relatam o uso da manipulação psicológica em processos seletivos para a ocupação de agente de uma das mais conceituadas instituições de investigação, espionageme inteligência do mundo. Como já conceituado em seções anteriores, a engenharia social emprega o engano para manipular os indivíduos a fornecerem informações confidenciais ou realizarem outros atos contra seus próprios interesses ou os interesses de sua organização ou nação. Hughes-Wilson (2016) e Burkett (2013) apontam como é possível utilizar o treinamento de contrainteligência baseado nas estruturas MICE+G e RASCLS para combater ataques cibernéticos.

Para Tuinier, Zaalberg e Rietjens (2023), o conceito de contrainteligência mais fundamental para capacitar as pessoas contra a engenharia social e ataques cibernéticos relacionados é “todo mundo é um alvo”, todos os usuários de computador e Internet devem estar conscientes da insegurança em ambientes diversos. O trabalho do pesquisador Plekhanov (2023), coloca que os agentes militares e governamentais são treinados em técnicas de contrainteligência antes de viajarem para o exterior para alertá-los sobre os perigos de serem manipulados por adversários estrangeiros. Para Wang, Sun e Zhu (2020) um dos primeiros passos para esse treinamento de contrainteligência é conscientizar o

sujeito de que ele é um alvo para agentes de inteligência estrangeiros.

Criminosos cibernéticos, organizações terroristas e agentes de estado-nação adversários estão constantemente procurando por indivíduos vulneráveis que podem ser enganados e entregar suas informações de identificação pessoal e informações confidenciais (MURPHY, 2023). Segundo Gentry (2023), uma abordagem de contrainteligência para segurança cibernética começa com uma maior conscientização da presença de agentes mal-intencionados.

Por fim, a pesquisas de Cleave (2013), coloca a necessidade de instigar as pesquisas no campo de contrainteligência, apontando que são escassas no campo de contrainteligência.

2.3 Considerações Finais

Após expor a gênese da Engenharia Social e da Contrainteligência, torna-se evidente a sinergia existente entre esses dois campos. Podemos traçar uma analogia com a sequência de Fibonacci, conforme discutido por Horadam (1961) e Sinha (2017), e tentar compor um prisma em que o crescimento da aplicabilidade das técnicas de engenharia social exija, de igual modo, um desenvolvimento correspondente em contrainteligência.

3 Framework de Contrainteligência em Engenharia Social

Este capítulo apresenta uma proposta incipiente de um framework de contrainteligencia a ser integrado de modo complementar ao framework consolidado da literatura, incorporando a contribuição da contrainteligência como uma estratégia essencial de mitigação de riscos. O objetivo deste aprimoramento é suprir uma lacuna relevante no conhecimento sobre as práticas de defesa contra ataques de engenharia social, uma vez que o framework tradicionalmente abordado na literatura se limita a descrever o funcionamento e as técnicas empregadas por atacantes, sem considerar de forma adequada as medidas de defesa. Tal abordagem deixa de lado uma análise crítica e prática sobre como se proteger de tais ameaças, restringindo-se a um enfoque passivo. Ao integrar o conceito de contrainteligência, este capítulo propõe um novo olhar sobre a questão, não apenas descrevendo o fenômeno, mas também fornecendo direções claras e robustas para a construção de defesas contra ataques de engenharia social.

Entende-se por contrainteligência a atividade de identificar, prevenir e neutralizar as ações de serviços de inteligência adversários (SHPIRO, 2023). Com base nesse conceito, o framework aqui proposto estende o framework ilustrado na Figura 1 a partir da premissa de que o conhecimento de contrainteligência de ataques de engenharia social permitirá às vítimas reduzir danos por meio de atitudes comportamentais de natureza proativa e reativa. Ou seja, o conhecimento por parte da vítima sobre os mecanismos de ação e das suas próprias vulnerabilidades em um ataque de engenharia social possui o efeito de neutralizar o ataque ou mitigar os eventuais danos pretendidos pelo atacante (adversário).

Este capítulo está organizado de forma a apresentar, de maneira clara e progressiva, os principais elementos que compõem a proposta de framework de contrainteligência.

Na **Seção 3.1**, o foco recai sobre o processo de *Construção de Inteligência*, considerado um dos pilares centrais da contrainteligência. Essa seção examina, de forma aprofundada, como o conhecimento é obtido, analisado e sistematizado com o objetivo de antecipar e neutralizar ameaças potenciais. Destaca-se aqui a importância desse processo para o fortalecimento das defesas organizacionais diante de ataques baseados em engenharia

social.

A **Seção 3.2** é dedicada à primeira grande estratégia apresentada: a *defesa proativa*. Nessa etapa, são discutidos os fundamentos dessa abordagem, bem como os mecanismos e práticas recomendadas para sua implementação. O foco recai sobre ações preventivas e antecipatórias, capazes de inibir a ocorrência de ataques antes que eles se concretizem.

Já na **Seção 3.3**, o texto se volta à *defesa reativa*, cujo propósito é lidar com incidentes em andamento ou já consumados. São abordadas as metodologias e técnicas voltadas à contenção de danos, destacando-se a importância de respostas rápidas e eficientes para reduzir os impactos negativos sobre a organização.

O capítulo se encerra com as **considerações finais**, nas quais são retomados os principais pontos discutidos, promovendo uma reflexão crítica e integradora. Essa última seção também aponta caminhos para investigações futuras e aplicações práticas, contribuindo para o avanço das estratégias de contrainteligência frente às ameaças oriundas da engenharia social.

3.1 Construção de Inteligência

A compreensão e a resposta eficaz aos ataques de engenharia social emergem como aspectos fundamentais no domínio da segurança da informação. Nesse cenário, a aquisição de conhecimentos especializados em inteligência revela-se imprescindível para a construção de defesas robustas e eficazes. Conforme argumentam (SHPIRO, 2023; TUINIER; ZAALBERG; RIETJENS, 2023), esse processo de capacitação não é trivial, implicando o desenvolvimento de habilidades estruturadas em etapas bem definidas. A seguir, serão delineadas essas etapas essenciais para o fortalecimento das capacidades de defesa, com o intuito de proporcionar uma abordagem sistemática e fundamentada para o enfrentamento das ameaças decorrentes da engenharia social.

1. **Coleta de informações**: Primordial para aquisição de conhecimento em contrainteligência, consiste em manter uma atitude permanente de busca por informações sobre os mecanismos de ação dos ataques de engenharia social, que podem ser obtidas em diversas fontes, como consultas a sites especializados, notícias na mídia, relatos de pessoas conhecidas, cursos de capacitação no contexto organizacional, etc.

2. **Análise de informações**: Compreende analisar as informações coletadas para identificar padrões, tendências e ameaças (potenciais e recorrentes) dos mecanismos de ação.

3. **Produção de resistência e inteligência**: Com base na análise de informações, constitui-se em promover o desenvolvimento de uma resistência em face do conhecimento do mecanismo de ação. A precisão e a relevância desse conhecimento é fundamental para uma tomada de decisão efetiva em um ataque de engenharia social.

4. **Proteção de fontes e métodos**: Consiste em assegurar que os dados coletados no passo inicial foram corretamente compreendidos de modo a produzir resistência que promova uma estrutura de defesa efetiva. Isso porque uma compreensão incorreta poderá gerar a falsa percepção de se estar preparado para se antepor a um ataque, podendo um indivíduo, em virtude disso, colocar-se em situação de maior risco.

5. **Cooperação Social**: Compreende compartilhar (e.g., com as autoridades, instâncias superiores, membros do círculo social mais próximo) experiências vivenciadas de ataques de engenharia social envolvendo mecanismos de ação diversos, para retroalimentar e enriquecer o processo de aquisição de conhecimento.

De acordo com a literatura especializada na produção de conhecimento nesta área, o aprimoramento da defesa, aliado à construção de uma base sólida de inteligência, constitui, para (SHPIRO, 2023), um avanço substancial na consolidação de uma defesa integrada contra ameaças, conhecimento que se emprega nesta investigação para o enfrentamento das técnicas de engenharia social apresentadas por (WANG; ZHU; SUN, 2021). A estruturação desses pilares de inteligência possibilita uma abordagem abrangente e multifacetada para enfrentar os desafios decorrentes da exploração do fator humano, na medida em que cada

ponto-chave complementa e fortalece as capacidades dos demais.

A integração do conhecimento de contrainteligência, conforme ilustrado na Figura 3, revela-se um fator determinante para que uma vítima de ataque de engenharia social adote medidas de defesa eficazes, tanto proativas quanto reativas, com o objetivo de neutralizar o ataque ou mitigar os danos subsequentes. Os conceitos de defesa proativa e reativa são amplamente discutidos na literatura, especialmente no contexto da segurança cibernética, e são frequentemente relacionados às estratégias de proteção de sistemas e informações contra ameaças externas e internas (HUGHES-WILSON, 2016). A aplicação desses conceitos no campo da engenharia social amplia a compreensão sobre as diferentes formas de abordagem defensiva, destacando sua relevância para a proteção dos indivíduos e organizações diante de ameaças cada vez mais sofisticadas e dinâmicas.

Figura 3 – Framework estendido com a contrainteligência. Fonte: elaborado pelo autor e adaptado de (WANG; ZHU; SUN, 2021)

3.2 Defesa Proativa

A defesa proativa em segurança configura-se como uma abordagem estratégica e preventiva, na qual indivíduos e organizações se capacitam, por meio de conhecimento especializado sobre potenciais ameaças, a desenvolver respostas antecipadas com vistas

Figura 4 – Processo de aquisição de conhecimento de contrainteligência. Fonte: elaborado pelo autor e adaptado de (WANG; ZHU; SUN, 2021)

à neutralização de ataques antes da consolidação de seus efeitos. Essa metodologia favorece uma detecção célere de tentativas de violação, fundamentada em um entendimento aprofundado das táticas comumente empregadas por agentes maliciosos. Através da antecipação das manobras adversas, o defensor reduz de forma substancial as vulnerabilidades inerentes, convertendo o domínio prévio dos mecanismos de ataque em um instrumento eficaz para a mitigação de riscos e para o desmantelamento de ações hostis em estágio inicial.

A defesa proativa refere-se ainda, sobre tomar medidas preventivas de modo a identificar e responder a ameaças na iminência de sua ocorrência, a fim de neutralizar o ataque. Ou seja, trata-se de uma resposta rápida de uma vítima contra tentativas de ataques a ela direcionados. Por exemplo, um indivíduo recebe uma ligação de um operadora de cartão de crédito informando que sua compra foi autorizada e que, caso a desconheça, entre em contato com um número telefônico citado. Sabendo previamente sobre este tipo de ataque, percebe que é uma manobra maliciosa de *phishing* e encerra imediatamente a comunicação com o atacante. A ideia, portanto, é que o conhecimento do mecanismo de ação por parte da vítima reduza suas vulnerabilidades, possibilitando-a se antecipar ao comportamento do atacante de forma a frustrar o ataque.

3.3 Defesa Reativa

A defesa reativa em segurança constitui-se como uma abordagem de emergência, pautada na adoção de contramedidas que visam à contenção de um ataque já em progresso e à mitigação de danos em estágio avançado de concretização, situação na qual a vítima apenas identifica a ameaça após ter sido parcialmente ludibriada pelo agente adversário. Em contraposição à defesa proativa, que antecipa e neutraliza investidas antes de sua materialização, a defesa reativa se impõe como um mecanismo de resposta imediata, buscando estancar os impactos de uma intrusão em curso. Nesse cenário, a capacidade da vítima de reconhecer o modus operandi do atacante torna-se essencial, permitindo-lhe interromper o ataque, implementar ações corretivas urgentes e notificar as instâncias competentes, com o intuito de minimizar os prejuízos e resguardar a integridade de suas informações.

A defesa reativa refere-se a tomada de medidas de sustação de um ataque em andamento e de redução de danos, ataque este que a vítima só consegue identificar quando já está ludibriada pelo mecanismo de ação. Ou seja, trata-se de uma reação para mitigar danos e cessar um ataque parcialmente bem sucedido. Por exemplo, no mesmo contexto da situação anterior ilustrada, o indivíduo entra em contato com o número fornecido pelo atacante e começa a ceder suas informações pessoais e, em determinado momento, percebe que está sob ataque de engenharia social. Nessa situação, com as informações já fornecidas, o indivíduo reage cessando imediatamente a comunicação com o atacante para, em seguida, trocar suas senhas, acionar o serviço de atendimento ao consumidor do cartão e informar as autoridades. A expectativa, portanto, é que a vítima, quando se percebe envolvida em um ataque, seja capaz reconhecer o mecanismo de ação de modo a reagir sustando o ataque e tomando medidas apropriadas para mitigar danos.

3.4 Considerações Finais

Ao se realizar uma análise comparativa entre as abordagens de defesa proativa e reativa, constata-se que a defesa proativa se destaca como a mais eficaz, uma vez que permite a neutralização de ataques antes que estes possam causar danos substanciais, devido ao seu caráter eminentemente preventivo. A adoção de uma postura proativa

possibilita a identificação precoce de ameaças, sua mitigação e, em muitos casos, a completa neutralização da ação do atacante, antes mesmo que o ataque se concretize e se materialize em danos organizacionais. Em contrapartida, a defesa reativa, embora de suma importância no contexto da segurança cibernética, apresenta uma eficácia consideravelmente reduzida, uma vez que é acionada apenas após a materialização do ataque, o que limita significativamente a capacidade de contenção e recuperação, além de exigir esforços consideráveis para a minimização dos danos.

Entretanto, é fundamental destacar que, independentemente da estratégia de defesa adotada, o conhecimento especializado em contrainteligência por parte da vítima emerge como um fator crucial para a efetividade de ambas as abordagens. A ausência desse conhecimento torna a vítima suscetível às táticas de manipulação dos atacantes, dificultando a identificação precoce dos sinais de alerta e o reconhecimento das técnicas empregadas. Portanto, a busca por uma educação permanente e contínua e a conscientização sobre práticas de contrainteligência são componentes essenciais para garantir que os indivíduos e organizações possam não apenas detectar e prevenir ataques, mas também responder de maneira ágil e eficaz diante de incidentes, seja em um contexto preventivo ou corretivo.

Dessa forma, a combinação sinérgica de defesas proativas e reativas, aliada a um robusto entendimento em contrainteligência, não apenas potencializa a capacidade de defesa, mas também promove o fortalecimento da resiliência organizacional. Essa abordagem integrada constitui um alicerce essencial para o enfrentamento das ameaças emergentes no campo da engenharia social, cujas técnicas são cada vez mais sofisticadas e dinâmicas, exigindo das organizações uma postura de segurança adaptativa, abrangente e em constante evolução para garantir a proteção eficaz de seus ativos e informações.

4 Metodologia

A metodologia descrita neste capítulo tem como objetivo avaliar a implementação do framework consolidado na literatura, incorporando a inovação proposta neste trabalho. Este capítulo detalha a abordagem metodológica adotada para a investigação, fundamentada nos objetivos estabelecidos no Capítulo 1. A escolha da metodologia é crucial para garantir a eficácia da pesquisa, proporcionando uma estrutura adequada para a análise dos dados e a formulação de conclusões. Ao alinhar os procedimentos metodológicos aos objetivos definidos, busca-se assegurar a consistência no desenvolvimento do estudo e a capacidade de responder às questões de pesquisa propostas. Assim, o capítulo oferece uma visão geral das estratégias, técnicas e instrumentos utilizados na coleta e análise dos dados, delineando o percurso metodológico adotado ao longo da investigação.

4.1 Referencial Teórico da Metodologia

A metodologia empregada nesta pesquisa é fundamentada em uma abordagem qualitativa exploratória, a qual se vale de entrevistas como principal ferramenta investigativa, seguindo os apontamentos das pesquisadoras Leitao e Prates (2017) e sua mais nova atualização Leitao (2021). Este método permite uma compreensão aprofundada dos fenômenos estudados, ao mesmo tempo em que oferece flexibilidade para explorar nuances e perspectivas diversas. As entrevistas são conduzidas com indivíduos selecionados, de acordo com critérios de inclusão previamente estabelecidos, visando garantir a relevância e representatividade dos participantes. Por outro lado, a base teórica desta investigação orienta que devem ser evitados os participantes que não atendem aos critérios de inclusão ou que atendam aos critérios de exclusão, a fim de manter a coerência e a precisão dos resultados. Essa abordagem metodológica proporciona uma análise detalhada e contextualizada dos temas investigados, permitindo a emergência de *insights* significativos e a construção de um conhecimento robusto sobre o objeto de estudo.

Os critérios trazidos na subseção 4.2 seguem orientações dos apontamentos e considerações apresentados nos trabalhos Leitao e Prates (2017), Leitao (2021) no que tange sua estrutura teórica.

4.1.1 Amostra de Pesquisa

Em pesquisa qualitativa, a técnica de composição amostra se afasta dos critérios de aleatoriedade e representatividade. Nesse tipo de pesquisa utiliza-se a técnica de seleção da amostra proposital, também chamada de amostra intencional ou por conveniência (SEIDMAN, 1998 apud LEITAO; PRATES, 2017).

Leitao e Prates (2017), destacam a importância do tamanho da amostra em estudos qualitativos, ressaltando que ele deve ser determinado pelo grau de saturação dos temas abordados. Segundo essas autoras, a saturação é alcançada quando as entrevistas não mais fornecem novas perspectivas ou temas relevantes relacionados ao objeto de estudo. Dessa forma, o trabalho declara que a definição do tamanho da amostra não é baseada em números arbitrários, mas sim na qualidade e na profundidade das informações coletadas em cada entrevista. As autoras afirmam que, uma vez que os dados obtidos se tornam repetitivos e não acrescentam mais *insights* significativos, pode-se considerar a amostra como suficiente para a compreensão abrangente dos temas em análise. As autoras Leitao e Prates (2017), Leitao (2021), afirmam ainda que essa abordagem flexível e orientada pela saturação permite uma pesquisa mais focada e enriquecedora, garantindo que os resultados reflitam a complexidade e a diversidade do fenômeno estudado.

4.1.2 Critérios

Na fase de seleção dos participantes para as entrevistas, são considerados critérios objetivos, dentre os quais se destaca a necessidade de que o entrevistado tenha previamente vivenciado uma experiência de uma ataque de engenharia social, bem ou mal sucedido. Essa exigência visa garantir que os participantes possuam *insights* e compreensões relevantes sobre o tema em análise, fornecendo informações substanciais e perspicazes durante

as entrevistas. A experiência prévia com engenharia social é crucial, pois permite aos entrevistados compartilhar suas percepções, desafios e estratégias adotadas diante dessa prática, enriquecendo assim a qualidade e a profundidade dos dados coletados.

Leitao e Prates (2017) e Leitao (2021), apontam de forma convergente que, ao estabelecer critérios claros e objetivos para a seleção dos entrevistados, busca-se assegurar a representatividade e a pertinência das informações obtidas, contribuindo para a robustez e a relevância da pesquisa como um todo.

4.1.3 Entrevistas

A literatura referência desta metodologia, Leitao e Prates (2017), Leitao (2021), explicam as principais estruturas e a execução do processo de entrevista. Para Leitao (2021), as entrevistas podem ser compreendidas em três dimensões: temporal, espacial e estrutural.

Dimensão Temporal

Específicamente para Leitao (2021) a dimensão temporal dá a entrevista sua definição mais geral e idiossincrática. A entrevista é uma comunicação direta entre pesquisador e participante, que se configura necessariamente como um contato síncrono. Para a pesquisadora, trata-se de uma interação em tempo real, que pode ocorrer presencialmente ou não.

A consideração dessa abordagem em relação à realização da entrevista abre novos horizontes para a pesquisa, possibilitando a obtenção de relatos de experiências provenientes de diversas culturas, sem se limitar às fronteiras territoriais dos países. Essa perspectiva ampliada permite uma análise mais abrangente e enriquecedora dos temas em estudo, promovendo uma compreensão mais profunda e holística dos fenômenos investigados.

A pesquisa mencionada, conduzida pela pesquisadora Leitao (2021), sugere que as entrevistas desempenham um papel fundamental na pesquisa qualitativa, fornecendo ao pesquisador uma fonte detalhada e profunda de informações sobre o tema em estudo, especialmente sobre aspectos que não podem ser totalmente compreendidos através da observação direta do fenômeno, essa assertiva é corroborada ainda no estudo de Leitao e Prates (2017). Segundo Leitao e Prates (2017), Leitao (2021) ao trabalhar com dados linguísticos, é possível construir uma rede complexa de significados relacionados ao fenômeno em análise, destacando a perspectiva única de cada participante e explorando as recorrências que surgem a partir desses diferentes prismas.

Dimensão Espacial

Leitao (2021) conceitua que a dimensão espacial descreve a disposição física dos interlocutores (pesquisador e entrevistado) em relação ao ambiente onde ocorre a entrevista, podendo ser entrevistas de forma remota ou presencial. Relata ainda que, este aspecto abrange não apenas a localização física, mas também a organização do espaço e sua influência na dinâmica da interação entrevistador-entrevistado.

Entrevista Presencial

Leitao (2021) explora a modalidade da entrevista presencial e ressalta as múltiplas vantagens associadas a essa prática histórica, observando que, ao estar frente a frente com o entrevistado, o pesquisador tem à sua disposição todas as informações disponíveis (sejam elas verbais, não verbais ou contextuais). Destaca-se que essa dinâmica favorece não apenas uma melhor condução da interação com o entrevistado, mas também a percepção de sutilezas expressas durante o diálogo. Além disso, Leitao (2021), Leitao e Prates (2017) argumentam que essa proximidade física cria um ambiente propício para a manifestação de uma fala espontânea e desprovida de censura.

Resumindo as conclusões dos estudos que abordam as metodologias qualitativas no âmbito das ciências da computação em Leitao e Prates (2017), bem como a utilização de

entrevistas para coletar relatos pessoais e experiências com o propósito de realizar uma análise aprofundada e construir uma compreensão a partir desses relatos em Leitao (2021), torna-se evidente que a entrevista presencial é uma ferramenta extremamente poderosa para a coleta de experiências vivenciadas pelos entrevistados. Isso se deve ao fato de que, durante uma entrevista presencial, não apenas as palavras são capturadas, mas também as emoções e nuances de cada contexto factual. As entrevistas realizadas pessoalmente tendem a criar um ambiente no qual o entrevistado se sente mais à vontade para compartilhar suas vivências, voluntariamente se colocando à disposição para relatar todos os aspectos de suas experiências. Essa proximidade física e emocional facilita uma comunicação mais profunda e autêntica, permitindo uma compreensão mais rica e completa do objeto de estudo.

Entrevista Remota

As entrevistas a distância tiveram sua difusão favorecida pelo desenvolvimento de tecnologias de comunicação síncronas cada vez mais amigáveis.(LEITAO, 2021). A pesquisadora coloca que esse tipo de entrevista é especialmente interessante para pesquisas cuja conversa envolve muito constrangimento e um certo grau de distanciamento é desejável para motivar a participação e a espontaneidade e que obviamente, ela também facilita e agiliza o encontro com participantes com os quais, por questões de localização, a entrevista presencial não é viável.

Em ambos os trabalho Leitao e Prates (2017) e Leitao (2021), apontam que não se deve priorizar a velocidade durante a pesquisa e sim a profundidade das informações obitidas nas entrevistas. Em síntese, o arcabouço teórico relativo às entrevistas realizadas de forma remota ressalta a importância de se garantir a qualidade na obtenção e no registro dos dados nesse formato. Além disso, estudos recentes destacam que os benefícios proporcionados por esse método frequentemente superam as dificuldades apresentadas. Ao conduzir entrevistas remotas, é crucial reconhecer que, quando o entrevistado está em um ambiente familiar e confortável, ele tende a se sentir mais à vontade para compartilhar suas experiências de maneira aberta e detalhada. Essa familiaridade com o ambiente pode contribuir significativamente para a qualidade e profundidade das informações coletadas

durante o processo de entrevista.

Dimensão Estrutural

Entrevistas Livres

Leitao (2021), coloca que as entrevistas livres não são estruturadas por um roteiro pré-estabelecido, permitindo uma abordagem mais flexível e exploratória. A pesquisadora alerta que é importante ressaltar que, mesmo nas entrevistas mais abertas, ligadas à pesquisa científica, há uma orientação para que os tópicos discutidos estejam alinhados com a questão de estudo em abordada. Portanto deixa a entender que, embora haja liberdade na condução da entrevista, ela ainda é direcionada para explorar aspectos relevantes ao tema em análise.

As pesquisadores Leitao e Prates (2017), trazem que esse tipo de entrevista é frequentemente utilizada como uma ferramenta de pesquisa-piloto, ajudando os pesquisadores a coletar insights valiosos que informam a construção de um roteiro mais definitivo e estruturado para futuras entrevistas. Também segundo Leitao (2021), através das entrevistas livres, os pesquisadores podem identificar temas emergentes, nuances e perspectivas dos participantes que podem não ter sido considerados inicialmente, enriquecendo assim o desenvolvimento do roteiro final.

Portanto, embora as entrevistas livres possam parecer menos formais e estruturadas, elas desempenham um papel fundamental no processo de pesquisa, contribuindo para a definição e refinamento das abordagens metodológicas utilizadas, e ajudando a garantir que as perguntas e discussões subsequentes sejam relevantes, significativas e bem direcionadas.

Entrevistas Estruturadas

Para Leitao (2021), as entrevistas de base estruturadas são caracterizadas pela adesão a uma definição e sequência rígida de formulação dos tópicos ou perguntas do

roteiro, de forma similar a um questionário. O estudo afirma que essa abordagem apresenta uma vantagem significativa ao conferir ao material coletado um alto potencial de comparabilidade entre as respostas dos participantes.

Em contraponto, a pesquisadora alerta que essa rigidez também traz consigo uma desvantagem importante, a limitação na coleta de significados espontâneos e não antecipados pelo pesquisador, mas que são considerados relevantes pelo próprio entrevistado. Segundo Leitao (2021), esta restrição pode comprometer a profundidade e a riqueza das informações obtidas durante o processo de entrevista.

Entrevistas Semiestruturadas

Leitao (2021) postula que as entrevistas semiestruturadas são amplamente preferidas em pesquisas científicas devido à sua capacidade de equilibrar a comparabilidade entre os depoimentos dos participantes e a abertura para a emergência de significados não planejados. A pesquisadora ressalta que as entrevistas semiestruturadas são por vezes equivocadamente confundidas com questionários, o que é uma comparação injusta. Isso se deve ao fato de que a definição de questionário implica em sua imutabilidade como um instrumento escrito e distribuído de forma padronizada. No entanto, as entrevistas semiestruturadas diferem significativamente, pois oferecem flexibilidade na condução do diálogo, permitindo a adaptação das perguntas de acordo com o contexto e as respostas dos participantes. Servem-se de um roteiro prévio mas obedecem um fluxo espontâneo de conversa.(LEITAO, 2021).

Com base na teoria apresentada, é possível concluir que as entrevistas semiestruturadas representam, na verdade, uma abordagem flexível e de fluxo natural, na qual as perguntas surgem organicamente conforme a conversa entre o entrevistador e o entrevistado se desenrola. Essa dinâmica permite uma maior profundidade na exploração dos temas discutidos, possibilitando a emergência de *insights* e nuances que podem não ser acessíveis em entrevistas estruturadas ou questionários padronizados. Essa flexibilidade inerente às entrevistas semiestruturadas as torna uma ferramenta valiosa para a pesquisa qualitativa, proporcionando uma compreensão mais rica e contextualizada dos fenômenos estudados e

isto pode ser analisado na Tabela 1.

Tabela 1 – As três dimensões da entrevista. (LEITAO, 2021)

Dimensão	**Características**			
		Livre	**Estruturada**	**Semiestruturada**
Estrutural	Roteiro	Não	Sim	Sim
	Flexibilidade	Sim	Não	Sim
	Comparabilidade	Não	Sim	Sim
Espacial	Presencial	Sim	Sim	Sim
	Remota	Sim	Sim	Sim
Temporal	Síncrona	Sim	Sim	Sim
	Interativa	Sim	Sim	Sim

4.1.4 Roteiro

Para apoiar a organização das perguntas ou itens, é interessante evitar uma sequência longa e linear das mesmas. Isto porque uma sequência longa de perguntas é de difícil consulta e visualização no momento da entrevista, contribuindo pouco para a organização do entrevistador.(LEITAO, 2021). Extrai-se do trabalho Leitao (2021) e Leitao e Prates (2017) que a estruturação do roteiro em blocos temáticos, onde itens ou perguntas relacionadas são agrupados, desempenha um papel fundamental no aprofundamento do tema e na orientação do entrevistado ao longo da entrevista reflexiva e exploratória. Essa abordagem facilita não apenas a organização do processo de entrevista, mas também proporciona uma direção clara para o diálogo, permitindo uma exploração mais abrangente e significativa dos tópicos em discussão. Para Leitao (2021), ao agrupar assuntos semelhantes, os blocos temáticos promovem uma análise mais aprofundada e uma compreensão mais rica do tema em questão, fornecendo um arcabouço sólido para a condução eficaz da entrevista.

O roteiro de execução da entrevista segue em blocos destacados com o objetivo de sanar as inquietações desta pesquisa. No primeiro bloco, é o momento inicial da entrevista que é apresentado ao entrevistado o contexto geral da pesquisa, deixando claro os objetivos os quais a investigação pretende alcançar, em sequeência, a motivação do trabalho e por fim a justificativa de se pesquiser este tema, apontando para o entrevistado o contexto do estado da arte atual acerca do tema da pesquisa. Ainda no primeiro bloco a pesquisadora Leitao (2021), afirma que é de suma importância que os blocos temáticos estabeleçam

um bom contato entre o pesquisador e os entrevistados e sugere a criação de um bloco denominado de 'Quebra-Gelo', onde este deixa evidente ao entrevistado a sequência da entrevista e como ela irá ocorrer, informando os blocos que serão percorridos, a duração e o modelo exploratório baseado em entrevistas. Na finalização do bloco, é feita a qualificação do entrevistado, tomando nota dos dados pessoais.

O segundo bloco tem uma estrutura com o objetivo de colher toda a descrição da experiência a qual o entrevistado se propôs a relatar. Busca-se a compreensão do contexto da ocorrência do ataque, trazendo os meios utilizados pelo atacante, qual tipo de comunicação foi estabelecida com a vítima, qual argumentação foi utilizada, a técnica empregada e percebida pela vítima, a vulnerabilidade humana explorada, deve-se ainda colher a descrição detalhada da reação que o entrevistado realizou no intuito de tentar mitigar o ataque de engenharia social, a descrição da eficácia da reação ante o ataque, qual o bem jurídico era alvo da investida maliciosa e compreender os sentimentos explorados.

Existem pesquisadores que defendem a inclusão desses aspectos na forma de itens abertos, destinados a servir como lembretes dos temas a serem abordados durante a entrevista.

Evita-se, dessa forma, a leitura artificial de perguntas prontas diante do entrevistado, priorizando-se que o entrevistador formule as perguntas em tempo real, com conteúdo fixo, mas com verbalizações diferenciadas, contextualizadas a partir do próprio vocabulário presente na conversa dos interlocutores (LEITAO; PRATES, 2017).

É suficiente ter feito uma única entrevista para saber a que ponto é difíci concentrar continuamente sua atenção no que está sendo dito (e não apenas nas palavras) e antecipar as perguntas capazes de se inscreverem "naturalmente" na continuidade da conversação seguindo uma espécie de "linha teórica". (BOURDIEU, 1998 apud LEITAO, 2021).

Para a melhor compreensão dos itens estabelecidos, utiliza-se indagações de esclarecimentos, estas tendo sido abordadas por Leitao (2021), que exemplifica como isto deve ser abordado: (como assim? ", "você pode me dar um exemplo?", "por quê?" etc.). A entrevista segue com uma lógica de conversação para evitar que a entrevista volte a

pontos já debatidos anteriormente e gere desconforto, seja por relembrar da experiência ou em decorrência dá sensação de euxastão do entrevistado. Para seguir um fluxo natural de conversação, a entrevista seguira a ordem cronologica dos acontecimentos, buscando a fluidez no dialógo. A entrevista terá uma duração mínima de 45 minutos, seguindo os itens declarados nos blocos temáticos.

4.1.5 Análise

A análise dos dados coletados nas entrevistas será realizada com o objetivo de transformá-los em informações pertinentes e relevantes para o presente estudo. Este processo não se limita à mera interpretação das respostas, mas envolve uma abordagem crítica e reflexiva, que busca identificar padrões, nuances e significados subjacentes nas opiniões dos entrevistados. Assim, procede-se à construção de uma perspectiva do entrevistador, fundamentada nas visões e experiências compartilhadas pelos participantes. Por meio desse diálogo entre as percepções individuais e a interpretação do pesquisador, busca-se não apenas compreender os fenômenos investigados, mas também situá-los em um contexto mais amplo, permitindo enriquecer as discussões teóricas e práticas relacionadas ao tema em questão (BOURDIEU, 1998 apud LEITAO, 2021). Segundo Leitao (2021), todo pesquisador que se dedica a estudos qualitativos deve estar ciente de que a análise dos dados provenientes das entrevistas não se resume à mera reprodução dos pontos de vista dos participantes; trata-se, portanto, de uma construção interpretativa (LEITAO, 2021). Além disso, o estudo ressalta que essa interpretação guarda correspondência clara com os dados coletados, onde a pontuação, a posição da vírgula e o registro de pausas ou expressões emocionais não apenas conferem um sentido ao depoimento, mas também desempenham um papel crucial na captura da riqueza semântica e na transmissão fiel das nuances expressivas dos participantes. Esses elementos moldam a estrutura do discurso e influenciam profundamente a percepção e a compreensão do conteúdo subjacente, destacando a importância da análise minuciosa da linguagem e do contexto na pesquisa qualitativa. "Assim, transcrever é necessariamente escrever, no sentido de reescrever", resume com propriedade o autor (BOURDIEU, 1998 apud LEITAO, 2021). Para complementar essa análise, utiliza-se a ferramenta ***Iramuteq***, que proporcionará uma análise textual das narrativas extraídas das entrevistas.

4.1.6 Considerações Finais

Diante do exposto, ratifica-se a adoção da abordagem metodológica qualitativa de maneira exploratória, valendo-se da aplicação de entrevistas como instrumento primordial para alcançar os propósitos delineados no primeiro capítulo deste estudo. Tal metodologia se mostra imprescindível para uma compreensão profunda e abrangente da engenharia social e sua gênese, permitindo uma análise rica em detalhes e nuances. Dessa forma, a escolha por esse método reforça o compromisso com a qualidade e a profundidade na investigação, visando não apenas obter resultados, mas também promover uma compreensão mais aprofundada da engenharia social e da contrainteligência adotada pelos entrevistados.

4.2 Protocolo de Pesquisa

Nesta seção, descreve-se a execução do planejamento metodológico, com ênfase nas decisões estratégicas e nas nuances que influenciaram o desenvolvimento e a implementação do protocolo de pesquisa. A metodologia empregada reflete a articulação entre os objetivos delineados no início da pesquisa e as abordagens investigativas que orientaram a coleta e a análise dos dados, com o intuito de validar o framework proposto. Este, por sua vez, constitui uma extensão do framework consolidado na literatura especializada, ampliando e refinando o estado da arte no domínio em questão. A escolha de cada procedimento foi cuidadosamente fundamentada na necessidade de garantir a robustez dos resultados e a coerência com as questões de pesquisa, assegurando que cada etapa do processo estivesse alinhada aos parâmetros estabelecidos para a investigação.

A construção do protocolo de pesquisa foi orientada pela necessidade de uma abordagem sistemática e rigorosa, capaz de proporcionar respostas precisas às hipóteses e objetivos propostos. Além disso, o capítulo explora as adaptações e ajustes realizados ao longo da execução, refletindo sobre os desafios encontrados e as soluções adotadas para superar as limitações contextuais e metodológicas. Ao integrar essas considerações, o capítulo proporciona uma visão detalhada da trajetória metodológica seguida, evidenciando como as decisões tomadas durante o processo de investigação contribuíram para a obtenção

de resultados válidos e confiáveis.

Este estudo é fundamentado nos princípios legais estabelecidos pela legislação em vigor, bem como em conceitos morais e éticos. Destaca-se que o projeto foi devidamente registrado junto à Plataforma Brasil e obteve aprovação sob o protocolo ***79474624.0.0000.5188***. Essa diligente observância das normativas legais e dos preceitos éticos ressalta o compromisso do estudo com a integridade e a responsabilidade na condução da pesquisa envolvendo humanos.

Este protocolo não se limita a um conjunto de procedimentos técnicos, mas reflete uma estrutura dinâmica, na qual a flexibilidade e a adaptação constante foram fatores cruciais para o sucesso da pesquisa. A descrição das etapas e das decisões metodológicas aqui apresentadas busca não apenas fornecer uma base sólida para a replicação do estudo, mas também oferecer uma reflexão crítica sobre as implicações das escolhas metodológicas no alcance dos objetivos da pesquisa.

4.2.1 Critérios

Foram estabelecidos critérios rigorosos de inclusão para a seleção inicial dos participantes, bem como definidos critérios de exclusão. Ressalta-se que a elegibilidade inicial não garante a continuidade no estudo, uma vez que, mesmo após a etapa de aceitação, o participante poderá ser posteriormente excluído, caso venha a atender a quaisquer dos critérios de exclusão previamente estipulados, comprometendo, assim, a pertinência de sua permanência nas etapas subsequentes da entrevista.

Critérios de Inclusão

- Experiência pretérita como vítima de ataques de engenharia social bem ou mal sucedidos;
- Idade entre 18-65 anos;
- Indivíduos com conhecimento ou envolvimento na área de Ciência da Computação;
- Concordar e assinar o Termo de Consentimento Livre e Esclarecido (TCLE).

Critérios de Exclusão

- Idade menor que 18 anos;
- Não concordar em assinar o Termo de Consentimento Livre e Esclarecido (TCLE);
- Não possuir experiência pretéritas com engenharia social;
- Declarar a qualquer momento e/ou ser percebido qualquer desconforto emocional ao relembrar eventos passados.

Impactos dos Critérios de Inclusão e Exclusão

Com a finalidade de salvaguardar o bem-estar emocional dos entrevistados, é fundamental considerar que recordar situações passadas envolvendo qualquer forma de sofrimento emocional pode causar consideráveis desconfortos, de modo que os critérios estabelecidos para a seleção não são passíveis de negociação em prol da ética na pesquisa científica. É imperativo respeitar esses critérios em nome da ética, e caso o entrevistado não preencha os requisitos cumulativos de inclusão ou se enquadre em algum critério de exclusão, a entrevista não poderá prosseguir. Tais critérios, tanto de inclusão quanto de exclusão, são definidos de forma cumulativa e excludente, ou seja, se o entrevistado atender a pelo menos um critério de exclusão, ele será automaticamente impedido de participar da entrevista. Essa abordagem rigorosa e inequívoca visa garantir que a pesquisa seja conduzida de maneira ética e responsável, protegendo os participantes de situações que possam gerar desconforto, constrangimento ou qualquer forma de prejuízo emocional. Por fim, a leitura e compreensão e a consequente assinatura do Termo de Consentimento Livre e Esclarecido (TCLE) é requisito cumulativo aos demais critérios de inclusão. Este procedimento visa assegurar ao pesquisador que o entrevistado foi devidamente informado sobre os detalhes da pesquisa, garantindo assim a segurança e integridade do processo.

Critérios de Inclusão

De forma lógica, a vivência direta com o objeto de estudo revela-se essencial; quanto mais profunda for essa imersão, mais rico e significativo tende a ser o relato pessoal oferecido durante a entrevista. O recorte etário entre 18 e 65 anos justifica-se pela ampla

familiaridade desse público com meios digitais, fator relevante para os objetivos da pesquisa. Além disso, a exigência de que os participantes tenham algum nível de conhecimento ou envolvimento com a área tecnológica fundamenta-se na premissa de que esse perfil apresenta maior resiliência frente a ataques cibernéticos. As respostas e estratégias adotadas por esses indivíduos diante de tentativas de violação são elementos-chave para a análise proposta neste estudo.

Critérios de Exclusão

Os critérios de exclusão, diferentemente dos critérios de inclusão — que possuem caráter cumulativo — são mutuamente excludentes. A participação de indivíduos com menos de dezoito anos é vedada, uma vez que essa faixa etária não possui, legalmente, plena capacidade de consentimento. Tal restrição é ainda mais relevante considerando a natureza sensível e complexa do tema tratado, que envolve experiências relacionadas a ataques cibernéticos, podendo incluir aspectos ligados a práticas ilícitas.

A ausência da assinatura no Termo de Consentimento Livre e Esclarecido também configura impedimento absoluto à participação, visto que esse documento é essencial para assegurar a voluntariedade e a compreensão plena dos objetivos e riscos envolvidos na pesquisa, além de proteger os direitos e a privacidade dos participantes.

Adicionalmente, qualquer manifestação de desconforto emocional durante a entrevista — seja por meio de verbalizações explícitas ou sinais não verbais evidentes — constitui motivo suficiente para a interrupção imediata, ou mesmo para que o processo de entrevista não seja iniciado. Tal precaução visa preservar o bem-estar e a integridade emocional dos entrevistados, assegurando que sua saúde mental seja sempre respeitada ao longo do estudo.

4.2.2 Blocos Temáticos

Conforme delineado na seção metodológica, todas as entrevistas foram conduzidas com base em um roteiro estruturado por blocos temáticos, o que proporcionou maior

fluidez à interlocução e atuou como referencial orientador da condução. Tal abordagem contribuiu para a manutenção do foco investigativo, minimizando desvios temáticos e assegurando a coerência dos dados obtidos.

Blocos Temáticos

Bloco Temático 1

- **Quebra-Gelo**
  - Recepção do Entrevistado
    - Explanar o contexto geral da pesquisa
      - objetivos
      - motivação
      - justificativa
    - Explicar o roteiro da entrevista
      - Blocos
      - Duração
      - Modelo exploratório
    - Qualificação
      - Nome
      - idade
      - sexo
      - curso em andamento
      - classe social *declarada

Bloco Temático 2

- **Itens Descritivos**
  - Compreensão do contexto do ataque
    - local da vítima no momento do ataque
      - compreensão sobre os meios digitais e físicos os quais foram utilizados
    - meio utilizado para a comunicação

    * argumento utilizado
    * técnica percebida
    * vulnerabilidade humana explorada
    * reação da vítima
    * eficácia da reação
    * Objeto Almejado
    * Sentimentos Explorados

Bloco Temático 3

- **Itens Explicativos**
  - Como o atacante escolheu a vítima
  - Como se deu a comunicação
  - Qual foi sua reação imediata
  - A reação imediata seria a mesma de agora
  - A resposta ao ataque foi suficiente, se não, como seria

Bloco Temático 4

- **Itens Hipotéticos**
  - Caso o atacante tivesse presencialmente, como seria o ataque e sua reação
  - E se, a reação não impedisse o ataque, qual seria o próximo passo para se defender
  - E se, essa o atacante utiliza-se de autoridade
  - E se, o ataque acontecer de modo que você não pudesse confirmar a identidade do atacante

Bloco Temático 5

- **Aferição de Postulado Teórico**
  - Busca conhecimento acerca dos ataques cibernéticos?
    * De que forma?

    * Por qual razão?
- Quais os últimos conhecimentos adquiridos sobre ataques cibernéticos envolvendo engenharia social?
- Atesta-se capaz de reagir a um ataque de engenharia social em curso?
- Acredita ter conhecimento suficiente para reduzir e até neutralizar um ataque de engenharia social?
- Caso não seja capaz de neutralizar um ataque de engenharia social de modo a inibir sua evolução, acredita ter informação suficiente para reagir a ponto ao menos mitigar os possíveis danos?

4.2.3 A captação de entrevistados

Para a seleção dos entrevistados, foram estabelecidos critérios rigorosos de inclusão e exclusão, com o objetivo de garantir que os participantes atendesse às características necessárias para a pesquisa e estivessem adequados ao perfil desejado. Além disso, os indivíduos interessados em participar foram instruídos a preencher um formulário eletrônico no qual deveriam fornecer uma descrição preliminar do caso, de forma superficial. Essa etapa foi fundamental para uma avaliação criteriosa da adequação do candidato, permitindo uma triagem inicial que minimizou a possibilidade de falsos positivos e assegurou a relevância dos participantes para o estudo.

Subsequentemente, os candidatos selecionados foram orientados a agendar a entrevista em um dos diversos dias e horários disponibilizados no formulário, oferecendo flexibilidade para atender às suas disponibilidades, garantindo assim uma maior adesão ao processo. Finalmente, para formalizar o processo de participação e assegurar o cumprimento das normas éticas da pesquisa, os participantes precisaram assinar o Termo de Consentimento Livre Esclarecido (TCLE), garantindo sua compreensão sobre os objetivos do estudo, a natureza da pesquisa e a utilização dos dados coletados.

4.2.4 As Entrevistas

As entrevistas foram conduzidas de maneira predominantemente fluida, com predominância da modalidade assíncrona na maioria dos casos, o que possibilitou maior flexibilidade e adequação às necessidades individuais dos participantes. O processo foi organizado em etapas distintas, contemplando momentos dedicados à formulação das perguntas e à coleta das respostas, sendo estas realizadas em formatos textuais e de áudio. O uso do áudio foi priorizado por sua capacidade de captar de maneira mais fidedigna as nuances emocionais e expressivas dos entrevistados, aspecto considerado essencial para a análise qualitativa da pesquisa.

Adicionalmente, as entrevistas transcenderam o formato presencial, incorporando o uso de recursos e plataformas digitais que viabilizaram a execução do estudo de forma abrangente e acessível. Foram empregadas diversas aplicações, como WhatsApp, Instagram, Microsoft Teams, Discord, Google Meet, Skype e Telegram, permitindo uma abordagem inclusiva e adaptável aos diferentes contextos dos participantes. Essa multiplicidade de ferramentas não apenas ampliou o alcance e a participação, mas também garantiu a coleta de dados em condições diversificadas, assegurando a robustez metodológica e o rigor científico na condução da pesquisa.

Em situações excepcionais, a incompatibilidade de horários entre o entrevistador e os entrevistados resultou na necessidade de estender a realização de algumas entrevistas ao longo de três dias consecutivos. Essa extensão revelou-se imprescindível para assegurar uma compreensão mais detalhada e aprofundada dos casos apresentados. Em determinados momentos, a duração prolongada do processo foi influenciada pela demora na emissão das respostas por parte dos entrevistados, o que exigiu uma adaptação no cronograma previamente estabelecido. Essa abordagem flexível foi adotada com o objetivo de preservar a qualidade e a integridade dos dados coletados, garantindo que as informações obtidas fossem suficientemente completas e representativas para os propósitos da pesquisa.

4.2.5 Identificação de Casos

Nesta seção, realiza-se a identificação e a anonimização dos casos descritos, com o objetivo de preservar a confidencialidade dos participantes e garantir a integridade da pesquisa. Para tanto, os nomes dos entrevistados serão substituídos pela expressão "entrevistado do CS - X", sendo "X" o número que corresponde a cada caso específico. Essa estratégia visa assegurar que a identidade dos indivíduos envolvidos nos relatos não seja revelada, promovendo o anonimato. Além disso, a nomenclatura utilizada para se referir aos casos será simplificada, passando de "CASO X" para "CS X", com a intenção de otimizar a leitura e a fluidez do texto, sem comprometer a clareza e a precisão da análise. Essa adaptação semântica facilita o entendimento e mantém o rigor acadêmico, além de proporcionar uma abordagem mais direta e objetiva no tratamento dos casos apresentados.

5 Resultados e Discussão

O presente capítulo tem como objetivo não apenas apresentar os resultados obtidos, mas também realizar uma análise crítica e aprofundada das implicações do framework proposto. Em um nível mais analítico, é realizada uma avaliação detalhada da interação entre este framework e as estratégias de defesa observadas nas entrevistas, tanto proativas quanto reativas, ressaltando tanto as potencialidades quanto as limitações intrínsecas a essas abordagens. Destaca-se, especialmente, a análise de similaridade apresentada na Figura 10, realizada por meio do software Iramuteq, que permite observar de maneira clara a convergência dos termos extraídos das entrevistas e suas conexões mais significativas. Entre os termos de maior interconexão, destacam-se: engenharia social, inteligência, contrainteligência, defesas proativa e reativa, e reação. Através dessa análise, torna-se possível delinear de forma precisa as relações centrais que permeiam os discursos dos entrevistados, oferecendo uma compreensão aprofundada das dinâmicas de segurança cibernética e das estratégias de defesa implementadas.

Ademais, o software mencionado também possibilitou a realização de uma análise adicional por meio de uma nuvem de palavras, apresentada na Figura 9, gerada com base nos dados extraídos das entrevistas. Esta abordagem visual permite a representação clara das palavras mais recorrentes e significativas, facilitando a identificação dos principais temas abordados pelos entrevistados, além de evidenciar padrões linguísticos e conceituais que se configuram como relevantes para a compreensão das questões discutidas.

Na seção 5.6, são ainda apresentados os metadados em forma de tabela, contendo informações detalhadas sobre os perfis dos entrevistados. Esses dados fornecem um contexto crucial para a análise, permitindo uma melhor compreensão das características demográficas e profissionais dos participantes, ao mesmo tempo em que possibilitam uma correlação mais precisa entre esses perfis e as tendências emergentes nos relatos sobre segurança cibernética.

A engenharia social, enquanto abordagem estratégica no campo da segurança da informação, fundamenta-se na exploração das vulnerabilidades humanas para a obtenção de objetivos maliciosos. No núcleo dessa prática, os atacantes elaboram métodos de intrusão

meticulosamente planejados, que, ao serem combinados com mecanismos de influência psicológica e comportamental, se tornam ferramentas altamente eficazes para manipulação das vítimas. Esses métodos amalgamam de forma sinérgica recursos técnicos e não técnicos, explorando as dimensões cognitivas, emocionais e sociais dos indivíduos. A eficácia dessas estratégias repousa, portanto, na exploração sistemática das fragilidades humanas, que incluem vulnerabilidades cognitivas, afetivas e socioculturais, tornando os alvos particularmente suscetíveis a manipulações.

Ao articular de maneira estratégica os métodos de ataque, os efeitos psicológicos e as vulnerabilidades humanas, os agentes de engenharia social são capazes de arquitetar cenários altamente persuasivos e complexos, que não apenas neutralizam resistências críticas, mas também facilitam a materialização dos objetivos maliciosos. A compreensão da interação entre esses componentes é essencial para desvendar a complexidade intrínseca desse fenômeno, além de ser um ponto crucial para o desenvolvimento de contramedidas robustas, que fortaleçam, de maneira integrada, tanto as defesas humanas quanto as tecnológicas, com vistas à mitigação dessas ameaças.

Para (WANG; ZHU; SUN, 2021), em seu framework sobre engenharia social, que aborda o prisma de quem ataca, o indivíduo visa criar certos cenários de ataque para conduzir uma combinação orgânica de métodos de ataque, mecanismos de efeito e vulnerabilidades humanas, através dos quais o processo de ataque tem efeito para atingir o objetivo do ataque.

No framework proposto neste estudo, a análise da reação da vítima diante de ataques de engenharia social é um aspecto central. Como apresentado no Capítulo 3, a estratégia de neutralização e/ou mitigação dos danos segue uma sequência bem estruturada, iniciando-se pela etapa de construção de inteligência, discutida na Seção 3.1. Essa fase tem como objetivo consolidar o conhecimento necessário sobre os ataques, permitindo compreender sua dinâmica e fornecer base sólida para a aplicação de medidas tanto proativas quanto reativas.

Na sequência, a Seção 3.2 explora em detalhes a defesa proativa, considerada a abordagem mais eficaz para prevenir a ocorrência de ataques. Essa estratégia antecipa ações ofensivas dos agentes maliciosos, buscando impedir que as ameaças se concretizem.

Em complemento, a Seção 3.3 trata da defesa reativa, voltada para responder a incidentes após sua identificação. Embora ocorra após o início do ataque, essa defesa tem papel crucial na contenção dos danos, reforçando a ideia de que ambas as abordagens são interdependentes e essenciais para um processo de proteção abrangente contra ameaças baseadas em engenharia social.

Já no Capítulo 5, especificamente nas Seções 5.1 e 5.2, são apresentados os resultados das entrevistas realizadas, seguidos de uma discussão crítica e aprofundada. Essa análise transversal busca ir além da simples descrição dos achados, interpretando-os à luz das teorias debatidas ao longo do trabalho e de sua aplicabilidade prática. Cada relato é examinado com atenção às suas particularidades, permitindo identificar padrões, revelar nuances e estabelecer conexões com os objetivos e hipóteses da pesquisa. A intenção é oferecer uma compreensão ampla e fundamentada dos fenômenos investigados, contribuindo significativamente para o entendimento dos mecanismos de defesa diante de ataques de engenharia social.

5.1 Resultados

As entrevistas realizadas fornecem uma visão abrangente das tendências emergentes nas fraudes cibernéticas, destacando a crescente sofisticação dos métodos utilizados pelos fraudadores e a exploração refinada das vulnerabilidades psicológicas das vítimas. Os relatos indicam que os fraudadores estão cada vez mais habilidosos em manipular as emoções humanas, como medo, ganância e a pressão por soluções rápidas, para induzir comportamentos precipitados. No entanto, também se evidenciou que a vigilância e o discernimento, frequentemente impulsionados pelo conhecimento prévio ou pela formação profissional das vítimas, desempenham um papel fundamental na mitigação dos danos. O estudo aponta que, apesar de algumas falhas nos sistemas de segurança e de controles internos em algumas organizações, a aplicação de um framework eficaz de defesa pode proporcionar uma barreira substancial contra as ameaças.

O framework proposto neste estudo se revela de extrema importância, demonstrando sua robustez ao ser validado pela reação das vítimas nos casos analisados. A combinação de defesas proativas e reativas, estruturadas com base no conhecimento de como os fraudadores agem, contribui significativamente para a eficácia da proteção contra os ataques de engenharia social. As vítimas que tomaram medidas de precaução baseadas em sua compreensão dos métodos fraudulentos conseguiram evitar ou minimizar os danos, evidenciando a aplicação prática e a relevância do framework no combate às fraudes digitais. Além disso, o estudo sugere que a educação digital e a conscientização são elementos chave, não apenas para os indivíduos, mas também para as organizações, para que a segurança cibernética seja tratada como um aspecto cultural e não exclusivamente técnico.

À medida que as fraudes digitais se tornam cada vez mais complexas, o framework proposto se destaca como uma abordagem holística e dinâmica, proporcionando uma base sólida para a adaptação às novas ameaças. A sua aplicação não apenas valida as premissas de defesa contra ataques de engenharia social, mas também oferece um caminho claro para futuras pesquisas e aprimoramentos, visando potencializar ainda mais a eficácia na mitigação de riscos e na proteção contra fraudes cibernéticas.

5.1.1 Estatísticas Gerais dos Casos

Este relatório apresenta uma análise detalhada com base nos dados fornecidos, incluindo gráficos, percentuais, estatísticas descritivas e interpretação dos resultados.

5.1.2 Estatísticas Gerais

- Total de casos analisados: **19**
- Média de idade: **38,9 anos**
- Mediana de idade: **38 anos**
- Distribuição por sexo:
  - Masculino: **63,2%**
  - Feminino: **36,8%**
- Resultados:
  - EVITOU: **52,6%**
  - DANO: **31,6%**
  - MITIGOU: **15,8%**

5.1.3 Gráficos e Análises

5.1.4 Distribuição por Sexo

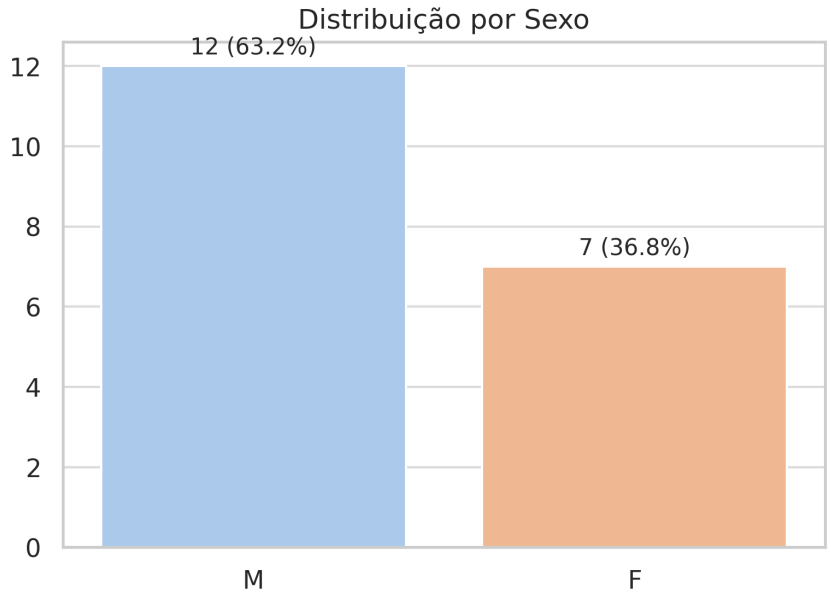

Figura 5 – Distribuição por sexo entre os participantes.

Interpretação: Há predominância masculina (63,2%) entre os participantes, mas os resultados não aparentam ser fortemente influenciados pelo sexo.

5.1.5 Distribuição de Idade

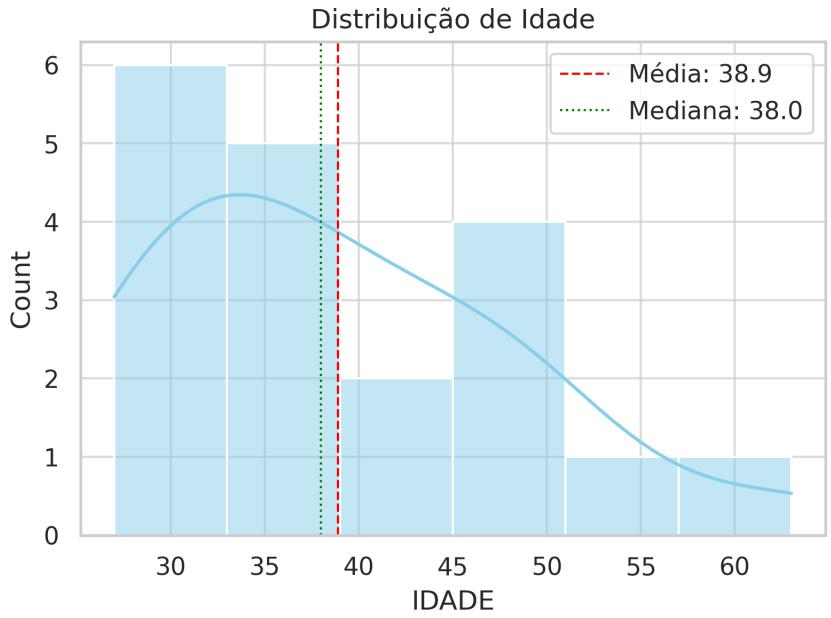

Figura 6 – Distribuição das idades dos participantes.

Interpretação: Idades variam entre 27 e 63 anos, com concentração na faixa de 28 a 47 anos. Média e mediana próximas indicam distribuição relativamente simétrica.

5.1.6 Tipo de Entrevista vs Resultado

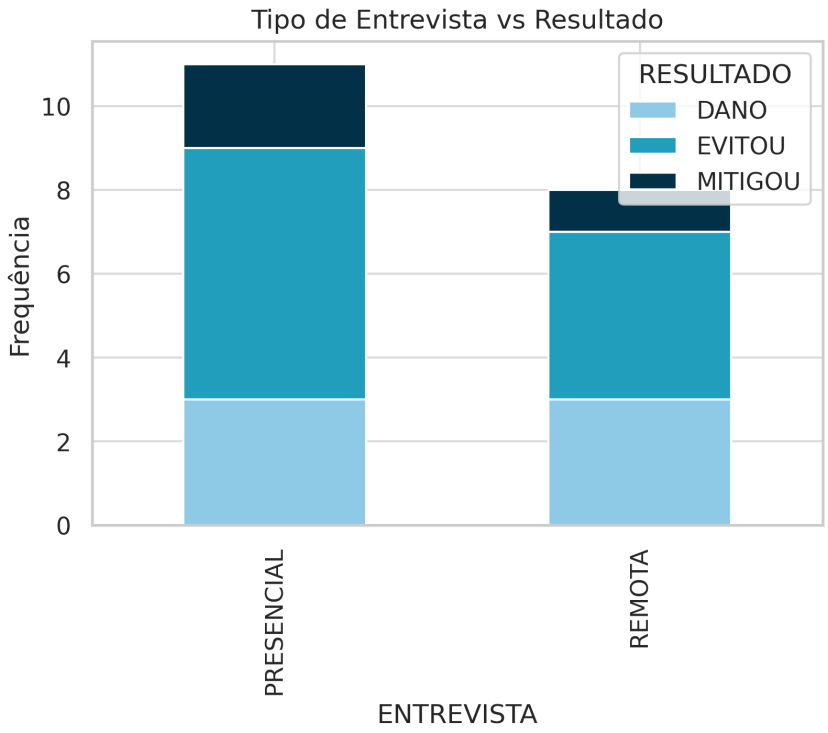

Figura 7 – Relação entre tipo de entrevista e resultado.

Interpretação: Entrevistas presenciais apresentam maior proporção de **EVITOU**, enquanto as remotas concentram mais casos de **DANO**.

5.1.7 Distribuição dos Resultados

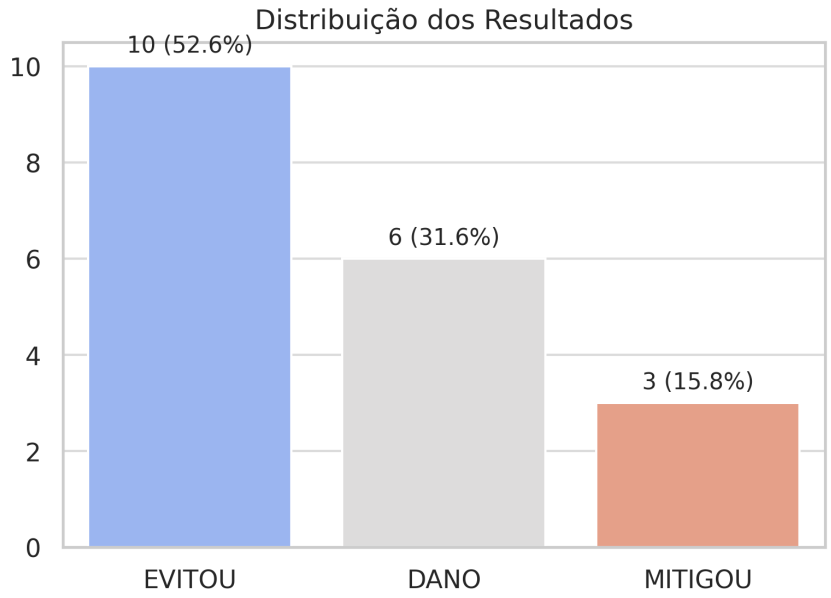

Figura 8 – Distribuição dos resultados finais.

Interpretação: A maioria (52,6%) conseguiu **EVITAR** problemas, 31,6% sofreram **DANO** e apenas 15,8% **MITIGARAM**.

5.1.8 CS1

Perfil do Entrevistado

Entrevistado: homem, 28 anos, ocupa a posição de responsável pela comunicação entre prepostos de empresas terceirizadas de tecnologia. Na época da entrevista, buscava aprimorar seus conhecimentos por meio de uma pós-graduação latu sensu com foco em Privacidade e Proteção de Dados.

Entrevista

Durante a entrevista, o relato do incidente de segurança, que o entrevistado se dispôs a compartilhar, foi feito de forma espontânea. No entanto, ao aprofundarmos a investigação sobre a responsabilidade direta de quem quebrou a cadeia de segurança, o entrevistado demonstrou visível desconforto. O ponto de tensão ocorreu quando foi questionado especificamente sobre qual elo da cadeia havia sido comprometido, o que resultou no encerramento abrupto da entrevista. Esse comportamento gerou discussões sobre as dificuldades enfrentadas por indivíduos ao assumirem responsabilidades ou ao detalharem falhas no contexto organizacional, o que pode dificultar a identificação precisa de vulnerabilidades.

5.1.9 CS2

Perfil do Entrevistado

Entrevistado: homem, 34 anos, coordenador de TI em uma empresa de médio porte, com ampla experiência na administração de redes e sistemas de segurança. O entrevistado busca conhecimento na area de redes no curso do mestrado profissional na mesma cidade em que trabalha.

Entrevista

O entrevistado relatou um incidente ocorrido durante a implementação de um sistema de gestão de dados. Ele descreveu como um funcionário recém-contratado, ao tentar acessar informações sensíveis, foi manipulado por um ataque de phishing altamente sofisticado. O atacante, se passando por um superior hierárquico, conseguiu persuadir o funcionário a fornecer suas credenciais de acesso, resultando em uma violação de dados. O entrevistado destacou a falta de treinamentos regulares sobre segurança digital como um fator importante para o sucesso do ataque. Ao ser questionado sobre os processos de verificação de segurança, o entrevistado revelou que a empresa estava em processo de atualização de suas políticas, mas sem uma estratégia de conscientização clara para os colaboradores.

5.1.10 CS3

Perfil do Entrevistado

Estrevistado: mulher, 52 anos, professora de ensino superior(graduação em cursos de tecnologia), está ativa em programa de pós-graduação em nível doutoral.

Entrevista

A entrevistada relatou que foi vítima de um ataque de engenharia social, no qual sua senha de acesso ao sistema de ensino da instituição em que exerce a docência foi comprometida, resultando em uma alteração indevida nas notas dos alunos sob sua responsabilidade. O atacante, utilizando-se de informações públicas disponíveis na internet, elaborou um ataque sofisticado que envolveu manipulação psicológica, induzindo a entrevistada a acreditar que estava acessando um portal legítimo da instituição. Esse ataque, caracterizado pela utilização de um site falso que replicava a interface do sistema de ensino real, visava especificamente capturar as credenciais da vítima. De acordo com o relato, o criminoso utilizou dados acessíveis sobre a entrevistada, como seu nome e afiliação institucional, para construir uma comunicação convincente e aparentemente legítima. A vítima recebeu um e-mail que, pela clareza e correção na redação, parecia ser uma mensagem institucional autêntica, levando-a a clicar em um link direcionado a um portal de acesso ao sistema de ensino. Sem perceber a fraude, a entrevistada inseriu suas credenciais na página falsa, o que possibilitou ao atacante o acesso ao sistema. Uma vez dentro do sistema, o atacante alterou as notas dos alunos, atribuindo-lhes, indiscriminadamente, a nota máxima. Esse tipo de ataque exemplifica como a engenharia social pode ser usada para explorar a confiança e a familiaridade dos usuários com os sistemas institucionais, comprometendo sua segurança. A eficácia do golpe reside justamente na habilidade do atacante em criar uma simulação tão convincente do ambiente legítimo, que a vítima, sem desconfiança, fornece suas informações sensíveis de forma voluntária.

5.1.11 CS4

Perfil do Entrevistado

Entrevistado: homem, 63 anos, analista de sistema de uma empresa estatal de tratamento de dados, está ativo em programa de pós-graduação em nível de mestrado.

Entrevista

Foi relatado que, devido à natureza da empresa estatal onde o entrevistado atua, a qual armazena e gerencia serviços de terceiros no âmbito da administração pública estadual, o profissional tem acesso a uma grande quantidade de informações sigilosas relacionadas aos serviços hospedados nesta instituição. Dada a sensibilidade dos dados com os quais a estatal lida, ela se torna um alvo constante de tentativas de ataques cibernéticos ao longo do ano. Para mitigar esses riscos e garantir a proteção das informações, a empresa realiza treinamentos frequentes e rotineiros com seus colaboradores, com o objetivo de manter a equipe sempre atualizada sobre as melhores práticas de segurança cibernética. Além disso, o entrevistado destacou a prática do '*Daily Report*', um exercício diário no qual os profissionais elaboram relatórios detalhados sobre o status de segurança dos sistemas e infraestruturas, visando identificar vulnerabilidades e manter um alto nível de vigilância e proteção contra ameaças externas. Em um dos relatos, o entrevistado mencionou um caso específico em que um atacante obteve as credenciais de uma servidora da estatal por meio de uma relação amorosa. Aproveitando-se da confiança estabelecida, o atacante conseguiu acesso a diversos sistemas e informações sigilosas, incluindo dados sensíveis relacionados aos serviços da Secretaria de Segurança Pública, o que evidenciou para o entrevistado, o risco de ataques baseados em engenharia social dentro do ambiente corporativo, relatou.

5.1.12 CS5

Perfil do Entrevistado

Entrevistado: mulher, 29 anos, atua diretamente com qualidade e testes de aplicações. Busca conhecimento na área de segurança e testes em nível latu sensu.

Entrevista

Durante a entrevista, foi relatado um incidente envolvendo uma tentativa de ataque cibernético por meio de engenharia social. O evento teve início quando um indivíduo, que se apresentou como representante de uma empresa parceira, estabeleceu contato por e-mail de forma formal e convincente. O atacante utilizou um tom amigável e demonstrou um conhecimento superficial do ambiente corporativo, o que conferiu maior credibilidade à interação. A comunicação inicial concentrou-se em questões técnicas relacionadas à integração de sistemas, momento em que o atacante formulou diversas perguntas sobre a infraestrutura de segurança da organização.

A solicitação de informações sensíveis, geralmente não compartilhadas com terceiros, despertou desconfiança, levando à interrupção da comunicação. O agressor tentou criar um vínculo de confiança, mencionando sua experiência anterior em segurança da informação e sugerindo uma colaboração para o aprimoramento da proteção dos sistemas. Em determinado momento, solicitou dados detalhados acerca do processo de testes de segurança, argumentando que essas informações seriam cruciais para uma análise de riscos mais aprofundada. Contudo, sinais de manipulação foram identificados e a comunicação foi interrompida. Na sequência, o atacante intensificou seus esforços, buscando outros meios de contato, como telefonemas, nos quais se apresentou de maneira ainda mais persuasiva, utilizando um número falsificado que aparentava ser legítimo.

A capacidade de identificar as tentativas de manipulação foi atribuída ao treinamento contínuo em segurança cibernética. Em resposta ao incidente, a equipe responsável pela segurança da informação foi notificada, adotando as medidas adequadas para bloquear o atacante e reforçar as práticas de segurança cibernética. O evento sublinhou a importância

de manter vigilância constante contra tentativas de engenharia social, mesmo em contextos aparentemente profissionais, e ressaltou a necessidade de atualização e aprofundamento contínuos no campo da segurança da informação, relatou.

5.1.13 CS6

Perfil do Entrevistado

Homem, 36 anos, analista de TI em uma empresa de segurança eletrônica, com foco em soluções de monitoramento e automação, está buscando especialização em Inteligência Artificial aplicada à segurança por meio de um curso de mestrado.

Entrevista

O entrevistado relatou um incidente envolvendo falsificação de biometria em um sistema de ponto eletrônico utilizado para registrar a presença de alunos em uma autoescola. O caso foi investigado e posteriormente confirmado por meio de câmeras de monitoramento instaladas no local. A fraude foi perpetrada por um aluno da autoescola e um terceiro envolvido, que utilizaram uma técnica sofisticada para enganar o sistema de registro de frequência. A estratégia criminosa consistia no uso de um dedo artificial, fabricado com material de silicone, para registrar a presença do aluno em momentos em que ele não se encontrava no local das aulas, as quais exigiam presença física obrigatória para cumprimento de requisitos. O uso de biometria como método de controle de frequência, embora seja considerado uma tecnologia segura, foi burlado devido à aplicação dessa técnica de falsificação. Após a descoberta da fraude, os indivíduos responsáveis foram identificados e devidamente processados, conforme as disposições da legislação vigente. O incidente ilustra as vulnerabilidades que podem ser exploradas em sistemas de segurança baseados em biometria, além de destacar a importância de medidas adicionais de verificação e monitoramento para garantir a integridade dos sistemas de controle de frequência em contextos diversos, relatou.

5.1.14 CS7

Perfil do Entrevistado

Profissional do sexo feminino, 28 anos, atua como administradora de sistemas em uma empresa do setor logístico. Possui sólida experiência na administração de servidores e redes corporativas. Atualmente, está em processo de especialização na área de cibersegurança, cursando uma pós-graduação com o objetivo de ampliar seus conhecimentos e fortalecer sua atuação no campo da segurança da informação.

Entrevista

A entrevistada relatou que recebeu uma mensagem de texto ('SMS') em seu telefone informando sobre o uso de seu cartão de crédito em uma compra online no valor de R$ 2.500,00. A mensagem destacava que, caso a compra não fosse reconhecida, ela poderia entrar em contato com um número fornecido na própria mensagem. Preocupada, a entrevistada ligou imediatamente para o número indicado, buscando resolver o suposto erro. Ao atender a ligação, uma pessoa se passou por um representante do serviço de atendimento ao cliente da operadora do cartão de crédito. O suposto atendente pediu que ela confirmasse informações pessoais, como o número completo do cartão, a senha de segurança e dados adicionais para verificar a transação. Embora tenha se sentido um pouco desconfortável com a abordagem, a entrevistada estava em estado de alerta devido ao valor significativo da compra mencionada e, por isso, forneceu os dados solicitados, acreditando que estava resolvendo o problema de forma legítima. Após a troca de informações, a entrevistada não recebeu mais nenhum retorno, o que a fez perceber que algo estava errado. Quando verificou sua conta bancária, constatou que várias transações não autorizadas haviam sido realizadas com seu cartão de crédito. Ao contatar a operadora do cartão para relatar o ocorrido, foi informada de que a ligação que ela recebera e as instruções fornecidas eram, na verdade, parte de uma tentativa de fraude. O incidente resultou em um prejuízo financeiro significativo e revelou a complexidade das táticas de engenharia social, nas quais os atacantes exploram a confiança e o desespero das vítimas para obter informações sensíveis. A entrevistada alertou sobre a importância de desconfiar de qualquer comunicação não solicitada, especialmente quando se trata de solicitações de dados pessoais,

e ressaltou a necessidade de medidas de segurança mais rigorosas, como a verificação em dois fatores e a vigilância constante sobre transações bancárias.

5.1.15 CS8

Perfil do Entrevistado

Homem, 29 anos, técnico de redes em uma pequena empresa de soluções em TI, busca especialização em segurança de redes e está cursando pós-graduação em Segurança Cibernética.

Entrevista

O relato do entrevistado descreve um incidente envolvendo uma técnica sofisticada de *deepfake*, na qual o indivíduo foi alvo de uma tentativa de fraude por meio de comunicação não solicitada via aplicativo de mensagens instantâneas, mais especificamente, o *WhatsApp*. No contexto desse ataque, a mensagem recebida continha um vídeo manipulado digitalmente de uma personalidade amplamente reconhecida e com elevado prestígio social no âmbito empresarial. A mensagem, produzida através de técnicas de *deepfake*, apresentava a figura da celebridade como porta-voz de uma proposta de investimento de caráter supostamente exclusivo, na qual o entrevistado seria convidado a participar mediante o envio de um pagamento para uma conta bancária especificada na própria mensagem. A manipulação de vídeo, caracterizada pelo uso de *deepfake*, visava induzir o entrevistado a acreditar na veracidade da oferta, criando uma ilusão de legitimidade e uma distorção da realidade, aproveitando-se da autoridade associada à imagem da referida personalidade. Frente a essa tentativa de engano, o entrevistado adotou uma postura proativa e, de forma imediata, bloqueou o número de origem do contato, prevenindo qualquer possível continuidade da interação fraudulentamente estabelecida. Essa ação de bloqueio evidenciou uma resposta decisiva no sentido de evitar maiores prejuízos, demonstrando vigilância e discernimento frente a ataques de natureza psicológica e digital. Este episódio ilustra não apenas a crescente sofisticação dos ataques de engenharia social baseados em deepfakes, mas também a importância da conscientização e da capacitação dos indivíduos para identificar e reagir adequadamente a ameaças cibernéticas de caráter manipulativo.

5.1.16 CS9

Perfil do Entrevistado

Mulher, 31 anos, coordenadora de projetos de TI em uma empresa de telecomunicações, com experiência em gestão de infraestrutura e desenvolvimento de soluções de TI, está cursando mestrado em Gerenciamento de Projetos de TI.

Entrevista

A entrevistada relatou uma experiência de engenharia social ocorrida em ambiente físico, na qual foi abordada por um indivíduo com intenções fraudulentas em uma instituição bancária, especificamente na área destinada ao autoatendimento, no contexto de uso de um caixa eletrônico. O atacante, adotando uma abordagem aparentemente cordial, ofereceu assistência à entrevistada na operação do equipamento. Durante a interação, ao solicitar o cartão da entrevistada com o pretexto de ajudá-la no uso do terminal, o atacante substituiu sutilmente o cartão legítimo por um cartão falso, sem que a vítima percebesse a troca no momento. Após a interação, a entrevistada, sem notar a substituição do cartão, prosseguiu com suas atividades, retornando ao seu veículo e seguindo para sua residência. A fraude só foi percebida posteriormente, quando, ao tentar realizar uma compra, a entrevistada percebeu que o cartão em sua posse não funcionava corretamente, revelando, assim, o golpe consumado. Este incidente exemplifica a aplicação de técnicas de engenharia social em um contexto físico, no qual a confiança estabelecida pelo atacante, aliada à distração e ao desconhecimento da vítima, resultou na realização de uma troca fraudulenta de cartões. A situação sublinha a vulnerabilidade dos indivíduos a manipulações psicológicas em cenários cotidianos e destaca a importância de estratégias de prevenção, que envolvam não apenas a conscientização sobre a segurança digital, mas também a vigilância em situações de interação direta, mesmo em ambientes tradicionalmente seguros, como agências bancárias.

5.1.17 CS10

Perfil do Entrevistado

Homem, 52 anos, técnico de suporte em uma instituição de ensino, com experiência no suporte a sistemas e redes acadêmicas, busca especialização em segurança em redes educacionais através de um curso de pós-graduação.

Entrevista

O entrevistado, relatou ter recebido um e-mail aparentemente enviado pelo setor de TI da instituição, solicitando a atualização de suas credenciais de acesso ao servidor acadêmico devido a uma suposta manutenção de segurança. O e-mail, bem elaborado e com o logo oficial da instituição, continha um link para validar suas credenciais. No entanto, ao verificar a URL, o técnico notou uma discrepância no endereço, que não correspondia ao oficial do sistema. Desconfiado, ele não inseriu suas credenciais e entrou em contato com a central de TI, confirmando que se tratava de uma tentativa de phishing.

5.1.18 CS11

Perfil do Entrevistado

Homem, 38 anos, desenvolvedor de software em uma empresa de consultoria tecnológica, busca aprimorar seus conhecimentos em arquitetura de sistemas distribuídos e está cursando um mestrado profissional.

Entrevista

O entrevistado relatou um incidente ocorrido durante sua participação em um pregão eletrônico destinado à contratação de uma empresa de consultoria especializada em tecnologia, com a finalidade de planejar a expansão do parque tecnológico de uma entidade pública. Durante a fase de lances do certame, o entrevistado recebeu uma ligação telefônica alegando que o sistema do pregão estava enfrentando dificuldades técnicas, e solicitando-lhe que se desconectasse da plataforma para tentar um novo acesso. Além disso, o interlocutor requereu suas credenciais de acesso, justificando que seria necessário realizar um procedimento para "liberar"o sistema e resolver o alegado problema técnico. Diante dessa solicitação, o entrevistado, cético em relação à veracidade da informação e à natureza da abordagem, resistiu à pressão e optou por manter sua conexão ativa no pregão. Ele compreendeu que, caso interrompesse sua participação e saísse da plataforma, perderia a oportunidade de retornar à fase de lances, o que implicaria em sua eliminação automática do processo licitatório. A situação foi prontamente identificada como uma tentativa de ataque de engenharia social, no qual o atacante buscava obter informações sensíveis, como as credenciais de acesso, com o intuito de comprometer a integridade do certame e obter vantagem indevida. Este episódio exemplifica de forma clara e precisa o uso de estratégias de engenharia social em processos licitatórios eletrônicos, evidenciando as táticas fraudulentas utilizadas por indivíduos mal-intencionados para manipular os participantes e obter acesso a dados confidenciais. A postura vigilante e a resistência do entrevistado em ceder às demandas do atacante destacam a importância crucial da conscientização, do ceticismo e da vigilância constante em ambientes digitais, especialmente em contextos de alta competitividade, como os pregões eletrônicos. Esse incidente pode ser visto como um aprendizado para a necessidade de implementar medidas preventivas e

de promover uma cultura organizacional voltada para a segurança da informação, a fim de mitigar os riscos associados a ataques desse tipo.

5.1.19 CS12

Perfil do Entrevistado

Homem, 27 anos, programador de software em uma startup de tecnologia, especializado no desenvolvimento de aplicativos móveis, busca qualificação por meio de um curso stricto sensu na área de computação, com foco em informática.

Entrevista

O entrevistado relatou que, após a apresentação de um trabalho acadêmico em um congresso de abrangência nacional, passou a receber uma série de e-mails oferecendo-lhe a publicação de seu artigo em um periódico de alto nível acadêmico, por um valor aparentemente acessível de 100 dólares. Inicialmente, atraído pela oportunidade de divulgar sua pesquisa, o entrevistado realizou o pagamento requerido para a publicação. Contudo, ao buscar esclarecimentos junto aos organizadores do periódico sobre os procedimentos subsequentes, o entrevistado começou a perceber indícios de que se tratava de uma fraude. A desconfiança foi confirmada quando, ao tentar entrar em contato com a operadora de seu cartão de crédito para resolver a situação, ele descobriu que o serviço oferecido não possuía a legitimidade anunciada. Em resposta à fraude, o entrevistado formalizou o pedido de cancelamento da transação junto à operadora do seu cartão de crédito, apresentando as evidências coletadas durante o processo para comprovar a natureza enganosa da transação. Após a análise do caso pela operadora, o entrevistado conseguiu reaver integralmente os valores pagos, após a defesa reativa. Esse episódio exemplifica a crescente prevalência de golpes no contexto acadêmico, particularmente no que diz respeito a ofertas fraudulentas de publicação científica, utilizando estratégias de engenharia social para explorar a credulidade de pesquisadores e acadêmicos. A resposta assertiva do entrevistado e a recuperação dos valores demonstram a importância da vigilância digital e da conscientização sobre as práticas fraudulentas no meio acadêmico, além de evidenciar a necessidade de mecanismos de proteção, como os serviços de contestação de transações financeiras.

5.1.20 CS13

Perfil do Entrevistado

Homem, 32 anos, consultor de tecnologia em uma empresa de segurança cibernética, trabalha com testes de penetração e auditoria de sistemas e está fazendo pós-graduação em Cibersegurança.

Entrevista

O entrevistado relatou a experiência de ter recebido, por meio de seu aplicativo de mensagens *Telegram*, uma oferta aparentemente promocional que incluía um link, o qual alegava necessitar de acesso direto a partir do dispositivo móvel do destinatário. Reconhecendo a alta probabilidade de que se tratasse de uma tentativa de fraude cibernética, o entrevistado, em virtude de sua expertise avançada em cibersegurança, optou por adotar uma abordagem estratégica e proativa, ao invés de simplesmente desconsiderar a ameaça, com o intuito de identificar o perpetrador do golpe. Consciente das táticas de engenharia social comumente empregadas em ataques desse gênero, o entrevistado criou um link manipulativo, concebido para coletar uma gama abrangente de informações sobre os dispositivos que realizassem requisições para ele. O link, meticulosamente desenvolvido, foi projetado para capturar dados críticos, como a localização geográfica do dispositivo, o endereço IP, o tipo de navegador e de dispositivo em uso, o endereço MAC, além de ativar remotamente a câmera do aparelho, permitindo a captura de imagens do atacante. Em um movimento subsequente, o entrevistado encaminhou ao atacante um link disfarçado sob o título "comprovante de pagamento", estrategicamente elaborado para induzir o alvo a clicar, resultando no redirecionamento do atacante para a página manipulada. Esse redirecionamento possibilitou ao entrevistado a coleta de informações fundamentais, incluindo imagens capturadas pelas câmeras frontal e traseira do dispositivo móvel utilizado pelo atacante, bem como sua localização exata e o endereço IP utilizado na conexão. Após a coleta dessas informações, o entrevistado procedeu de forma diligente, formalizando um boletim de ocorrência e repassando todos os dados obtidos às autoridades competentes, especificamente à Polícia Civil, com o objetivo de possibilitar uma investigação formal e potencial localização do infrator. Este episódio não apenas evidencia a habilidade do

entrevistado em empregar seus conhecimentos técnicos em cibersegurança de forma prática e eficaz, mas também ilustra a crescente sofisticação dos ataques baseados em engenharia social, que combinam manipulação psicológica com exploração técnica. O uso de estratégias de contra-ataque fundamentadas em uma análise aprofundada dos mecanismos de ataque sublinha o framework aqui proposto como a contrainteligencia pode ser empregada de maneira ativa e estratégica na identificação e neutralização de ameaças cibernéticas. Adicionalmente, destaca a relevância de capacitação técnica especializada para apoiar as autoridades na identificação e responsabilização de criminosos cibernéticos, contribuindo assim para o fortalecimento das respostas institucionais no combate a fraudes digitais e outras infrações no espaço cibernético.

5.1.21 CS14

Perfil do Entrevistado

Mulher, 46 anos, chefe de departamento de TI em uma empresa pública, possui mais de 20 anos de experiência na área e está buscando aprimorar seu conhecimento em gestão de riscos e segurança cibernética por meio de um mestrado.

Entrevista

A entrevistada relata que foi vítima de um ataque no qual o atacante enviou um e-mail solicitando acesso a um email o qual a entrevistada sabia não ser do solicitante. O atacante, escreveu no corpo do email que estarai sem acesso a um determinado email e que seu chefe estava necessitando enviar um relatório com urgencia a um determinado orgão de controle fiscal e que para isto, precisava do acesso ao email do gestor que seria ordenador de despesa naquela edilidade. A entrevistada, na posção de chefe do departamento de Tecnologia da informação responsável por liberar os acessos aos emails institucionais, mesmo sendo verdadeiro o email, carecia do tramite correto para a liberação do referido acesso e relatou ainda que estranhou aquela forma de requerimento não seria o procedimento adotado no ordinário.

5.1.22 CS15

Perfil do Entrevistado

Mulher, 33 anos, arquiteta de sistemas em uma empresa de soluções em nuvem, possui uma formação acadêmica em Ciência da Computação e está buscando uma pós-graduação em Computação em Nuvem.

Entrevista

A entrevistada relatou, com considerável detalhamento, a ocorrência de uma tentativa de golpe cibernético orquestrada por meio de uma comunicação eletrônica fraudulenta, na qual o atacante se fez passar, de maneira estratégica e engenhosa, pela empresa fornecedora de energia elétrica. A sofisticada manipulação visou explorar a confiança da vítima ao fazer uso de elementos visuais e linguísticos que imitavam com precisão a aparência e o estilo das comunicações oficiais da companhia legítima. O infrator, com o intuito de causar a impressão de autenticidade, elaborou um e-mail que, à primeira análise, parecia perfeitamente legítimo, ao empregar um endereço eletrônico virtualmente idêntico ao utilizado pela empresa, o que visava enganar a vítima e criar uma falsa sensação de segurança. No corpo da mensagem, o criminoso anexou um documento cuidadosamente preparado para simular a fatura mensal do consumo de energia elétrica, contendo valores e informações detalhadas sobre o consumo, estruturados de forma a imitar com precisão os elementos típicos das faturas oficiais emitidas pela companhia. Tais informações foram dispostas de maneira a criar uma ilusão de veracidade e credibilidade, induzindo o destinatário a acreditar que estava diante de uma comunicação genuína. A fatura apresentava, ainda, detalhes que tornavam a fraude ainda mais convincente, como o uso de termos técnicos específicos e a inclusão de códigos de barras, com a clara intenção de tornar o e-mail ainda mais realista e difícil de ser detectado como uma fraude. O principal objetivo do atacante, segundo a entrevistada, seria induzir a vítima a tomar ações específicas que comprometeriam sua segurança cibernética, como clicar em links embutidos no e-mail ou abrir arquivos maliciosos anexados. Essas ações poderiam resultar em sérias consequências, incluindo o roubo de dados pessoais, informações bancárias ou outras credenciais sensíveis, com implicações diretas para a segurança financeira e privacidade da vítima. A natureza

sofisticada do ataque, que buscava explorar a confiança da vítima em uma comunicação que aparentava ser de uma fonte confiável, é um indicativo claro da evolução das técnicas de engenharia social utilizadas em fraudes digitais. Contudo, a entrevistada, demonstrando um elevado grau de cautela e discernimento, percebeu imediatamente as incongruências no e-mail, particularmente no que se referia à procedência do endereço eletrônico e ao formato do conteúdo, que destoava de práticas habituais da empresa de energia elétrica. Essa percepção crítica e a tomada de uma postura proativa impediram que a vítima fosse induzida a tomar ações precipitadas, como o clique nos links ou a abertura de arquivos, evitando assim os danos que poderiam ter sido causados pelo golpe. Este incidente destaca não apenas a crescente sofisticação das fraudes digitais, mas também a necessidade urgente de conscientização e educação contínuas sobre segurança cibernética, tanto por parte dos consumidores quanto das organizações que operam no meio digital. A evolução dos métodos utilizados pelos criminosos evidencia a capacidade adaptativa desses ataques, tornando-os cada vez mais difíceis de detectar e, consequentemente, mais perigosos. Assim, o caso sublinha a importância fundamental de se manter vigilante diante de tentativas de fraudes virtuais e de adotar práticas preventivas, como a verificação cuidadosa da origem das mensagens e a utilização de ferramentas de segurança robustas, a fim de mitigar os riscos e proteger dados sensíveis em um cenário digital cada vez mais desafiador.

5.1.23 CS16

Perfil do Entrevistado

Homem, 50 anos, gerente de TI em uma instituição financeira, com vasta experiência em gestão de infraestrutura de TI. Atualmente, está cursando um MBA em Governança de TI.

Entrevista

O entrevistado, um usuário experiente de mesas online de poker, participa ativamente de jogos nos quais realiza apostas em valores reais, convertidos da moeda brasileira (real) para dólares americanos, conforme o modelo adotado pela plataforma em questão. O ambiente virtual e toda a comunicação entre os participantes são conduzidos exclusivamente em inglês, idioma no qual o entrevistado possui competência linguística avançada, garantindo-lhe plena capacidade para interagir e estabelecer comunicações eficazes com os demais jogadores. Essa proficiência na língua estrangeira é um fator que, de certa forma, proporciona uma inserção mais qualificada do entrevistado no universo digital das apostas, tornando-o um jogador experiente e consciente das dinâmicas do jogo online. Em uma mesa qualquer, o entrevistado foi abordado por um dos participantes da mesa, que lhe apresentou uma proposta de parceria que, à primeira vista, parecia vantajosa e alinhada aos seus interesses. O atacante, utilizando-se de uma retórica estratégica e sedutora, ofereceu-lhe uma oportunidade de ascensão no ranking da plataforma, prometendo-lhe um aumento considerável de pontos, o que garantiria ao entrevistado o acesso a mesas de maior prestígio, com jogadores de nível profissional e celebridades do poker, além de perspectivas de retornos financeiros mais elevados. O esquema, aparentemente, envolvia um pagamento significativo por parte do entrevistado, cujo montante seria destinado à aquisição dos pontos prometidos, os quais, por sua vez, alavancariam sua posição no ranking, resultando em vantagens competitivas dentro da plataforma. Movido pela ambição e pelo desejo de acelerar sua ascensão no jogo, o entrevistado decidiu realizar o pagamento solicitado, acreditando na veracidade da proposta. No entanto, após a transação, não houve qualquer alteração substancial em sua posição no ranking, tampouco foram creditados os pontos prometidos. O entrevistado se viu, então, confrontado com a realidade de que

fora vítima de um golpe cibernético. A frustração, decorrente da falha em atingir os objetivos esperados, foi acentuada pela percepção de que ele não tinha como reivindicar formalmente seus direitos dentro da plataforma. O conhecimento prévio do entrevistado sobre a ilegalidade da prática de compra de pontos, amplamente proibida pelas políticas da plataforma, gerou um sentimento de apreensão e de impossibilidade de recorrer a qualquer tipo de assistência, uma vez que o reconhecimento público do golpe poderia implicar em sanções disciplinares, incluindo a exclusão de sua conta e outras penalidades decorrentes da infração das normas da plataforma. Esse entendimento jurídico e ético sobre a natureza ilegal da transação, aliado ao temor das repercussões legais, impediu que o entrevistado tomasse medidas formais para contestar a fraude, o que o deixou em uma posição de vulnerabilidade irreparável. O atacante, por sua vez, desapareceu com os valores pagos, sem deixar rastros ou meios de resgatar a quantia. O entrevistado, então, se viu impotente, sem alternativas viáveis para reverter a situação ou recuperar o valor perdido. O relato do entrevistado ilustra de forma clara e contundente as complexas dinâmicas de fraude e engano presentes no universo das apostas online. Ele expõe as vulnerabilidades intrínsecas de indivíduos que, movidos por uma busca incessante por vantagens rápidas e ascensão no jogo, acabam sendo alvos de criminosos que se utilizam de promessas fraudulentas e técnicas de manipulação psicológica, explorando a ganância e o desejo de sucesso dos jogadores. Este caso também evidencia a multiplicidade de fatores envolvidos em fraudes digitais no contexto do jogo online, incluindo as questões legais, éticas e psicológicas, que tornam as vítimas frequentemente hesitantes em buscar reparações formais. Além disso, a situação ressalta a necessidade urgente de educação digital e de uma maior conscientização sobre os riscos associados a comportamentos imprudentes no ambiente virtual, bem como a importância de vigilância contínua por parte dos jogadores, que devem estar atentos a propostas que, aparentemente, se apresentam como oportunidades vantajosas, mas que, na realidade, são armadilhas destinadas a explorar suas fraquezas e vulnerabilidades.

5.1.24 CS17

Perfil do Entrevistado

Homem, 47 anos, diretor de TI em uma empresa de grande porte do setor bancário(meios de pagamentos), com ampla experiência em governança de TI e compliance, atualmente está cursando doutorado em Computação.

Entrevista

O entrevistado relatou, com minúcia, a experiência de uma tentativa de golpe cibernético orquestrada por meio de uma comunicação telefônica fraudulenta, na qual o atacante se disfarçou como representante de uma instituição financeira renomada. Durante a ligação, o criminoso alegou que o cartão de crédito do entrevistado havia sido indevidamente utilizado em transações online, e que, como medida de precaução para a proteção de sua conta, seria necessário confirmar imediatamente seus dados pessoais. O golpista, de forma estratégica e manipuladora, solicitou informações altamente sensíveis, incluindo o número do cartão de crédito, o nome impresso no cartão, o código de segurança (CVV) e a data de validade, com o intuito de obter os dados essenciais para a realização de transações fraudulentas. O atacante, ao empregar uma técnica clássica de engenharia social, procurava explorar a confiança e o senso de urgência do entrevistado, utilizando a justificativa de "segurança"para induzi-lo a fornecer informações críticas. Contudo, o entrevistado, demonstrando um elevado grau de discernimento e uma postura vigilante, reconheceu de imediato os sinais típicos de uma fraude, os quais incluem a solicitação de dados confidenciais sob a alegação de emergência. Essa percepção rápida, aliada ao seu conhecimento prévio sobre as táticas comuns de fraude telefônica, possibilitou-lhe tomar a decisão de uma defesa pró-ativa acertada vindo a interromper a conversa de forma imediata, desligando o telefone e evitando fornecer qualquer dado pessoal ou bancário ao criminoso. Como uma medida de proteção adicional e de defesa pró-ativa, o entrevistado procedeu ao bloqueio do número telefônico utilizado pelo golpista, antecipando qualquer nova tentativa de contato ou manipulação. Tal ação não apenas neutralizou a ameaça iminente, mas também demonstrou a eficácia de uma abordagem proativa e cautelosa no enfrentamento de fraudes digitais, as quais são frequentemente disfarçadas como interações

legítimas com entidades financeiras. Este episódio destaca, de maneira significativa, a crescente sofisticação das tentativas de fraude por meio de engenharia social, nas quais os atacantes se aproveitam da confiança e do medo do indivíduo para obter dados sensíveis. A resposta imediata e racional do entrevistado ilustra a importância de uma conscientização contínua acerca dos riscos cibernéticos e da necessidade de vigilância constante. Além disso, a situação sublinha a relevância de cultivar uma postura crítica frente a comunicações inesperadas, especialmente aquelas que demandam informações confidenciais, reiterando a indispensabilidade da educação digital e da formação de uma cultura de segurança cibernética robusta para a mitigação de riscos associados a fraudes.

5.1.25 CS18

Perfil do Entrevistado

Homem, 39 anos, desenvolvedor de software em uma empresa de soluções em nuvem, especializado em segurança de aplicativos, está fazendo mestrado em informática com foco em engenharia de software.

Entrevista

O entrevistado compartilhou um relato detalhado sobre sua experiência como vítima de uma tentativa de fraude em um jogo online, especificamente no MMORPG WYD - With Your Destiny. O incidente teve início quando o atacante entrou em contato com o entrevistado e lhe fez uma proposta aparentemente vantajosa: a venda de uma conta de jogo, a qual o golpista alegou ter um valor estimado superior a meio salário mínimo, mas ofereceu por um valor significativamente inferior, cerca de vinte por cento do valor de mercado da conta. A proposta seduziu o entrevistado, que, diante da perspectiva de adquirir uma conta com recursos valiosos e vantagens dentro do jogo, se viu atraído pela oferta. O golpista, com o intuito de criar um ambiente de confiança e garantir que o entrevistado se sentisse seguro durante o processo, permitiu que o comprador realizasse o login na conta, possibilitando-lhe visualizar todos os detalhes e funcionalidades da conta de jogo. Esse acesso inicial ao perfil da conta, que parecia genuíno, fortaleceu a confiança do entrevistado na legitimidade da negociação, levando-o a decidir pela compra da conta. Convencido da veracidade da transação, o entrevistado efetuou o pagamento por meio de uma transferência eletrônica, conforme acordado. No entanto, após a conclusão do pagamento, e embora o entrevistado ainda estivesse logado na conta, o atacante, de maneira fraudulenta, alterou os dados de segurança da conta, começando pela modificação do endereço de e-mail associado a ela. Posteriormente, o golpista alterou a senha de acesso, tomando controle absoluto da conta e impedindo que o entrevistado pudesse recuperá-la. A ação de modificar o e-mail e a senha de acesso foi realizada de maneira estratégica, aproveitando-se da confiança inicial gerada pela falsa transparência do processo. Mesmo após a realização do pagamento e enquanto o entrevistado ainda estava logado, o atacante conseguiu, com relativa facilidade, se apropriar dos dados de login e transferir a posse da conta para si. Após a alteração dos dados de

segurança e da senha da conta, o entrevistado foi impedido de acessar o perfil adquirido, e todas as tentativas subsequentes de reaver a conta foram infrutíferas. Desprovido de meios para reverter a transação e sem a possibilidade de acessar a conta de jogo ou recuperar os valores pagos, o entrevistado se viu em uma situação de vulnerabilidade extrema. O atacante, por sua vez, obteve não apenas o controle da conta, mas também a quantia transferida, deixando a vítima sem recursos ou alternativas viáveis de reparação. Este caso exemplifica de maneira paradigmática as intricadas dinâmicas das fraudes virtuais no contexto dos jogos online, nas quais os golpistas exploram de forma astuta a confiança dos jogadores, empregando técnicas de manipulação avançadas, fundamentadas na engenharia social, para perpetrar enganos. A fraude aqui descrita não apenas revela as estratégias sofisticadas utilizadas pelos atacantes, mas também ressalta a necessidade premente de uma vigilância contínua e do desenvolvimento de práticas aprimoradas de segurança nos ecossistemas digitais. Esse aspecto é particularmente relevante em plataformas de jogos, onde as transações financeiras, muitas vezes desprovidas de regulamentação formal, se tornam alvo de abusos, exacerbando a vulnerabilidade dos usuários. A experiência do entrevistado ilustra com clareza as dificuldades intrínsecas enfrentadas pelos jogadores ao tentar recuperar valores ou ativos digitais após a ocorrência de fraudes desse tipo. Além disso, evidencia a lacuna existente na implementação de mecanismos de reparação ou regulação eficazes, os quais, ao se mostrarem insuficientes ou inexistentes, contribuem para a perpetuação de práticas fraudulentas e dificultam a proteção dos usuários.

5.1.26 CS19

Perfil do Entrevistado

Homem, 45 anos, gerente de TI em uma empresa de sistemas e meios de pagamentos, com experiência em gestão de infraestrutura e automação de processos industriais, está cursando doutorado em Sistemas de Controle e Automação.

Entrevista

O entrevistado relatou um incidente ocorrido durante o processo de recrutamento e seleção para a contratação de um novo colaborador na área de Tecnologia da Informação de sua empresa, da qual ocupa o cargo de gerente. O candidato em questão demonstrou uma disposição atípica para aceitar uma proposta salarial substancialmente inferior à média do mercado, considerando seu nível de qualificação e experiência. Embora tal comportamento tenha gerado desconforto e suspeitas iniciais, o setor de Recursos Humanos, em sua avaliação, optou por proceder com a contratação, presumindo que o candidato representasse uma oportunidade vantajosa para a equipe, dado o seu perfil técnico. No entanto, após a integração do colaborador à equipe, foram observados problemas significativos nos repositórios de código com os quais ele conseguiu interação. A empresa, por não ter implementado uma gestão robusta de acessos e permissões nos sistemas críticos, não conseguiu identificar a natureza do problema de imediato. Com o tempo, ficou claro que o colaborador não possuía as intenções que havia externado durante o processo seletivo. Na realidade, tratava-se de um agente infiltrado, contratado por uma empresa concorrente com o propósito deliberado de sabotar as operações da organização e, possivelmente, roubar informações confidenciais, comprometendo a integridade do processo de desenvolvimento de um sistema estratégico para a empresa. Este episódio revela, de forma contundente, a vulnerabilidade das organizações frente a ameaças internas camufladas sob a aparência de colaboradores legítimos. Ele também destaca a importância crucial de uma gestão de acessos criteriosa e estratégica, especialmente em ambientes organizacionais que lidam com dados sensíveis e ativos intelectuais de alto valor. A falha em estabelecer restrições adequadas de acesso aos repositórios de código e a ausência de uma política de segurança da informação suficientemente robusta expuseram a empresa ao risco de exploração de

sua confiança e recursos por um agente mal-intencionado. Ademais, este caso ilustra a crescente sofisticação das ameaças cibernéticas no contexto corporativo, evidenciando a necessidade de processos de recrutamento mais rigorosos, aliados a uma vigilância constante sobre as ações dos colaboradores e ex-colaboradores, sobretudo em relação ao acesso e manipulação de ativos digitais críticos. A falha em identificar a ameaça interna e a subsequente exploração dos pontos fracos na arquitetura de segurança da organização sublinham a importância de uma abordagem holística e proativa na mitigação de riscos relacionados à segurança cibernética, que envolva tanto a prevenção de ameaças externas quanto a identificação e contenção de ameaças internas.

5.1.27 CS20

Perfil do Entrevistado

Mulher, 38 anos, professora universitária na área de Computação, com experiência em ensino e pesquisa em sistemas embarcados e internet das coisas (IoT). Possui mestrado em Engenharia Elétrica e está cursando doutorado em Computação com foco em Sistemas Inteligentes.

Entrevista

A entrevistada, relatou que foi alvo de uma tentativa de golpe de engenharia social envolvendo a plataforma de pagamentos instantâneos, o Pix. Ela recebeu uma mensagem de texto em seu celular, aparentemente enviada pelo banco em que possui conta. O texto informava que uma transação de grande valor havia sido realizada em sua conta e solicitava que ela confirmasse a operação imediatamente para evitar bloqueio de sua conta. A mensagem estava bem estruturada e parecia legítima, incluindo o nome do banco, logotipo e até mesmo um número de atendimento que parecia oficial. A mensagem informava também que, para "reverter"a transação, ela deveria clicar em um link que redirecionaria para uma página de login de seu banco, onde deveria confirmar a operação e fornecer alguns dados de segurança. Embora a mensagem fosse convincente, a professora percebeu que algo estava errado. Ela desconfiou do tom urgente e do fato de que o número de telefone não correspondia ao canal de atendimento oficial de seu banco. Além disso, o link não levava ao site oficial do banco, mas a um endereço suspeito, com um domínio ligeiramente modificado. Antes de tomar qualquer ação, ela decidiu verificar diretamente com o banco. Ligou para o número oficial de atendimento ao cliente, que confirmou que não havia qualquer transação sendo realizada em sua conta e que a mensagem era, de fato, uma tentativa de golpe. O atendente também orientou sobre os passos a seguir para garantir a segurança de sua conta. A professora então bloqueou o número de telefone do golpista e alertou seus colegas e amigos sobre o golpe, para que estivessem atentos a tentativas semelhantes. Ela também revisou suas configurações de segurança bancária, incluindo o uso de autenticação de dois fatores, para garantir maior proteção contra possíveis ataques futuros.

5.1.28 Metadados

Tabela 2 – Tabela Metadados da Pesquisa.

COD	SEXO	IDADE	TCLE	DATA	ENTREVISTA	REAÇÃO/DEFESA			RESULTADO
						SEM REAÇÃO	PRÓ-ATIVA	REATIVA	
CS1	M	28	X	05/09/2024	PRESENCIAL	-	-	-	-
CS2	M	34	X	06/07/2024	REMOTA	NÃO	X	X	DANO
CS3	F	42	X	07/07/2024	PRESENCIAL	SIM	X	SIM	MITIGOU
CS4	M	63	X	08/07/2024	REMOTA	SIM	X	SIM	MITIGOU
CS5	F	29	X	09/07/2024	PRESENCIAL	SIM	SIM	X	EVITOU
CS6	M	36	X	10/07/2024	PRESENCIAL	SIM	X	SIM	MITIGOU
CS7	F	28	X	11/07/2024	PRESENCIAL	NÃO	X	X	DANO
CS8	M	29	X	12/07/2024	REMOTA	SIM	SIM	X	EVITOU
CS9	F	31	X	13/07/2024	REMOTA	NÃO	X	X	DANO
CS10	M	52	X	14/07/2024	REMOTA	SIM	SIM	X	EVITOU
CS11	M	38	X	15/07/2024	PRESENCIAL	SIM	SIM	X	EVITOU
CS12	M	27	X	16/07/2024	PRESENCIAL	SIM	X	SIM	EVITOU
CS13	M	32	X	17/07/2024	PRESENCIAL	SIM	SIM	X	EVITOU
CS14	F	46	X	18/07/2024	REMOTA	SIM	SIM	X	EVITOU
CS15	F	33	X	19/07/2024	PRESENCIAL	SIM	SIM	X	EVITOU
CS16	M	50	X	20/07/2024	PRESENCIAL	NÃO	X	X	DANO
CS17	M	47	X	21/07/2024	REMOTA	SIM	SIM	X	EVITOU
CS18	M	39	X	22/07/2024	PRESENCIAL	NÃO	X	X	DANO
CS19	M	45	X	23/07/2024	REMOTA	NÃO	X	X	DANO
CS20	F	38	X	24/07/2024	PRESENCIAL	SIM	SIM	X	EVITOU

Figura 9 – Nuvem de Palavras (*iramuteq*) Fonte: Elaborado pelo autor.

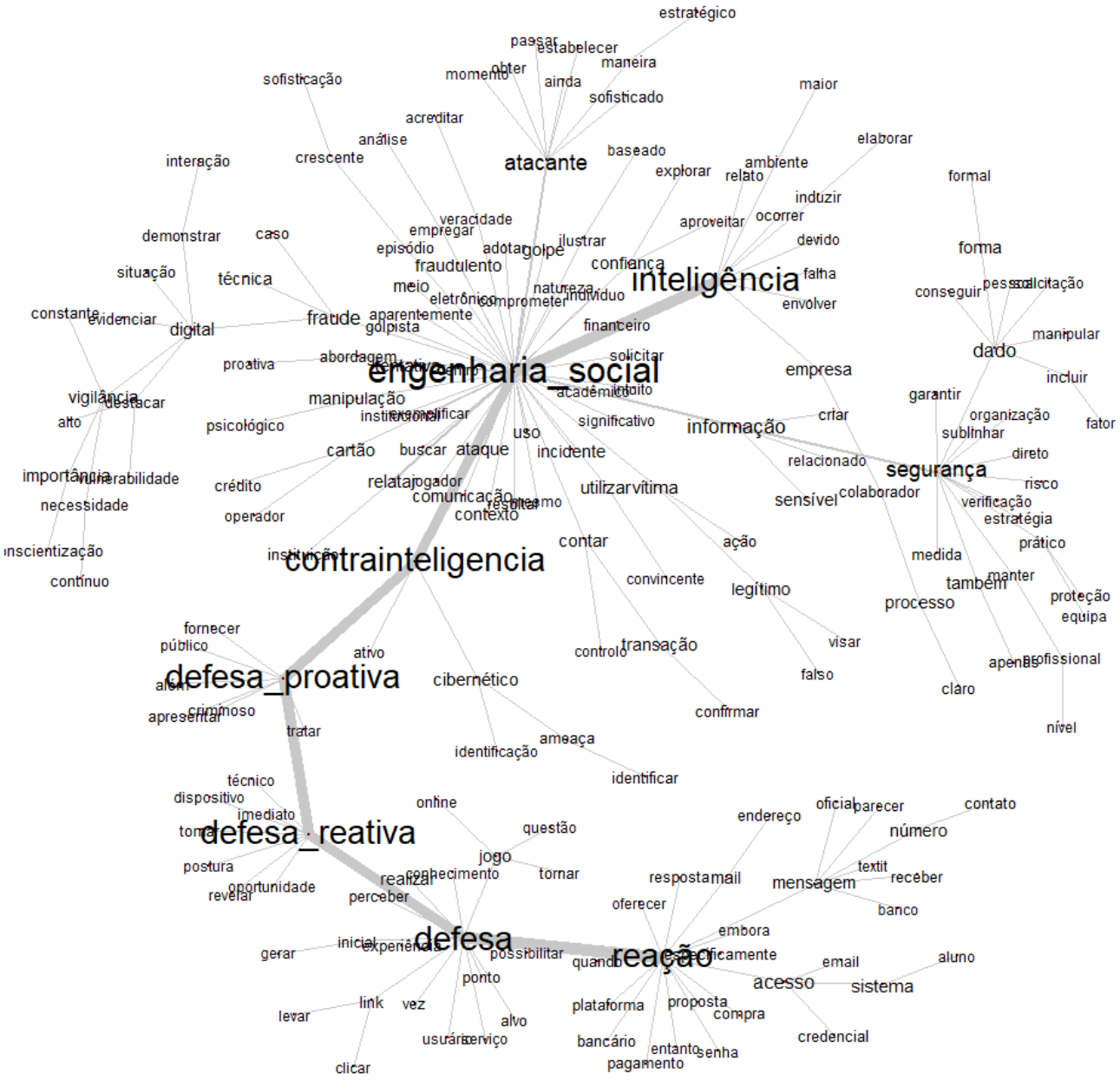

Figura 10 – Análise de Similitude (*iramuteq.*) Fonte: Elaborado pelo autor.

5.2 Discussão

Nesta seção, realizamos uma análise aprofundada e uma discussão transversal das entrevistas realizadas, com o objetivo de identificar padrões e tendências comuns que emergem das experiências relatadas pelos entrevistados. Cada relato proporciona uma perspectiva distinta sobre a segurança cibernética, evidenciando como as ameaças virtuais se manifestam de maneira complexa e multifacetada no cotidiano de indivíduos com perfis variados, desde profissionais de TI até jogadores e consumidores. Com base nessas entrevistas, abordaremos questões centrais relacionadas à crescente sofisticação dos golpes cibernéticos, aos fatores que facilitam a exploração das vulnerabilidades dos alvos e às estratégias de defesa empregadas pelos entrevistados. Além disso, discutiremos práticas recomendadas para mitigar riscos, aprimorar as respostas a incidentes de segurança e promover uma maior conscientização sobre a importância da segurança digital no enfrentamento dessas ameaças emergentes.

5.2.1 Análise e Discussão

A primeira e mais marcante característica observada nos relatos é a crescente sofisticação das fraudes cibernéticas, extrapolando o mundo digital e vindo também ao meio fisico. Nos relatos de golpes, como o ocorrido com a professora universitária vítima de uma tentativa de phishing envolvendo o Pix (CS20), e o gerente de TI que foi abordado por um golpista em um jogo online (CS18), percebe-se que os criminosos estão cada vez mais habilidosos em criar comunicações falsas que imitam a aparência e o tom das interações legítimas, utilizando mesmo os nomes de marcas e plataformas de confiança. Este fenômeno é visível em múltiplos casos, como a tentativa de fraude por e-mail que se passou pela fornecedora de energia elétrica (CS15) e a manipulação no jogo de poker online (CS16), onde os golpistas adotam um discurso persuasivo e convincente para explorar as fraquezas psicológicas dos alvos.

Os métodos utilizados pelos criminosos mostram uma estratégia cada vez mais refinada, em que, ao invés de simples tentativas de engano, eles procuram estabelecer um contexto de urgência, confiança ou vantagem, levando os indivíduos a tomar decisões

precipitadas. Isso fica evidente no caso do diretor de TI que foi abordado por telefone por um golpista que se fez passar por representante de um banco (CS17), e também nas tentativas de fraude por meio de transações financeiras no contexto dos jogos online (CS18).

Uma característica comum nas tentativas de fraude descritas é a exploração de fatores psicológicos que tornam os indivíduos mais vulneráveis. No caso de um golpista em um jogo de poker online (CS16), a promessa de ascensão no ranking do jogo e a perspectiva de ganhos financeiros foi suficiente para enganar o jogador, fazendo-o acreditar em uma oferta vantajosa. Esse mesmo princípio foi observado no caso do gerente de TI, em que o golpista criou uma sensação de urgência, solicitando dados bancários sob o pretexto de proteger a conta contra um uso indevido (CS17). Em ambos os casos, o fator psicológico da ganância e do medo foi explorado para facilitar a transação fraudulenta.

Além disso, há uma exploração do desejo humano de uma solução rápida ou de "atacar oportunidades"que se apresentam como vantajosas, como exemplificado pelo golpista que manipulou um desenvolvedor de software com uma conta de jogo falsa (CS18) ou o caso da professora universitária, que recebeu uma mensagem do banco alegando uma transação não autorizada (CS20).

Esses casos demonstram que os fraudadores estão cientes de que os seres humanos frequentemente tomam decisões baseadas em emoções, como o medo de perder uma vantagem ou a necessidade de resolver rapidamente um problema, como no caso da tentativa de fraude envolvendo o Pix (CS20). Eles utilizam esses gatilhos para induzir os alvos a agir sem a devida cautela.

Um ponto de convergência nas entrevistas está na vigilância e discernimento demonstrados pelas vítimas, que, em sua maioria, conseguiram identificar sinais de alerta antes de tomar decisões erradas. O caso da professora universitária (CS20), que desconfiou da mensagem recebida e optou por verificar diretamente com o banco, exemplifica a importância de manter uma postura crítica diante de mensagens não solicitadas, mesmo quando elas parecem genuínas. O mesmo cuidado foi demonstrado pelo diretor de TI (CS17), que rapidamente identificou a fraude telefônica e tomou as medidas necessárias para se proteger.

Essas ações de defesa indicam que a conscientização e o conhecimento sobre as práticas de fraude desempenham um papel fundamental na prevenção de danos. Em todos os relatos, as vítimas utilizaram de alguma forma sua experiência prévia ou formação profissional para detectar as fraudes. O entrevistado de TI (CS16), com um perfil altamente técnico, possuía a experiência necessária para perceber as inconsistências no e-mail de phishing, assim como a mulher, arquiteta de sistemas, que reconheceu os sinais da fraude ao lidar com um e-mail falso. Esses comportamentos desempenham um papel crucial na validação e fortalecimento da eficácia do framework proposto neste estudo, corroborando sua relevância e aplicabilidade diante dos desafios apresentados pela engenharia social. A inter-relação entre as estratégias de defesa e as reações observadas diante dos ataques demonstra a robustez do modelo, evidenciando sua capacidade de adaptação e resposta diante de um cenário dinâmico e em constante evolução. A análise desses comportamentos, portanto, não apenas valida as premissas do framework, mas também oferece uma base empírica sólida para futuras refinamentos e ajustes que possam potencializar ainda mais a sua eficácia na mitigação de riscos associados a essas ameaças.

Embora a vigilância seja uma resposta eficiente à fraude, a ausência de sistemas de segurança robustos e a falta de medidas preventivas também facilitaram as fraudes em alguns casos. O entrevistado que sofreu uma tentativa de golpe em sua conta de jogo (CS18) ficou vulnerável, pois não havia mecanismos adequados para prevenir fraudes no ambiente de jogos online. Isso ressalta a importância de uma regulamentação e de práticas mais rigorosas de segurança no setor de jogos online e outras plataformas digitais que envolvem transações financeiras.

Além disso, em outros casos, a falta de um gerenciamento adequado de acessos e permissões, como no caso do gerente de TI (CS19), expôs a empresa a um ataque interno deliberado. A empresa não conseguiu detectar a ameaça a tempo, pois não havia controles suficientes sobre o acesso aos sistemas críticos, permitindo que um agente mal-intencionado, aparentemente um colaborador legítimo, sabotasse o ambiente digital da organização.

Os relatos apontam para a necessidade urgente de educação digital e conscientização, tanto para os indivíduos quanto para as organizações. A grande maioria dos entrevistados demonstrou uma atitude pró-ativa na defesa contra as fraudes, o que, sem dúvida, pode ser

atribuído ao seu nível de conhecimento sobre segurança cibernética. Contudo, é evidente que a maioria das vítimas de golpes não são especialistas, e muitas podem não ter o discernimento necessário para detectar fraudes. Portanto, a educação digital precisa ser mais acessível e aplicável à vida cotidiana das pessoas, com foco em como identificar sinais de fraude e como agir de maneira segura e eficaz quando confrontadas com ameaças cibernéticas.

Além disso, a conscientização também deve se estender ao ambiente corporativo. O caso do gerente de TI (CS19) ressalta a importância de processos de recrutamento rigorosos, aliados a uma vigilância constante sobre os colaboradores e o acesso a informações sensíveis dentro das empresas. A segurança cibernética não deve ser vista apenas como uma responsabilidade técnica, mas como uma questão cultural, que envolve todos os níveis organizacionais.

Em resumo, as entrevistas revelam um quadro claro sobre as tendências emergentes no campo das fraudes cibernéticas. A sofisticação dos métodos de engano, a exploração de vulnerabilidades psicológicas, a importância da vigilância e da educação digital, e a necessidade de robustecer sistemas de segurança, são questões cruciais que emergem dessas experiências. À medida que as fraudes digitais se tornam cada vez mais complexas, a melhor defesa continua sendo a conscientização, o discernimento e a adoção de práticas preventivas, tanto a nível individual quanto corporativo.

6 Conclusão

Com base no levantamento da literatura e considerando os trabalhos previamente analisados e as referências consultadas para a compreensão do tema em discussão, conclui-se que o objeto de pesquisa investigado demanda um aprofundamento temporal e analítico mais abrangente, a fim de possibilitar uma compreensão integral e multidimensional.

Apesar dessa limitação, foi possível delinear uma compreensão inicial acerca do comportamento da vítima e de sua percepção durante um ataque de engenharia social. Observou-se que as estratégias utilizadas pelos atacantes exploram vulnerabilidades humanas fortemente relacionadas a fatores emocionais e cognitivos, o que reforça a complexidade e relevância do fenômeno em questão.

A presente investigação contribui, ainda que de forma preliminar, para o direcionamento de futuras pesquisas que visem a elaboração de um framework mais abrangente e eficaz, incorporando políticas e recomendações comportamentais destinadas à mitigação de riscos e à neutralização de ataques baseados na exploração de emoções humanas.

Importa ressaltar que as emoções são inerentes à natureza humana e, por esse motivo, representam um vetor de vulnerabilidade de difícil eliminação. Alterar padrões emocionais não constitui tarefa simples, tampouco passível de padronização, uma vez que cada indivíduo apresenta singularidades determinadas por seu histórico de vida e por experiências pregressas, sejam elas positivas ou negativas. Essa variabilidade individual constitui um desafio adicional para o desenvolvimento de estratégias preventivas universalmente eficazes.

6.0.1 Oportunidades para Trabalhos Futuros

- **Aperfeiçoamento do Framework com Análise Comportamental**: Uma área promissora para a evolução do framework seria a integração de análises comportamentais mais detalhadas, com ênfase nas reações psicológicas das vítimas. A exploração de como as emoções e os gatilhos psicológicos impactam as decisões pode ser incorporada ao framework para aprimorar as estratégias de defesa, personalizando as respostas de segurança conforme o perfil do alvo.

- **Validação Empírica do Framework em Diversos Cenários**: A aplicação do framework em uma gama mais ampla de contextos e ambientes, incluindo diferentes perfis de usuários e setores empresariais, pode fornecer dados empíricos robustos sobre sua eficácia. Isso permitiria ajustes específicos para torná-lo ainda mais eficaz em diferentes situações de risco, adaptando-se de forma dinâmica às novas táticas de fraude.

- **Desenvolvimento de Ferramentas Automatizadas Baseadas no Framework**: A criação de ferramentas automatizadas que implementem as estratégias do framework poderia proporcionar uma defesa ainda mais robusta. A combinação de inteligência artificial e aprendizado de máquina para detectar padrões fraudulentos em tempo real, integrados ao modelo de defesa proativa e reativa, representaria uma evolução significativa na proteção contra fraudes cibernéticas.

- **Integração de Educação Digital Contínua no Framework**: Embora a educação digital já tenha sido destacada como um fator fundamental, sua integração contínua dentro do próprio framework pode ser explorada de forma mais aprofundada. A implementação de programas de conscientização adaptados ao longo do tempo, com base nas lições aprendidas a partir de incidentes recentes, pode fortalecer a prevenção e melhorar a capacidade de resposta dos indivíduos e das organizações.

- **Análise da Efetividade das Estratégias de Defesa em Diversos Contextos Corporativos**: A aplicação do framework em diferentes tipos de organizações, com ênfase nas peculiaridades de segurança cibernética de cada setor, poderia proporcionar uma visão detalhada de como adaptar as defesas para diferentes ambientes corporativos. A análise das melhores práticas em segurança cibernética para pequenas, médias e grandes empresas pode enriquecer o framework, tornando-o ainda mais aplicável em diversos cenários organizacionais.

- **Exploração de Políticas Públicas para Prevenção de Fraudes Cibernéticas**: Uma possível linha de pesquisa futura envolve a criação de políticas públicas que integrem o framework proposto, visando à implementação de medidas preventivas mais amplas e à regulamentação do setor de segurança cibernética. O fortalecimento da legislação e a promoção de práticas de segurança cibernética por meio de políticas

governamentais poderiam facilitar a adesão do framework em maior escala, tanto a nível individual quanto organizacional.

As oportunidades delineadas para pesquisas futuras não apenas ampliam a aplicação do framework proposto, mas também fornecem soluções práticas e inovadoras para a mitigação de fraudes cibernéticas, potencializando a eficácia das respostas frente a ameaças cada vez mais sofisticadas. A contínua adaptação e refinamento desse modelo de defesa detêm um significativo potencial para oferecer respostas mais ágeis e assertivas, por meio de uma abordagem integrada que abarca dimensões preventivas, reativas e adaptativas. Essa abordagem holística visa enfrentar as fraudes digitais de maneira abrangente e dinâmica, proporcionando não apenas uma adaptação às novas táticas criminosas, mas também uma preparação contínua para cenários futuros, com ênfase na construção de uma resiliência mais robusta frente às ameaças emergentes.

Referências

ABIN, A. B. de I. *Contrainteligência*. 2020. Disponível em: ⟨https://www.gov.br/abin/pt-br/assuntos/inteligencia-e-contrainteligencia/CI⟩. Citado 2 vezes nas páginas 15 e 37.

ABRI, F.; ZHENG, J.; NAMIN, A. S.; JONES, K. S. Markov decision process for modeling social engineering attacks and finding optimal attack strategies. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 10, p. 109949–109968, 2022. ISSN 21693536. Citado na página 31.

ALMOUSA, M.; ANWAR, M. A url-based social semantic attacks detection with character-aware language model. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 11, p. 10654–10663, 2023. ISSN 21693536. Citado na página 34.

ALQARNI, Z.; ALGARNI, A.; XU, Y. Toward predicting susceptibility to phishing victimization on facebook. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2016. p. 419–426. ISBN 9781509026289. Citado na página 16.

ALTURKI, A.; ALSHWIHI, N.; ALGARNI, A. Factors influencing players' susceptibility to social engineering in social gaming networks. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 8, p. 97383–97391, 2020. ISSN 21693536. Citado na página 32.

ANSARI, M. F.; PANIGRAHI, A.; JAKKA, G.; PATI, A.; BHATTACHARYA, K. Prevention of phishing attacks using ai algorithm. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. ISBN 9781665478397. Citado na página 16.

ARIYO, O.; ZHENG, J. A study on security and privacy risks of self-disclosure on social networking sites during covid-19 pandemic. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. p. 2828–2832. ISBN 9781665480451. Citado na página 17.

ASCH, S. E. Studies in the principles of judgments and attitudes: Ii. determination of judgments by group and by ego standards. *The Journal of social psychology*, Taylor e Francis Group, Worcester, Mass, v. 12, n. 2, p. 433–465, 1940. ISSN 0022-4545. Citado na página 33.

ASIRI, S.; XIAO, Y.; ALZAHRANI, S.; LI, S.; LI, T. A survey of intelligent detection designs of html url phishing attacks. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 11, p. 6421–6443, 2023. ISSN 21693536. Citado na página 34.

AWAD, M.; ALLAM, A. E.; SALAMEH, K.; MAZROUEI, R. A. Phishing for legitimacy: The use of ssl certificates to ensnare internet users. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. p. 313–317. ISBN 9781665456005. Citado 2 vezes nas páginas 31 e 37.

BHATTACHARYA, M.; ROY, S.; CHATTOPADHYAY, S.; DAS, A. K.; JAMAL, S. S. Aspa-mosn: An efficient user authentication scheme for phishing attack detection in mobile online social networks. *IEEE Systems Journal*, Institute of Electrical and Electronics Engineers Inc., v. 17, p. 234–245, 3 2023. ISSN 19379234. Citado 2 vezes nas páginas 32 e 33.

BOURDIEU, P. Compreender. em bourdieu, p. (coord.) a miséria do mundo. 2ªed. *Petrópolis: Vozes, p. 693 – 732.*, 1998. Citado 2 vezes nas páginas 55 e 56.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Diário Oficial da República Federativa do Brasil*, Brasília, DF, 2018. ISSN 1677-7042. Disponível em: ⟨https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm⟩. Citado na página 17.

BURKETT, R. An alternative framework for agent recruitment: From mice to rascls. *Studies in Intelligence*, 2013. Citado 2 vezes nas páginas 21 e 38.

CLEAVE, M. V. What is counterintelligence. *Intelligencer: Journal of US Intelligence Studies*, v. 20, n. 2, p. 57–65, 2013. Citado na página 39.

DAVIS, N.; GRANT, E. S. Simulated phishing training exercises versus gamified phishing education games. In: . [S.l.]: Institute of Electrical and Electronics Engineers (IEEE), 2023. p. 1–8. ISBN 9781665456357. Citado na página 22.

EFTIMIE, S.; MOINESCU, R.; RACUCIU, C. Spear-phishing susceptibility stemming from personality traits. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 10, p. 73548–73561, 2022. ISSN 21693536. Citado na página 22.

FALKOV, Y. "tried and trusted patriots"for the cia: Latvian case study of the kgb operativnaia igra theory. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 1, p. 41–62, 2023. ISSN 0885-0607. Citado na página 37.

FESTINGER, L. Psychologist leon festinger dies; studied cognitive dissonance: Final edition. *The Washington post*, WP Company LLC d/b/a The Washington Post, Washington, D.C, 1989. ISSN 0190-8286. Citado na página 33.

FISCHER, B. B. Penkovsky, the spy who tried to destroy the world. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 1, p. 156–178, 2023. ISSN 0885-0607. Citado na página 37.

GENTRY, J. A. Demographic diversity in u.s. intelligence personnel: Is it functionally useful? *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 2, p. 564–596, 2023. ISSN 0885-0607. Citado na página 39.

GONG, X. Asymmetric information dissemination in double-layer networks helps explain the emergence of cooperation. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 11, p. 13202–13210, 2023. ISSN 21693536. Citado na página 22.

GRBIC, D. V.; DUJLOVIC, I. Social engineering with chatgpt. In: . IEEE, 2023. p. 1–5. ISBN 978-1-6654-7546-4. Disponível em: ⟨https://ieeexplore.ieee.org/document/10094141/⟩. Citado na página 22.

HANCOCK, B. Kevin mitnick finally gets a plea — and a sentence. *Computers e security*, Elsevier Ltd, OXFORD, v. 18, n. 3, p. 196–197, 1999. ISSN 0167-4048. Citado na página 34.

HIJJI, M.; ALAM, G. A multivocal literature review on growing social engineering based cyber-attacks/threats during the covid-19 pandemic: Challenges and prospective solutions. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 7152–7169, 2021. ISSN 21693536. Citado na página 17.

HOQUE, M. A.; FERDOUS, M. S.; KHAN, M.; TARKOMA, S. Real, forged or deep fake? enabling the ground truth on the internet. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 160471–160484, 2021. ISSN 21693536. Citado na página 16.

HORADAM, A. A generalized fibonacci sequence. *The American Mathematical Monthly*, Taylor & Francis, v. 68, n. 5, p. 455–459, 1961. Citado na página 39.

HOSSAIN, M. J.; RIFAT, R. H.; MUGDHO, M. H.; JAHAN, M.; RASEL, A. A.; RAHMAN, M. A. Cyber threats and scams in fintech organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in bangladesh. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. p. 190–195. ISBN 9781665473279. Citado 2 vezes nas páginas 18 e 22.

HSIEH, W.-B.; LEU, J.-S.; TAKADA, J.-I. Use chains to block dns attacks: A trusty blockchain-based domain name system. *Journal of Communications and Networks*, Institute of Electrical and Electronics Engineers (IEEE), v. 24, p. 347–356, 5 2022. ISSN 1229-2370. Citado na página 35.

HUANG H. TAN J., . L. L. Countermeasure techniques for deceptive phishing attacks. *International Conference on New Trends in Information and Service Science.*, 2009. Citado 2 vezes nas páginas 37 e 38.

HUGHES-WILSON, J. The secret state: A history of intelligence and espionage. *Pegasus Books, Ltd*, 2016. Citado 2 vezes nas páginas 38 e 43.

KHONJI, M.; IRAQI, Y.; JONES, A. *Phishing detection: A literature survey*. 2013. 2091-2121 p. Citado na página 31.

KIM, D.; PAN, Y.; PARK, J. H. A study on the digital forensic investigation method of clever malware in iot devices. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 8, p. 224487–224499, 2020. ISSN 21693536. Citado na página 17.

LEE, J.; LEE, Y.; LEE, D.; KWON, H.; SHIN, D. Classification of attack types and analysis of attack methods for profiling phishing mail attack groups. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 80866–80872, 2021. ISSN 21693536. Citado na página 17.

LEITAO, C. F. *Jornadas de Atualização em Informática 2021, Cap. 7. A entrevista como instrumento de pesquisa científica: planejamento, execução e análise*. [S.l.]: Sociedade Brasileira de Computação - SBC, Florianópolis/SC, 2021. ISBN 978-85-7669-824-1. Citado 10 vezes nas páginas 47, 48, 49, 50, 51, 52, 53, 54, 55 e 56.

LEITAO, C. F.; PRATES, R. O. *Jornadas de Atualização em Informática 2017, Cap. 2. A Aplicação de Métodos Qualitativos em Computação*. [S.l.]: Sociedade Brasileira de Computação - SBC, Porto Alegre/RS, 2017. ISBN 978-85-7669-374-1. Citado 8 vezes nas páginas 47, 48, 49, 50, 51, 52, 54 e 55.

LONG, J.; MITNICK, K. D. *No Tech Hacking*. [S.l.]: Syngress, 2011. ISBN 1597492159. Citado na página 35.

LONG, J.; MITNICK, K. D. *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Rockland, MA: Elsevier Science, 2011. ISBN 9780080558752. Citado na página 33.

MAMBINA, I. S.; NDIBWILE, J. D.; MICHAEL, K. F. Classifying swahili smishing attacks for mobile money users: A machine-learning approach. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 10, p. 83061–83074, 2022. ISSN 21693536. Citado 2 vezes nas páginas 24 e 32.

MARCHAND-NINO, W. R.; FONSECA, B. P. G. Social engineering for diagnostic the information security culture. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2019. v. 2019-November. ISBN 9781728108834. Citado na página 34.

MARTíNEZ, G. H. La sociedad como artefacto: Sistemas sociotécnicos, sociotecnologías y sociotécnicas.v. 14, n. 40, p. 267-295. *CTS: Revista iberoamericana de ciencia, tecnología y sociedad*, 2019. Citado na página 16.

MIFTARI, A.; LUMA-OSMANI, S.; IDRIZI, F. Analysis of cybercriminals and where they fall on the spectrum of crime. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. p. 287–291. ISBN 9781665490580. Citado na página 35.

MILGRAM, S. Behavioral study of obedience. *Journal of Abnormal and Social Psychology*, v. 4, n. 2, p. 201–213, 7 1963. This article describes a procedure for the study of destructive obedience in the laboratory. It consists of ordering a naive S to administer increasingly more severe punishment to a victim in the context of a learning experiment. Citado na página 34.

MURPHY, W. T. Soviet espionage in france during the cold war: An overview. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 2, p. 466–491, 2023. ISSN 0885-0607. Citado 2 vezes nas páginas 37 e 39.

NICHOLLS, J.; KUPPA, A.; LE-KHAC, N. A. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 9, p. 163965–163986, 2021. ISSN 21693536. Citado na página 31.

ORBACH, D. Former nazis in german intelligence politics: The exposure of moles and reckless decision making, 1959-1962. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 1, p. 20–40, 2023. ISSN 0885-0607. Citado na página 35.

OVEH, R. O.; AZIKEN, G. O. Mitigating social engineering attack: A focus on the weak human link. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. ISBN 9781509064229. Citado na página 15.

PAICU, S. C. Data-driven security and democratic intelligence: Key role of critical engagement by academia. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 3, p. 711–728, 2023. ISSN 0885-0607. Citado 2 vezes nas páginas 14 e 37.

PLEKHANOV, A. A. The activities of the russian joint stock company ≪manufacturing company singer≫ in siberia on the eve and during the first world war: espionage or spy mania? *Omsk Scientific Bulletin: Series "Society. History. Modernity"*, Omsk State Technical University, Federal State Budgetary Educational Institution of Higher Education, v. 8, n. 2, p. 30–36, 2023. ISSN 2542-0488. Citado na página 38.

QIN, J.; CHEN, Y.; FU, W.; KANG, Y.; PERC, M. Neighborhood diversity promotes cooperation in social dilemmas. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 6, p. 5003–5009, 11 2017. ISSN 21693536. Citado 2 vezes nas páginas 17 e 31.

RAJA, A. S.; MADHUBALA, R.; RAJESH, N.; SHAHEETHA, L.; ARULKUMAR, N. Survey on malicious url detection techniques. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. p. 778–781. ISBN 9781665483285. Citado na página 17.

RUEDA, G. C. Entre piratas y fantasmas: ciberespacio y contracultural. *Iconos : publicación de FLACSO-Ecuador*, n. 8, p. 20–26, 1999. ISSN 1390-1249. Citado na página 34.

SANCHEZ-PANIAGUA, M.; FERNANDEZ, E. F. Phishing url detection: A real-case scenario through login urls. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 10, p. 42949–42960, 2022. ISSN 21693536. Citado na página 22.

SEIDMAN, I. Interviewing as qualitative research: a guide for researchers in education and social sciences. *New York, Teachers College Press*, 1998. Citado na página 48.

SHARMEEN, S.; AHMED, Y. A.; HUDA, S.; KOCER, B. S.; HASSAN, M. M. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 8, p. 24522–24534, 2020. ISSN 21693536. Citado na página 32.

SHPIRO, S. Blinding the bear: Israeli double agents and russian intelligence. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 1, p. 1–19, 2023. ISSN 0885-0607. Citado 4 vezes nas páginas 37, 40, 41 e 42.

SINHA, S. The fibonacci numbers and its amazing applications in nature. *International Journal of Engineering Science Invention*, v. 6, n. 9, p. 7–14, 2017. Citado na página 39.

SINKó, G.; BESENYő, J. Comparison of the secret service of al-shabaab, the amniyat, and the national intelligence and security agency (somalia). *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 1, p. 220–240, 2023. ISSN 0885-0607. Citado na página 33.

SIRIGIRI, M.; SIRIGIRI, D.; AISHWARYA, R.; YOGITHA, R. Malware detection and analysis using machine learning. In: . IEEE, 2023. p. 1074–1081. ISBN 978-1-6654-6408-6. Disponível em: ⟨https://ieeexplore.ieee.org/document/10083809/⟩. Citado na página 15.

THEGUARDIAN. *Target data breach: what you need to know about identity theft. Available in:*. 2013. ⟨https://www.theguardian.com/money/us-money-log/2013/dec/19/target-identity-theft-credit-card-breach⟩. Access at: 10/05/2023. Citado 2 vezes nas páginas 35 e 36.

THEGUARDIAN. *Twitter hack: accounts of prominent figures, including Biden, Musk, Obama, Gates and Kanye compromised. The Guardian, 2020. Available in:.* 2013. ⟨www.theguardian.com/technology/2020/jul/15/twitter-elon-musk-joe-biden-hacked-bitcoin.⟩ Access at: 10/05/2023. Citado 2 vezes nas páginas 35 e 36.

THEGUARDIAN. *Yahoo hack: 1bn accounts compromised by biggest data breach in history. Available in:.* 2016. ⟨https://www.theguardian.com/money/us-money-log/2013/dec/19/target-identity-theft-credit-card-breach⟩. Access at: 10/05/2023. Citado 2 vezes nas páginas 35 e 36.

THEGUARDIAN. *Equifax: credit firm was breached before massive May hack. Available in:.* 2017. ⟨https://www.theguardian.com/technology/2017/sep/19/equifax-credit-firm-march-breach-massive-may-hack-customers⟩. Access at: 10/05/2023. Citado 2 vezes nas páginas 35 e 36.

TROMBLAY, D. E. Taking the fight abroad: The fbi's legal attachés and chinese intelligence. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 1, p. 260–270, 2023. ISSN 0885-0607. Citado na página 32.

TUINIER, P.; ZAALBERG, T. B.; RIETJENS, S. The social ties that bind: Unraveling the role of trust in international intelligence cooperation. *International journal of intelligence and counterintelligence*, Routledge, Philadelphia, v. 36, n. 2, p. 386–422, 2023. ISSN 0885-0607. Citado 2 vezes nas páginas 38 e 41.

TYAGI, S.; TYAGI, D. R. K.; DUTTA, D. P. K.; DUBEY, D. P. Next generation phishing detection and prevention system using machine learning. In: . IEEE, 2023. p. 1–6. ISBN 978-1-6654-7275-3. Disponível em: ⟨https://ieeexplore.ieee.org/document/10085529/⟩. Citado na página 15.

TZU, S.; PIN, S. *A arte da guerra*. [S.l.]: WWF Martins Fontes, 2015. Citado na página 34.

UPLENCHWAR, S.; SAWANT, V.; SURVE, P.; DESHPANDE, S.; KELKAR, S. Phishing attack detection on text messages using machine learning techniques. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. ISBN 9781665498975. Citado na página 22.

WANG, Z.; SUN, L.; ZHU, H. Defining social engineering in cybersecurity. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 8, p. 85094–85115, 2020. ISSN 21693536. Citado 2 vezes nas páginas 32 e 38.

WANG, Z.; ZHU, H.; SUN, L. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, v. 9, p. 11895–11910, 2021. Citado 14 vezes nas páginas 10, 14, 17, 22, 23, 28, 29, 30, 32, 35, 42, 43, 44 e 67.

WILLIAMS, K.; BLEIMAN, R.; REGE, A. Educating educators on social engineering experiences developing and implementing a social engineering workshop for all education levels. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2022. p. 188–194. ISBN 9781665484299. Citado na página 17.

ZAMBRANO, P.; TORRES, J.; TELLO-OQUENDO, L.; JACOME, R.; BENALCAZAR, M. E.; ANDRADE, R.; FUERTES, W. Technical mapping of the grooming anatomy using machine learning paradigms: An information security approach. *IEEE Access*, Institute of

Electrical and Electronics Engineers Inc., v. 7, p. 142129–142146, 2019. ISSN 21693536. Citado na página 31.

ZHENG, K.; WU, T.; WANG, X.; WU, B.; WU, C. A session and dialogue-based social engineering framework. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 7, p. 67781–67794, 2019. ISSN 21693536. Citado 2 vezes nas páginas 14 e 15.

ZHENG, K.; WU, T.; WANG, X.; WU, B.; WU, C. A session and dialogue-based social engineering framework. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 7, p. 67781–67794, 2019. ISSN 21693536. Citado na página 34.

ZIENI, R.; MASSARI, L.; CALZAROSSA, M. C. Phishing or not phishing? a survey on the detection of phishing websites. *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., v. 11, p. 18499–18519, 2023. ISSN 21693536. Citado na página 31.