UNIVERSIDADE FEDERAL DO CEARÁ

CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

MARILENE SANTOS DUARTE

ENGENHARIA SOCIAL: UM ESTUDO SOBRE O NÍVEL DE CONHECIMENTO E SUSCETIBILIDADE EM DIFERENTES FAIXAS ETÁRIAS

ITAPAJÉ

2025

MARILENE SANTOS DUARTE

ENGENHARIA SOCIAL: UM ESTUDO SOBRE O NÍVEL DE CONHECIMENTO E SUSCETIBILIDADE EM DIFERENTES FAIXAS ETÁRIAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Segurança da Informação.

Orientador: Prof. Dr. João Henrique Gonçalves Medeiros Corrêa

ITAPAJÉ

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

D873e Duarte, Marilene Santos.
Engenharia Social: Um estudo sobre o nível de conhecimento e suscetibilidade em diferentes faixas etárias / Marilene Santos Duarte. – 2025.
66 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Itapajé, Curso de Segurança da Informação, Fortaleza, 2025.
Orientação: Prof. Dr. João Henrique Gonçalves Medeiros Corrêa..

1. Segurança da Informação. 2. Engenharia Social. 3. Phishing. 4. Pretexting. 5. Baiting. I. Título.

CDD 005.8

MARILENE SANTOS DUARTE

ENGENHARIA SOCIAL: UM ESTUDO SOBRE O NÍVEL DE CONHECIMENTO E SUSCETIBILIDADE EM DIFERENTES FAIXAS ETÁRIAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Segurança da Informação do da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de tecnólogo em Segurança da Informação.

Aprovada em: 25 de Fevereiro de 2025

BANCA EXAMINADORA

Prof. Dr. João Henrique Gonçalves Medeiros Corrêa
(Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Solon Alves Peixoto
Univerisdade Federal do Ceará (UFC)

Prof. Dr. Tarek Sayjari
Univerisdade Federal do Ceará (UFC)

À meu pai, que, com suas mãos calejadas e coração forte, enfrentou os maiores desafios sob o sol e o suor, sempre pensando no meu futuro. Sua coragem, dedicação e amor inabaláveis foram a força que me impulsionaram a seguir em frente, mesmo nos momentos mais difíceis. Tudo o que sou e tudo o que conquistei, devo a ele.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão a todas as pessoas que me ajudaram a concluir este trabalho. Primeiramente, agradeço a Deus, cuja graça e força me sustentaram em cada etapa desta caminhada, dando-me sabedoria e perseverança para superar os desafios.

Com todo o meu coração, agradeço também aos meus pais, Marcos e Josiana, que foram e sempre serão o principal motivo de todo o meu esforço. Por eles, sou imensamente grata, pois foram eles que, com amor incondicional, dedicação e apoio inabalável, me criaram e me guiaram até aqui. Tudo o que conquistei até hoje e tudo que sou é reflexo dos valores que me ensinaram e do carinho com que sempre me acolheram.

Expresso minha mais profunda gratidão ao meu orientador, Professor Dr. João Henrique Gonçalves Medeiros Corrêa, por sua orientação atenta, paciência e dedicação ao longo de todo o desenvolvimento deste trabalho. Seu vasto conhecimento, suas valiosas orientações e seu compromisso incansável foram fundamentais para a realização desta monografia. Seu apoio e feedback precisos não apenas enriqueceram este estudo, mas também contribuíram significativamente para o meu crescimento acadêmico e profissional.

Sou igualmente grata à Universidade Federal do Ceará (UFC) e aos professores do curso de Segurança da Informação por todo o conhecimento transmitido ao longo da minha jornada acadêmica. Em especial, expresso minha profunda gratidão ao Prof. Aminadabe Barbosa de Sousa, cuja dedicação e apoio inestimáveis foram fundamentais para que eu continuasse na faculdade. Seu acolhimento e incentivo desde o início da minha trajetória fizeram toda a diferença. Também sou grata ao Prof. Germano Fenner, cuja orientação teve um papel essencial no meu desenvolvimento profissional. A todos que contribuíram para minha formação, meu sincero muito obrigado.

Com imensa gratidão, agradeço à minha tia Regina, que, com todo carinho, me ajudou da melhor forma possível e, mesmo à distância, fez com que eu sentisse o verdadeiro aconchego de uma família. Seu apoio e afeto foram inestimáveis ao longo dessa caminhada. Estendo também minha gratidão às minhas irmãs, meus tios Edi, Roberto, César, minhas tias, Elisabeth, Ana, Marcilene, Roseli e Claúdia que nos momentos em que precisei, com carinho me estenderam a mão e às minhas queridas avó e bisavó, que, desde o início, estiveram ao meu lado, oferecendo amor, incentivo e força para que eu seguisse em frente.

Meu sincero agradecimento a Seu Mardonio e Dona Lucilene, que agora considero parte da minha família. Seu carinho, apoio e imensa gentileza fizeram toda a diferença desde

quando os conheci. Acolheram-me com generosidade e afeto. Sou profundamente grata por todo o cuidado e pelas palavras de incentivo que me ofereceram.

Agradeço de todo o coração a Ruan, que, com seu amor e cuidado, me salvou inúmeras vezes. Nos momentos em que me faltavam forças e a dor parecia impossível de expressar em palavras, foi ele quem me trouxe um pouco de luz, acolhendo-me e me fazendo sorrir quando eu mais precisava. Sua presença foi um refúgio, seu apoio, uma força, e seu carinho, um alívio para os dias mais difíceis. Sou imensamente grata por tê-lo ao meu lado.

Agradeço aos meus amigos queridos, Leyd, Isa, Thais, Alana, Kawan, Cássio, Lincoln, Luís, Ana Júlia, Brena, Alysson, e Edwiges, que, com sua amizade, tornaram esses anos muito mais leves e especiais. Estiveram ao meu lado não apenas nos momentos de alegria, mas também nas dificuldades, oferecendo apoio, risadas e companhia nos dias mais desafiadores. Cada conversa, cada gesto de carinho e cada lembrança compartilhada estarão sempre guardadas em meu coração. sou imensamente grata por cada um de vocês.

Gostaria de agradecer também aos meus amigos, quase colegas de casa, Pablo, Kurt e Jefter, por generosamente disponibilizarem seu espaço, companhia e até mesmo sua internet, permitindo que eu pudesse concluir a escrita deste trabalho.

Aos meus amigos que não foram diretamente citados, muitos deles que convivi em sala de aula, conhecidos e agregados, pessoas que, embora não estivessem presentes no meu dia a dia, ofereceram apoio, conversas breves, mas profundas, ou uma ajuda inesperada. Sou muito grata pois cada interação foi valiosa e contribuiu para que eu mantivesse a fé em minha jornada.

Por fim, agradeço sinceramente a todas as pessoas que responderam à minha pesquisa, contribuindo de maneira essencial para a conclusão deste trabalho. Sem a colaboração de cada um de vocês, não seria possível reunir as informações necessárias para embasar e enriquecer este estudo. Agradeço pelo tempo dedicado e pela disposição em compartilhar seus conhecimentos e opiniões. Cada resposta foi de grande importância e fez toda a diferença no resultado final.

"A vida é uma peça de teatro que não permite ensaios. Por isso, cante, chore, dance, ria e viva intensamente, antes que a cortina se feche e a peça termine sem aplausos."

(Charles Chaplin - 1972)

RESUMO

A engenharia social é uma técnica de manipulação psicológica utilizada para enganar indivíduos e obter informações sigilosas, representando uma ameaça crescente à segurança da informação. Este estudo analisou o nível de conhecimento e a suscetibilidade da população de Itapajé a ataques desse tipo, considerando diferentes faixas etárias e níveis de escolaridade. Para isso, foi realizada uma pesquisa com 124 participantes, que responderam a um questionário online abordando temas como *phishing*, *pretexting* e baiting, além de suas práticas de segurança digital. Os resultados indicam que, embora muitos participantes tenham ouvido falar sobre engenharia social, uma parcela significativa não sabe identificar ataques ou desconhece os riscos envolvidos. Além disso, 74,2% nunca receberam treinamento sobre o tema, e grande parte desconhece a Lei Geral de Proteção de Dados (LGPD), o que pode comprometer sua segurança digital. Observou-se também que ataques via e-mail e redes sociais são os mais reconhecidos pelos participantes como potenciais ameaças. Diante desses achados, conclui-se que há uma necessidade urgente de campanhas educativas e treinamentos voltados à conscientização sobre engenharia social, especialmente entre os grupos mais vulneráveis. A implementação de programas de educação digital contínuos, tanto em instituições de ensino quanto em empresas, pode reduzir os riscos associados a esses ataques. Sugere-se que estudos futuros investiguem a eficácia de diferentes métodos de conscientização e o impacto da evolução tecnológica na segurança digital dos usuários.

Palavras-chave: engenharia social; segurança da informação; phishing; pretexting; baiting; suscetibilidade; conscientização; cibersegurança; LGPD; educação digital.

ABSTRACT

Social engineering is a psychological manipulation technique used to deceive individuals and obtain confidential information, posing a growing threat to information security. This study analyzed the level of knowledge and susceptibility of the population of Itapajé to such attacks, considering different age groups and educational levels. To achieve this, a survey was conducted with 124 participants who responded to an online questionnaire addressing topics such as phishing, pretexting, and baiting, as well as their digital security practices. The results indicate that although many participants have heard of social engineering, a significant portion cannot identify attacks or are unaware of the associated risks. Additionally, 74.2% have never received training on the topic, and a large proportion are unfamiliar with the General Data Protection Law (LGPD), which may compromise their digital security. It was also observed that email and social media attacks are the most recognized threats among participants. Given these findings, there is an urgent need for educational campaigns and training programs focused on raising awareness about social engineering, especially among the most vulnerable groups. The implementation of continuous digital education programs, both in educational institutions and in companies, can help mitigate the risks associated with these attacks. Future studies are suggested to explore the effectiveness of different awareness methods and the impact of technological advancements on digital security.

Keywords: social engineering; information security; phishing; pretexting; baiting; susceptibility; awareness; cybersecurity; LGPD (General Data Protection Law); digital education.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Com o avanço da tecnologia e a crescente digitalização da sociedade, a segurança da informação tornou-se uma preocupação essencial para indivíduos e organizações. Porém, mesmo que os métodos de segurança também tenham evoluído, os ataques cibernéticos se aprimoram cada vez mais. Entre as diversas ameaças existentes, a engenharia social se destaca por explorar a confiança e o comportamento humano para obter informações sigilosas. Diferente de ataques baseados exclusivamente em brechas tecnológicas, essa prática manipula as pessoas para que, muitas vezes sem perceber, forneçam dados importantes ou realizem ações que comprometem sua própria segurança.

Segundo o blog Claranet (2024) os seres humanos são os pontos de entrada de segurança cibernética mais vulneráveis. O blog cita o relatório *Human Hacking* publicado por SlashNext (2024) no qual apresenta dados que mostram que os ataques de *phishing* aumentaram 51% em 2020 e 59% dos ataques de engenharia social foram roubo de credenciais. O autor do relatório segue dizendo que os casos de ataques de engenharia social se tornam populares e perigosos por geralmente serem mais fáceis do que encontrar uma vulnerabilidade de rede ou *software*. Os *hackers* costumam usar essas táticas como uma primeira etapa em uma campanha maior para se infiltrar em um sistema ou rede e roubar dados confidenciais.

O *phishing* é um golpe que consiste no envio de mensagens fraudulentas para enganar a vítima e induzi-la a revelar informações sensíveis, como senhas, dados bancários ou credenciais de acesso. Essas mensagens costumam se passar por comunicações legítimas de empresas, bancos ou serviços *online*, utilizando linguagem persuasiva e elementos visuais muito semelhantes aos originais para ganhar a confiança do destinatário. O *phishing* pode ocorrer por e-mail, mensagens de texto, redes sociais ou até mesmo ligações telefônicas, explorando a desatenção e a confiança das pessoas para atingir seu objetivo.

O blog ThreatLabz (2024) divulgou um relatório indicando um aumento de 58% nos ataques de *phishing* no ano de 2023, em comparação com o ano anterior. A publicação deu destaque as táticas avançadas, como *vishing* e *deepfake phishing* que crescem à medida que criminosos utilizam ferramentas de IA generativa.

O impacto negativo dos ataques de engenharia social podem ser prejudiciais tanto para os indivíduos separadamente, quanto para organizações. Muitas pessoas não têm consciência do valor de seus dados pessoais e, por esse motivo, compartilham suas informações em diversos sites e plataformas sem receio das possíveis consequências. Essa falta de cuidado, junto a

outras falhas de segurança digital, é justamente o que permite que a engenharia social prospere BUGHUNT (2022).

Dessa forma, há a necessidade de se aprofundar nessa temática, devido o grande aumento de ataques de engenharia social, que podem ser de vários tipos, *phishing*, *pretexting*, *baiting*, *vishing*, *deepfake phishing*, entre outros que exploram as vulnerabilidades técnicas e psicológicas das vítimas. Diante do aumento desses ataques, é fundamental entender como diferentes grupos etários percebem e reagem a esse tipo de ameaça. Algumas faixas etárias podem ser mais vulneráveis devido à falta de experiência com o meio digital, enquanto outras podem superestimar sua capacidade de identificar golpes. Este estudo busca investigar o nível de conhecimento sobre engenharia social em diferentes idades, analisando os fatores que contribuem para a suscetibilidade aos ataques e apontando estratégias para minimizar os riscos associados.

Dado o exposto, o restante deste trabalho está organizado do seguinte modo na Seção 2 serão apresentados conceitos sobre segurança da informação, engenharia social, e os ataques, *phishing*, *pretexting* e *baiting*. Na seção 3 será apresentada a metodologia utilizada para o desenvolvimento do trabalho. Na seção 4 os resultados serão analisados e por fim na seção 5 serão apresentadas as conclusões do trabalho e as sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Nesta seção serão apresentados conceitos importantes para o desenvolvimento do trabalho, sendo eles, segurança da informação, e ataques de engenharia social, mais especificamente os de *Phishing*, *Pretexting* e *Baiting.*

2.1 Segurança da Informação

A Informação nada mais é do que um ativo, e assim como qualquer outro ativo importante, é crucial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente de negócios cada vez mais interconectado. Este aumento de interconectividade resultou na maior exposição da informação a um crescente número de pessoas e uma grande variedade de ameaças e vulnerabilidades ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2005)

A segurança da informação por sua vez, se trata da proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar seus riscos e maximizar o retorno sobre os investimentos e as oportunidades de negócio ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2005). Segundo o artigo CASTRO e SOUSA (2010) a inexistência da adoção de um modelo de boas práticas de segurança da informação pode expor as empresas a um desastre de continuidade de negócios.

A segurança da informação pode ser entendida também como a proteção que existe sobre as informações de uma empresa ou pessoa, aplicando tanto para as informações corporativas quanto para as pessoais. E essa segurança pode ser afetada por fatores comportamentais de quem utiliza da informação, isto pelo ambiente ou pela infraestrutura que a cerca, pessoas com intenções maliciosas, com finalidade de obter, furtar ou destruir tal informação Sêmola (2006).

A norma NBR ISO/IEC (2005), por sua vez, define segurança da informação como sendo a "preservação da confidencialidade, da integridade e da disponibilidade da informação". Nesse contexto, confidencialidade pode ser definida como a garantia de que as informações serão acessadas apenas pelas pessoas que tem autorização para acessá-las, integridade é a garantia de que as informações são corretas e completas e disponibilidade é a garantia de que as informações estarão disponíveis para serem acessadas pelas pessoas que tem autorização para vê-las quando forem necessárias.

Os três pilares norteadores da segurança da informação expostos na Figura 1, unidos,

buscam enfrentar os desafios de segurança e evitar consequências negativas, principalmente em empresas. Além destes três pilares, pode-se mencionar também alguns aspectos complementares para viabilizar a garantia da segurança da informação, segundo Lyra *et al.* (2008) eles são:

a) **Autenticação:** "Garantir que um usuário é de fato quem alega ser".
b) **Não repúdio:** "Capacidade do sistema de provar que um usuário executou uma determinada ação".
c) **Legalidade:** "Garantir que o sistema esteja aderente à legislação".
d) **Privacidade:** "Capacidade de um sistema de manter anônimo um usuário, impossibilitando o relacionamento entre o usuário e suas ações".
e) **Auditoria:** "Capacidade do sistema de auditar tudo o que foi realizado pelos usuários, detectando fraudes ou tentativas de ataque"

Figura 1 – Os três pilares da segurança da informação

Fonte: (KAVLAC, 2023).

Para que a segurança da informação seja efetivamente alcançada, é fundamental adotar um conjunto estruturado de práticas e atividades que garantam a proteção dos ativos organizacionais. Isso inclui a definição e implementação de processos bem estabelecidos, a elaboração de políticas de segurança da informação (PSI) que orientem a conduta dos usuários, o desenvolvimento de procedimentos específicos para o tratamento de dados sensíveis, o treinamento contínuo de profissionais para estarem preparados contra ameaças emergentes, e o uso de ferramentas avançadas de monitoramento e controle Lyra (2015).

A necessidade dessas medidas se justifica pelo crescente número de ataques cibernéticos e pela sofisticação das técnicas utilizadas por agentes mal-intencionados, sendo a engenharia social um dos vetores mais preocupantes. A engenharia social explora a vulnerabilidade humana para obter acesso a informações confidenciais, muitas vezes manipulando indivíduos a fornecerem credenciais, clicarem em *links* maliciosos ou executarem ações prejudiciais à segurança da organização. Dessa forma, não basta investir apenas em soluções tecnológicas; é imprescindível estabelecer uma cultura organizacional voltada para a conscientização e a prevenção de ataques que exploram falhas humanas.

2.2 Engenharia social

Segundo Eiras (2004) ENGENHARIA SOCIAL é o termo utilizado para definir a área que estuda as técnicas e práticas utilizadas para a obtenção de informações importantes ou sigilosas de uma organização, através das pessoas, funcionários e colaboradores de uma corporação ou de pessoas em uma sociedade. Essas informações podem ser obtidas por ingenuidade ou confiança. Conforme é citado por Coelho *et al.* (2013) examinado por Peixoto (2004) pode-se considerar o significado de engenharia social como sendo a junção dos significados de duas partes, sendo elas:

a) **Engenharia**: Refere-se à aplicação de conhecimento científico, experiência prática e habilidades específicas na criação de estruturas, dispositivos e processos destinados a transformar recursos naturais em formas que atendam às necessidades humanas.
b) **Sociedade**: Refere-se à sociedade. Em outras palavras, refere-se a questões sociais e coisas que interessam à sociedade em geral.

Engenharia Social por sua vez, refere-se à habilidade de influenciar indivíduos com o propósito de superar medidas de segurança. Essa prática fundamenta-se na aplicação de técnicas persuasivas e na exploração da falta de conhecimento ou da ingenuidade dos usuários de 19 um sistema, GOMES (2023).

Ainda dito por GOMES (2023), analisado por Hadnagy e Maxwell (2009) Engenharia Social no contexto das Ciências Políticas consiste em técnicas e artes dirigidas a manipulação das pessoas para conseguir que elas realizem atos que normalmente não fariam, em grande escala, ou divulguem voluntariamente informações pessoais, ou da empresa onde prestam serviço; explorando a vulnerabilidade humana.

Existem no mundo inúmeras formas de ataques, esses ataques exploram a inge-

nuidade e fragilidade das pessoas, estes ataques podem ter dois enfoques diferentes: o físico, como local de trabalho, lixo, telefones; e o psicológico, como persuasão, criando confiança, ou simplesmente sendo gentil. Coelho *et al.* (2013)

Coelho *et al* também cita Filho (2004) mostrando os traços comportamentais, que tornam o ser humano susceptível a ataques como sendo:

a) **Persuasão**: Compreende quase uma arte a capacidade de induzir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas têm características comportamentais que as tornam vulneráveis à manipulação;
b) **Vontade de ser útil**: O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário;
c) **Busca por novas amizades**: O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações;
d) **Propagação de responsabilidade**: Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

O engenheiro social pode ser indicado como uma pessoa que utiliza um conjunto de técnicas para a manipulação da confiança de outras pessoas para ter acesso às informações privadas. Também é possível, por meio das poucas informações que ele tem acesso, montar um plano sobre o alvo e com informações que ele acha irrelevantes, dando ao engenheiro a possibilidade de prejudicá-lo empresarialmente, social, financeira ou psicologicamente. Mitnick e Simon (2004)

Na maioria das vezes o engenheiro social é um tipo de pessoa agradável, educada, simpática e carismática. Mas, sobretudo, criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente. Até, mesmo, pessoas sem conhecimento antecipado desta denominação, já cometeram algum ato de engenharia social involuntariamente. Peixoto (2004)

Segundo Zager (2002) há quatro tipos de engenheiros sociais e cada um deles é caracterizado por determinado objetivo, sendo:

a) **Casual:** Composto com um grupo grande, motivado ao ataque por curiosidade e o desafio de invadir sistemas;
b) **Político:** tomam ação por uma causa, utilizando suas habilidades com o intuito de divulgar esta causa ou prejudicar entes que representam o oposto de sua causa;
c) **Criminoso:** elaborado por profissionais no crime;
d) **Interno:** este é caracterizado por serem funcionários ou terceiros de uma organização, são

os mais perigosos devido ao seu acesso padrão a informações da empresa.

Os ataques de engenharia social vem se tornando comuns já há muito tempo por conta da crescente evolução tecnológica e podem ser utilizados por qualquer pessoa que tenha interesse em suas informações AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (2021). Segundo LaFrance (2004) alguns dos principais objetivos dos engenheiros sociais com esses ataques são:

a) **Lucro financeiro:** motivo mais almejado pelo atacante;
b) **Interesse próprio**: para fins exploratórios sem más intenções, porém podendo provocar danos;
c) **Pelo desafio:** o invasor visa testar suas capacidades ou provar algo, sem más intenções;
d) **Vantagem competitiva:** obter informações para ganhar vantagem competitiva;
e) **Pressão:** o próprio engenheiro social se sente pressionado a ponto de tentar exibir suas habilidades para chamar a atenção de algum grupo com o intuito de ser chamado para participar do mesmo, ou também para pressão de manter sua reputação;
f) **Mitigar danos:** objetiva em ajudar as pessoas ou organizações, com o intuito de corrigir suas vulnerabilidades;
g) **Política:** o atacante atua para dar vantagem a uma causa.

Em Pereira *et al.* (2022) é falado que nos últimos tempos, os atacantes têm tido muito sucesso ao executar este tipo de ação, o que acarretou o aumento contínuo deste tipo de ataque. A utilização de equipamentos eletrônicos e redes sociais, acompanhados do mau uso e falta de conhecimento, por parte das vítimas, agregam para o sucesso do engenheiro social. Em virtude disto, as empresas devem dar devida atenção ao fator humano relacionado a segurança da informação, assim tendo funcionários bem treinados, resultando em uma empresa mais segura e consciente.

Pereira *et al.* (2022) também acrescenta que os ataques de engenharia social vêm ganhando espaço devido às dificuldades de mitigar este tipo de crime, e analisado por Alves (2010) estes ataques são divididos em dois grupos, direto e indireto. Os ataques diretos se referem quando há contato direto com a vítima, sendo por ligação ou pessoalmente. Neste grupo é necessário que o engenheiro social realize uma espécie de planejamento de como executar o ataque, pois o ataque de forma direta exige mais contato com o alvo, onde o menor dos erros pode comprometer o objetivo.

Por sua vez os ataques indiretos são caracterizados por utilizarem outros meios para chegar até a vítima e concluir seu objetivo. Isto é feito por meio de *softwares* ou ferramentas,

por exemplo, vírus, sites falsos, cavalos de troia ou por e-mails falsos (*phishing*). Dessa forma, através desses meios o atacante pode obter as informações que deseja.

Quando o engenheiro social utiliza o ataque a partir do grupo indireto, ele fica de certa forma mais seguro, uma vez que não há contato direto com a vítima e pode ser distribuído pela Internet de forma que atinja não só um, mas vários alvos. Segundo Gaspar (2015) este método é bastante utilizado pelos engenheiros sociais, onde primeiro criam os sites e depois utilizam as redes sociais para fazerem a divulgação dos mesmos.

Figura 2 – Estrutura do modelo de ataque de engenharia social

Fonte: (GASPAR, 2015)

A estrutura do ataque de engenharia social definida por Oosterloo (2008) é distribuída em quatro fases, sendo elas: Preparação, Manipulação, Exploração e Execução. Esta estrutura está ilustrada conforme a Figura 2.

Para compreender melhor como funcionam as fases do ataque de engenharia social Gaspar (2015) explica os termos para cada fase como:

a) **Preparação:** Se trata do pré-envolvimento do alvo, mais conhecido como *footprint*. Nesta fase é necessário recolher o máximo de informações possíveis sobre o alvo, como: negócio da organização, nome de funcionários, suas funções, telefones, e-mails e processos internos. Também, quais atributos (físicos) para seguir para a próxima fase.
b) **Manipulação:** O engenheiro social utiliza suas técnicas e meios para conquistar a confiança do alvo e criar um ambiente credível. A manipulação pode ser de várias formas, como fisicamente, interação direta, ou por meios de comunicação indireta, sendo por telefones ou e-mails, tudo com o intuito de reunir e organizar informações.
c) **Exploração:** Após a confiança e influência que foram conquistadas na fase anterior,

essas são utilizadas para adquirir informações mais afundo sobre o alvo, como nome dos servidores, aplicações, IPs, manuais, entre outras.

d) **Execução:** Nesta fase é realizado o ataque a partir de todas as informações obtidas nas fases anteriores. Definem-se as ações que devem ser tomadas para chegar ao objetivo final. O engenheiro social irá utilizar das suas habilidades técnicas, que demonstram sua perícia.

O engenheiro social, para atingir seus objetivos, busca se aproximar de sua vítima, ganhando sua confiança e explorando suas vulnerabilidades. Nesse processo, são utilizados diversos fatores sociais, como vaidade, curiosidade, persuasão e excesso de autoconfiança. Além disso, os engenheiros sociais empregam diferentes técnicas para alcançar suas metas, como Fonseca (2017):

a) **Análise do lixo:** que se trata dos objetos que foram descartados pelo alvo, adquirindo informações e até rotinas, que podem ser utilizados pelos engenheiros. O lixo descartado por pessoas físicas ou jurídicas muitas vezes é descartado de forma errada e se torna uma das fontes mais ricas de informações para os engenheiros sociais;

b) ***phishing***: O mais utilizado, também conhecido como pesca onde os atacantes enviam e-mails, normalmente se passando por bancos, órgãos públicos ou uma notícia que esteja na moda e que atraia a atenção do alvo, com objetivo de obter informações privilegiadas como nomes de usuários, senhas, dados sobre o cartão de crédito, entre outros;

c) **Redes sociais:** As informações colocadas nas redes sociais podem ser usadas pelos engenheiros sociais para entrar em contato com familiares e amigos, se tornando uma mina de ouro para o atacante;

d) ***Internet relay chat (IRC)***: O Internet relay chat (IRC) é um protocolo de comunicação pela Internet utilizado, resumidamente, como chat ou bate-papo. As vítimas são manipuladas durante a conversa, sendo incentivadas a clicar em um link ou foto, executando algum programa malicioso;

e) **Telefone**: O método de chamadas em cadeia é utilizado quando o objetivo é obter informações mais detalhadas sobre uma empresa ou indivíduo. Primeiramente, realiza-se uma ligação para coletar dados pessoais ou empresariais, frequentemente se passando por uma empresa ou patrocinador. Em seguida, uma segunda ligação é feita, utilizando as informações obtidas na primeira para obter mais dados de outra pessoa. As chamadas não são feitas de forma consecutiva, para evitar que uma se conecte à outra.

f) ***Cavalo de Tróia:*** É um tipo de *software* disfarçado como programa legítimo, mas com

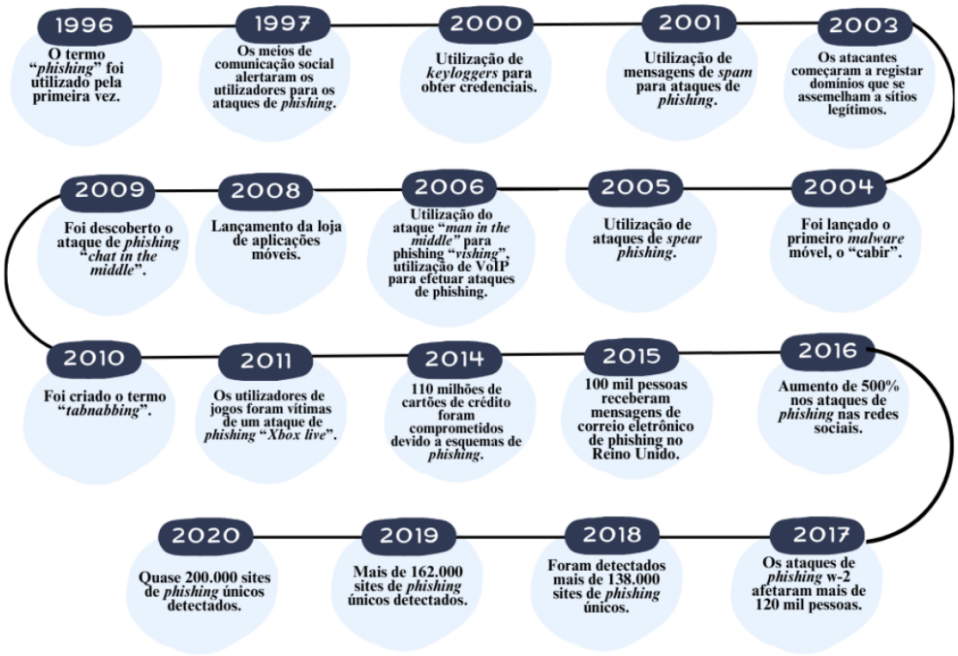
finalidades maléficas que pode ser para destruir a informação, envio a terceiros ou até roubo de senhas dos usuários.

Todavia, os Engenheiros Sociais possuem um leque bastante vasto para ser usado a sua disposição e podem fazer a utilização de mais de uma técnica ao mesmo tempo visando ter informações mais concretas e elaborar um ataque mais eficiente. (PIOVESAN *et al.*, 2019)

2.3 *Phishing*

O vocábulo *"phishing"* surgiu em meados da década de 1990, quando os *hackers* começaram a usar e-mails fraudulentos para "pescar" informações de usuários desavisados. Como esses primeiros *hackers* eram frequentemente chamados de "*phreaks*", o termo ficou conhecido como "*phishing*", com um "ph". E-mails de *phishing* atraem as pessoas e as fazem morder a isca Proofpoint (2022). Este termo foi utilizado pela primeira vez em 1996 em um fórum de notícias da provedora americana American Online (AOL) para se referir a ataques que estavam acontecendo em sua rede Phishing.org (2012) A imagem na Figura 3 mostra a evolução do *phishing*.

Figura 3 – Evolução do *phishing*



Fonte: (OLLMANN, 2024)

Phishing é um ataque que explora técnicas de engenharia social para realizar um roubo de informações confidenciais. Aleroud e Zhou (2017) Para que um ataque de *phishing*

aconteça, é necessário ter um meio para haver a interação entre o atacante e o alvo, e, para que isso aconteça, existem alguns meio mais comuns, que seria o meio da Internet, *Short Messaging Service* (SMS), meios dos quais pessoas utilizam normalmente e que podem ser usados por atacantes para interagir com vítimas. Chiew *et al.* (2018)

O autor Olivo (2010) salienta que na Internet, o *phishing* pode chegar ao usuário de diversas formas diferentes, por uma janela *pop-up* no navegador, de mensagens instantâneas ou de *emails*. Em geral, a vítima é convencida a executar um clique de *mouse*, que descarregará e instalará algum *malware* (código malicioso) ou acessará um site fraudulento.

Segundo Ramzan (2010) uma operação de *phishing* começa com um golpista *(phisher)* que elabora a ideia para o ataque. Entre outras coisas, o golpista precisará de uma lista de endereços de *e-mail* de potenciais vítimas. Uma maneira de obter essa lista é trabalhar com um *spammer*. Afinal, *spammers* são especialistas em fazer com que *e-mails* cheguem aos usuários finais e possuem a infraestrutura necessária para realizar essas tarefas. O *spammer*, por sua vez, pode entrar em contato com um *botherder*, alguém que gerencia um exército de máquinas comprometidas. Essas máquinas comprometidas podem ser usadas para hospedar programas de envio massivo de *e-mails* e disseminar mensagens de *phishing* para as vítimas.

O autor acrescenta que o golpista precisará fornecer uma mensagem de *phishing*, embora possa usar um modelo existente retirado de um *phishing* kit (que pode ser adquirido separadamente no mercado clandestino). Um *e-mail* proveniente de um *phishing* kit também é útil no caso de o golpista não ser fluente no idioma falado pela vítima. *Botnets* são particularmente eficazes para enviar mensagens de *phishing* e *spam* não solicitadas porque, mesmo que uma máquina-fonte ofensiva na rede seja detectada e bloqueada, outra pode assumir o seu lugar. Quando as mensagens de *phishing* chegam aos destinatários pretendidos, eles podem ser enganados a visitar um site fraudulento.

2.4 *Pretexting*

O *pretexting* é um seguimento do *phishing* um método de ataque também muito utilizado por *hackers*, esse tipo de ataque cibernético envolve a criação de um cenário fictício visando persuadir a vítima a conceder acesso a informações do sistema. O atacante geralmente se apresenta como uma autoridade ou alguém em um cargo superior, explorando a hierarquia para pressionar e intimidar a vítima. Tieso e Santo (2020)

Pretexting definido por IBM (2024) se trata do uso de uma história fabricada, ou

pretexto, para ganhar a confiança de uma vítima e enganá-la ou manipulá-la para compartilhar informações confidenciais, baixar malware, enviar dinheiro para criminosos ou prejudicar a si mesma ou à organização para a qual trabalha.

Para se informar e decidir por quem o atacante deve se passar para fazer o ataque em geral são utilizadas as redes sociais para analisar o perfil da vítima, descobrindo dados importantes como por exemplo, onde a vítima frequenta, onde trabalha, a função dentro da empresa, os familiares, entre outras informações que nas mãos de um criminoso especialista em *Pretexting* pode ser crucial para fazer um ataque efetivo.

Com todas essas informações adquiridas sem muito esforço, o atacante pode simplesmente mandar um *e-mail* para a vítima se passando por um familiar ou chefe, e solicitar o que deseja, muitas das vezes a vítima não percebe que se trata de um golpe cibernético e cede as informações para o criminoso. Proofpoint (2022)

A principal diferença entre pretexto e *phishing* é que o pretexto configura um ataque futuro, enquanto o *phishing* pode ser o próprio ataque. Na verdade, muitas tentativas de *phishing* são construídas em torno de cenários de pretexto. Fortinet (2025) Existem vários tipos de ataque de pretexto, dentre eles os mais comuns são:

a) **Personificação:** Um personificador imita as ações de outra pessoa, normalmente uma pessoa em quem a vítima confia, como um amigo ou colega de trabalho. Isso envolve estabelecer credibilidade, geralmente por meio de números de telefone ou endereços de *e-mail* de organizações ou pessoas fictícias.
b) **Rastreamento:** Os agentes de ameaças podem entrar fisicamente nas instalações usando *tailgating*, que é outro tipo de engenharia social. O *Tailgating* refere-se a entrar espionadamente em uma instalação depois de alguém autorizado a fazê-lo, mas sem ele perceber. Antes que a porta esteja totalmente fechada e travada, o agente de ameaças pode inserir rapidamente sua mão, pé ou qualquer outro objeto dentro da entrada.
c) **Piggybacking:** O "piggybacking" envolve uma pessoa autorizada que dá permissão a um agente de ameaças para usar suas credenciais. Por exemplo, um indivíduo não autorizado aparece na entrada de uma instalação, aborda um funcionário que está prestes a entrar no edifício e solicita assistência, dizendo que esqueceu seu passe de acesso, chaveiro ou crachá. O funcionário pode optar por ajudar o invasor a entrar nas instalações sem ao menos perceber.
d) **Isca:** Um ataque isca atrai um alvo para uma armadilha para roubar informações confi-

denciais ou espalhar *malware*. Isso pode envolver dar a eles unidades flash com *malware*. A isca frequentemente tem um elemento de aparência autêntica, como um logotipo de empresa reconhecível.

e) **Vishing:** *Vishing*, muitas vezes conhecido como *phishing* de voz, é uma tática usada em muitos ataques de engenharia social, incluindo pretexto. Essa técnica de ataque envolve o uso de chamadas telefônicas para coagir as vítimas a divulgar informações privadas ou dar aos invasores acesso ao computador da vítima.

f) **Scareware:** O *malware* sobrecarrega os alvos com mensagens de perigos falsos. Por exemplo, um ataque de *scareware* pode enganar um alvo para pensar que um malware foi instalado em seu computador. A vítima é então solicitada a instalar software de "segurança", que é realmente *malware*.

A força desses tipos de ataque dependem totalmente da conscientização e inteligência da vítima. Se a vítima for inteligente o suficiente para identificar esses ataques, então o ataque pode ser prevenido. Esse ataque é, na maioria das vezes, realizado por meio de falsificação de número de telefone. Muitas empresas de TI atualmente educam seus funcionários sobre esses ataques e como preveni-los. Lohani (2019)

2.5 *Baiting*

Os ataques de isca (baiting), também chamados de *"road apples"*, são um tipo de *phishing* que convida os usuários a clicar em um link para obter algo gratuitamente. Eles funcionam como Cavalos de Troia, onde o ataque é realizado explorando materiais de informática desprotegidos. Salahdine e Kaabouch (2019)

Um ataque de *baiting* é aquele em que iscas são usadas para atrair a vítima, despertando sua curiosidade. As iscas podem ser itens físicos ou não físicos, como *pen drives*, ou CDs com logotipos da empresa, usados para roubar informações confidenciais da vítima.

O atacante deixa a isca em uma área comum, como estacionamento ou banheiro. Assim que a vítima pega a isca por curiosidade e a conecta em um computador de trabalho ou doméstico, o dispositivo será automaticamente infectado com *malware* Chetioui *et al.* (2022). *Torrents* ilegais que contornam as leis de direitos autorais e geralmente são gratuitos são notórios por conter *malware* e vírus, sendo um bom exemplo de isca para casos assim. Venkatesha *et al.* (2021)

O *baiting* costuma prometer algo em troca, por exemplo, o hacker promete música

grátis, telefones, prêmios em dinheiro, e outros, para obter isso, a vítima precisa apenas fazer login em uma página ou compartilhar algumas informações pessoais. Alguns *hackers* enviam *pen drives* infectados para os funcionários da empresa como presente, e esse *pen drive* contém malware usado para invadir a rede da empresa. O *baiting* é comumente feito por meio de *e-mails* e anúncios. Anúncios de *baiting* são comuns em sites inseguros e na *dark web* Lohani (2019).

O *baiting* em cibersegurança representa uma ameaça real para a segurança digital. Ao entender como funciona e adotar medidas preventivas, pode-se ajudar a proteger-se contra essa tática maliciosa. A conscientização, a vigilância constante e o investimento em soluções de segurança adequadas são passos essenciais para manter sua cibersegurança robusta e resistente a ameaças de *baiting* Casa do Desenvolvedor (2023).

Tendo em vista o mencionado, o estudo sobre engenharia social e ataques como o *baiting* pode fornecer *insights* valiosos sobre as vulnerabilidades humanas exploradas por cibercriminosos, um trabalho que explore a interseção entre engenharia social e ataques de *phishing*, *pretexting* e *baiting* não apenas amplia o conhecimento acadêmico, mas também desempenha um papel crucial na proteção de indivíduos e organizações contra esse tipo de golpe.

3 METODOLOGIA

A metodologia deste trabalho é constituída por uma pesquisa bibliográfica e um questionário online. Esta abordagem busca investigar a relação entre o nível de conhecimento acadêmico e a suscetibilidade a ataques de engenharia social em diferentes faixas etárias a partir de métodos qualitativos e quantitativos.

Para a construção da pesquisa por meio do questionário online o referencial teórico foi essencial. Ele abordou os pilares da segurança da informação (confidencialidade, integridade e disponibilidade) conforme definido pela ISO (2005) ISO/IEC (2005), destacando que a proteção contra ameaças digitais depende não apenas de soluções técnicas, mas também de fatores humanos, como a conscientização e os comportamentos dos usuários. Com base nisso, foi desenvolvida uma seção no questionário dedicada a medir o nível de familiaridade dos participantes com temas como *phishing*, *pretexting* e *baiting* Gaspar (2015). Além disso, as definições de engenharia social fornecidas por autores como Gaspar (2015), que descreve a manipulação de vulnerabilidades humanas para obtenção de informações sigilosas, inspiraram as perguntas relacionadas à identificação de ataques.

Outros estudos, enfatizaram a importância da formação educacional para prevenir ataques de engenharia social, ressaltando a necessidade de integrar o tema à rotina de instituições acadêmicas e profissionais. Esses *insights* foram usados como base para explorar as percepções dos participantes sobre o impacto de treinamentos em segurança da informação e como tais ações podem reduzir vulnerabilidades. LaFrance (2004) reforça que o comportamento humano é o elo mais fraco na cadeia de segurança, o que justificou a inclusão de perguntas sobre hábitos e práticas rotineiras, como a verificação de *links* e mensagens antes de interagir com eles.

Por fim, o questionário foi estruturado para investigar não apenas o nível de conhecimento teórico dos participantes, mas também suas habilidades práticas, atitudes em relação à segurança e entendimento dos riscos associados à engenharia social. Esse enfoque multidimensional foi projetado para fornecer uma visão abrangente sobre como o conhecimento acadêmico pode ser aplicado para mitigar ameaças na prática

O questionário que se encontra no apêndice A, é composto por sete seções, com 29 perguntas diversas sobre dados demográficos, conhecimento, experiência, comportamento e atitude sobre ataques de engenharia social, além de percepção, conscientização e conhecimento a cerca de leis de proteção de dados como a LGPD. As seções da pesquisa foram divididas da seguinte forma:

a) **Seção 0 - Concordo em participar da pesquisa:** Termo de Consentimento Livre e Esclarecido (TCLE): Onde os participantes devem concordar em participar da pesquisa para prosseguir;
b) **Seção 1 - Perfil demográfico:** Dados como idade, gênero e escolaridade.
c) **Seção 2 - Conhecimento sobre engenharia social:** Incluiu perguntas sobre experiências pessoais com ataques e o nível de familiaridade com os tipos de engenharia social.
d) **Seção 3 - Práticas de segurança, comportamento e atitude:** Avaliação de como os participantes lidam com situações de possíveis ataques e como avaliam autenticidade de *sites* e *e-mails.*
e) **Seção 4 - Habilidades práticas de identificação:** Testou os participantes com exemplos simulados de *phishing*, *pretexting* e *baiting*.
f) **Seção 5 - Educação e conscientização:** Análise da opinião dos participantes sobre a importância da educação em engenharia social e os métodos mais eficazes de conscientização.
g) **Seção 6 - Conhecimento legal:** Esta seção abordou o nível de conhecimento sobre a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet.

O embasamento teórico também contribuiu para a estruturação das fases de análise. Por exemplo, a análise comportamental dos ataques de engenharia social Coelho *et al.* (2013) e as classificações de atacantes propostas por Zager (2002) permitiram ajudar a identificar vulnerabilidades específicas nas respostas dos participantes. Além disso, a abordagem de Oosterloo (2008), que detalha as etapas de preparação, manipulação, exploração e execução de ataques, inspirou questões voltadas à conscientização sobre os métodos usados pelos atacantes.

Ao final, os dados coletados foram analisados quantitativamente por meio de gráficos e qualitativamente por interpretações baseadas no referencial teórico, possibilitando conclusões robustas sobre as lacunas de conhecimento e as estratégias práticas para mitigá-las. Este alinhamento entre teoria e prática reforça a contribuição acadêmica e aplicada deste estudo.

4 RESULTADOS

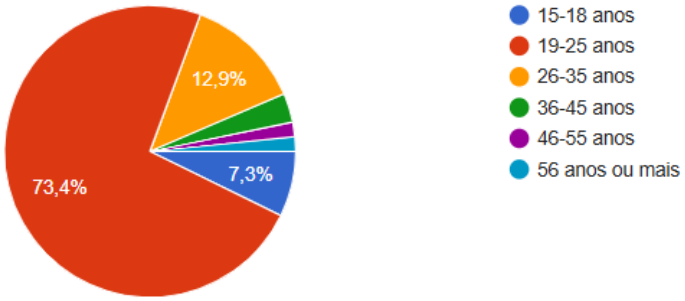
O questionário que se encontra disponibilizado no apêndice A foi aplicado no período de 16 de dezembro de 2024 a 21 de janeiro de 2025. Ele contou com a participação de moradores da cidade de Itapajé, sede da Universidade Federal do Ceará, campus Jardins de Anita. A pesquisa foi realizada com pessoas de idades variadas, porém apenas a partir de 15 anos, isto a fim de trabalhar com pessoas que podem estar cursando o ensino médio no momento da aplicação do questionário.

O questionário foi aplicado com o objetivo de analisar o nível de conhecimento e opiniões de pessoas em diferentes faixas etárias e com níveis de escolaridade variados, a respeito de ataques de engenharia social. A pesquisa feita por meio do questionário alcançou um conjunto total de 124 amostras válidas, estas amostram servirão como os elementos de análise deste trabalho.

A pesquisa realizada levou em consideração aspectos legais como a Lei geral de proteção de dados (LGPD), especialmente no que se refere à coleta, armazenamento e uso de dados dos participantes. Antes de mais nada, foi garantido que houvesse o consentimento informado do participante para coleta de quaisquer dados pessoais a fim de assegurar que todos estivessem cientes das finalidades da pesquisa, da natureza dos dados que seriam coletados e de como essas informações serão utilizadas. Para garantir a privacidade e segurança dos participantes o questionário foi respondido por todos de forma anônima.

A primeira seção do questionário é composta por três perguntas. No gráfico da Figura 4 é possível observar a classificação dos participantes por faixa etária. A faixa etária que conteve maior representatividade foi a de 19 a 25 anos, com 74,4%, seguida por 12,9% de 26 a 35 anos, 7,3% de 15 a 18 anos, 3,2% de 36 a 45 anos, 1,6% de 46 a 55 anos, e 1,6% de 56 anos ou mais. Portanto, a maioria das pessoas que responderam o questionário são jovens e adultos de 19 a 25 anos.

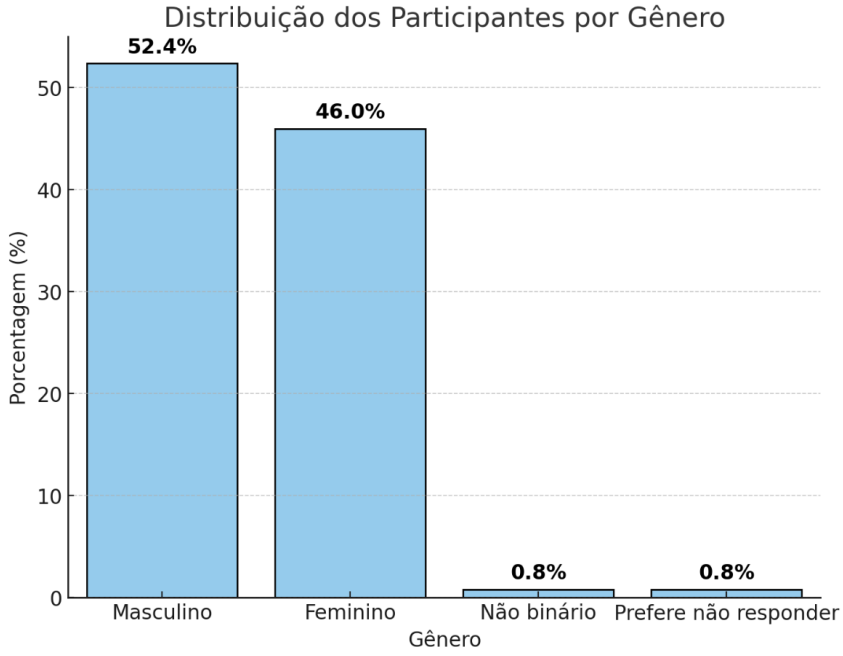
Figura 4 – Distribuição das idades dos participantes



Fonte: Elaborada pela autora.

O gráfico da Figura 5 por sua vez, apresenta a separação dos participantes por gênero, sendo 52,4% do sexo masculino, 46% do sexo feminino, 0,8% não binário e 0,8% que preferiu não responder. O gráfico pôde demonstrar a relevante presença do sexo masculino na participação da pesquisa.

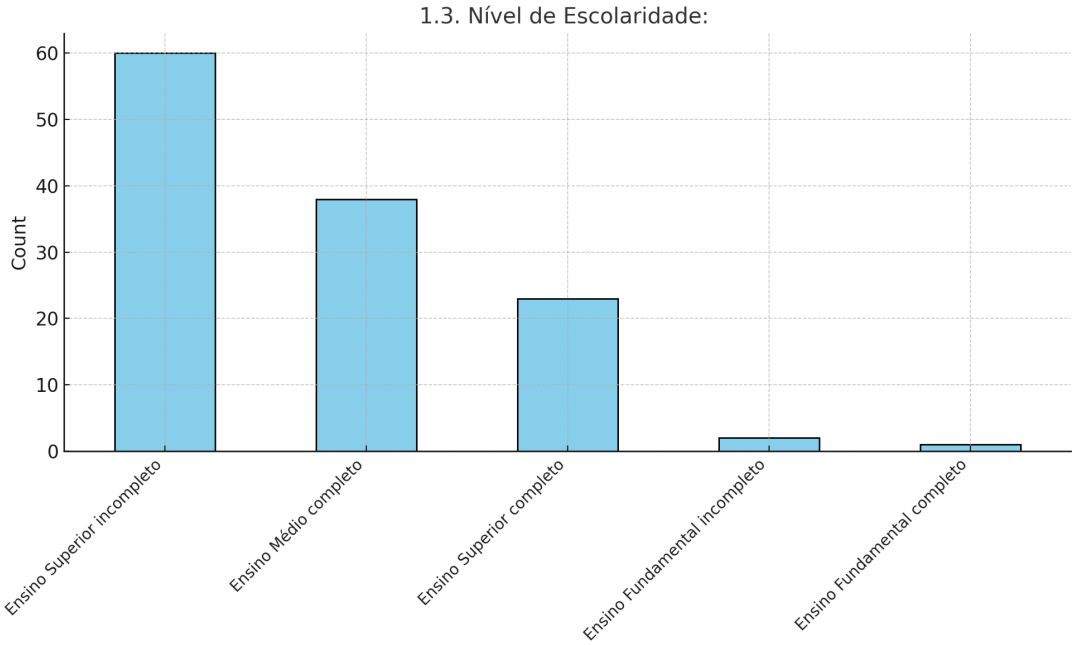
Figura 5 – Distribuição por gênero dos participantes



Fonte: Elaborada pela autora.

No gráfico da Figura 6 é possível observar os resultados da terceira e última pergunta da primeira seção que separa os participantes por nível de escolaridade. Conforme a figura, a maioria dos participantes, com 60% apresentam o ensino superior incompleto, seguido por 30,6% participantes que possuem o ensino médio completo, 18,5% apresentam o ensino superior completo, 1,6% ensino fundamental incompleto e 0,8% ensino fundamental completo. É possível

Figura 6 – Distribuição por nível de escolaridade



Fonte: Elaborada pela autora.

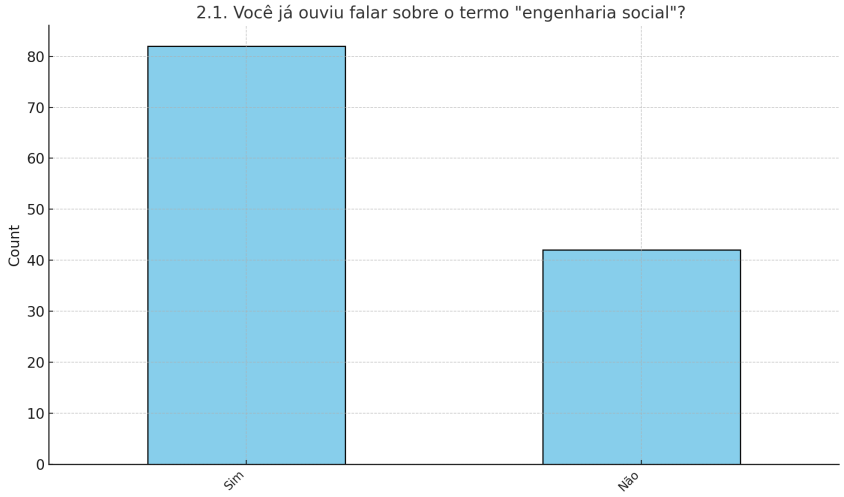
observar que a partir dos dados apresentados a grande maioria dos participantes possuem ao menos o nível médio de escolaridade.

A segunda seção é composta perguntas referentes ao conhecimento sobre engenharia social. O gráfico da Figura 7 é referente ao conhecimento que os participantes têm a respeito de engenharia social. Por meio do gráfico pode-se observar que a maioria dos participantes, composta por 66,1% já ouviram falar ao menos alguma vez sobre engenharia social, o que é um ponto positivo em se tratando de segurança. Porém, o número de pessoas que nunca ouviram falar de engenharia social é composto de 33,9% o que sugere que há ainda bastante desinformação a respeito de ataques desse tipo.

O gráfico da Figura 8 mostra se o participante acredita que já foi vítima de um ataque de engenharia social, não sabe ao certo ou tem certeza que nunca foi. A maioria de 41,9% demonstrou dúvida optando por responder que talvez tenham sido vítimas, mas não há certeza. Dado este que é muito importante para a pesquisa, uma vez que isso indica que muitas pessoas não apresentam conhecimento suficiente para identificar ou reconhecer ataques de engenharia social. Isto destacando a necessidade de maior exposição do assunto a fim de melhorar as capacidades de conscientização e detecção de ataques. A segunda maior parte, composta por 40,3% afirmou já ter sido vítima de ataque de engenharia social, e 17,7% relatam nunca terem passado por uma situação de ataque de engenharia social.

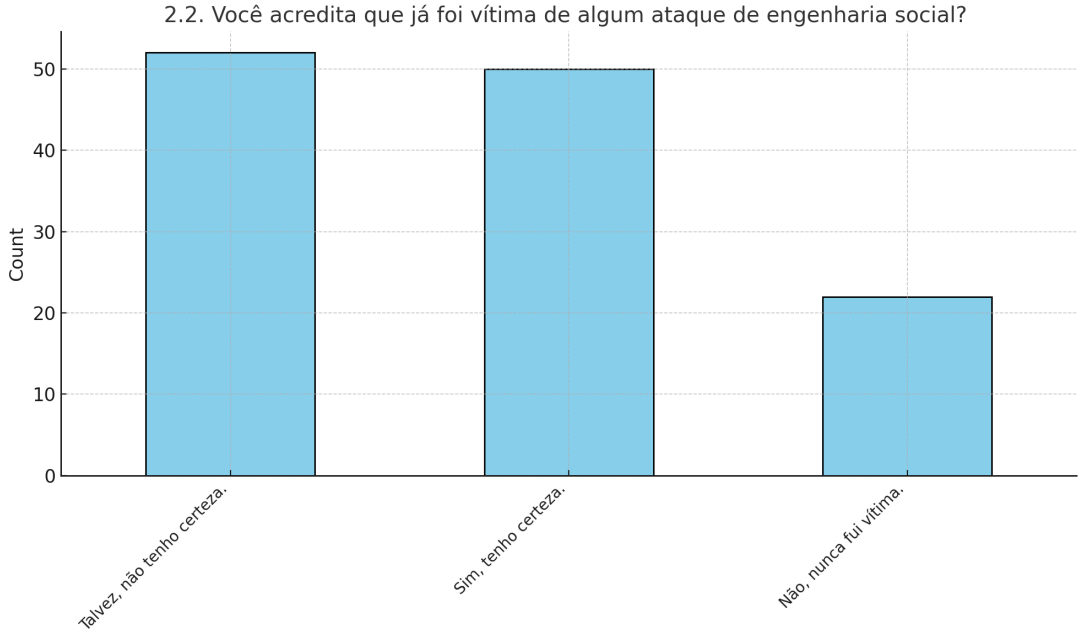
Seguindo as respostas apresentadas na Figura 8, foi questionado aos que responderam

Figura 7 – Conhecimento sobre engenharia social



Fonte: Elaborada pela autora.

Figura 8 – Pergunta 2.2: já foi vítima de engenharia social?

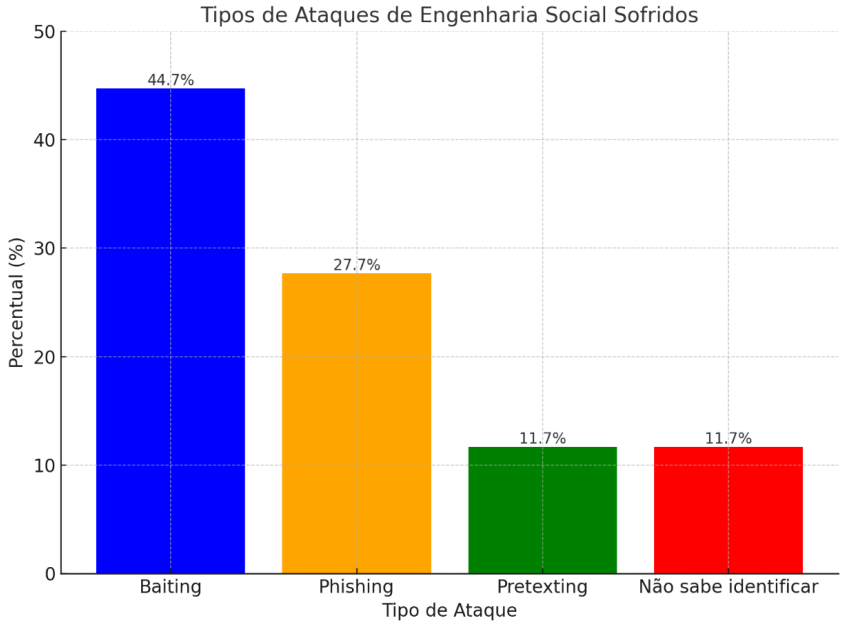


Fonte: Elaborada pela autora.

que já haviam sido vítimas de ataque de engenharia social se eles saberiam informar por qual tipo de ataque foram vítimas, para isso foram sugeridas três opções de ataques, o ataque de *phishing*, o de *pretexting* e o de *baiting*, além das opções de todos acima e de que foi vítima, mas não consegue reconhecer qual o tipo específico. Na Figura 9 observa-se que a maioria com 44,7% afirma ter sofrido um ataque de *baiting*, conhecido por atrair a vítima com algo aparentemente valioso ou interessante. Em segundo lugar com 27,7% o *phishing* que são mensagens fraudulentas pedindo informações pessoais ou financeiras, e em terceiro o *pretexting* em que o atacante cria uma história para enganar a vítima e obter informações sensíveis ou acesso a recursos com 11,7%.

Além destes, houveram ainda 11,7% dos participantes que afirmaram não saber identificar, o que reforça mais uma vez a falta de conhecimento a respeito do assunto, uma vez que até mesmo pessoas que sabem que foram vítimas de um ataque não terem confiança para afirmar qual tipo de ataque foi.

Figura 9 – Pergunta 2.3: Qual tipo de ataque?

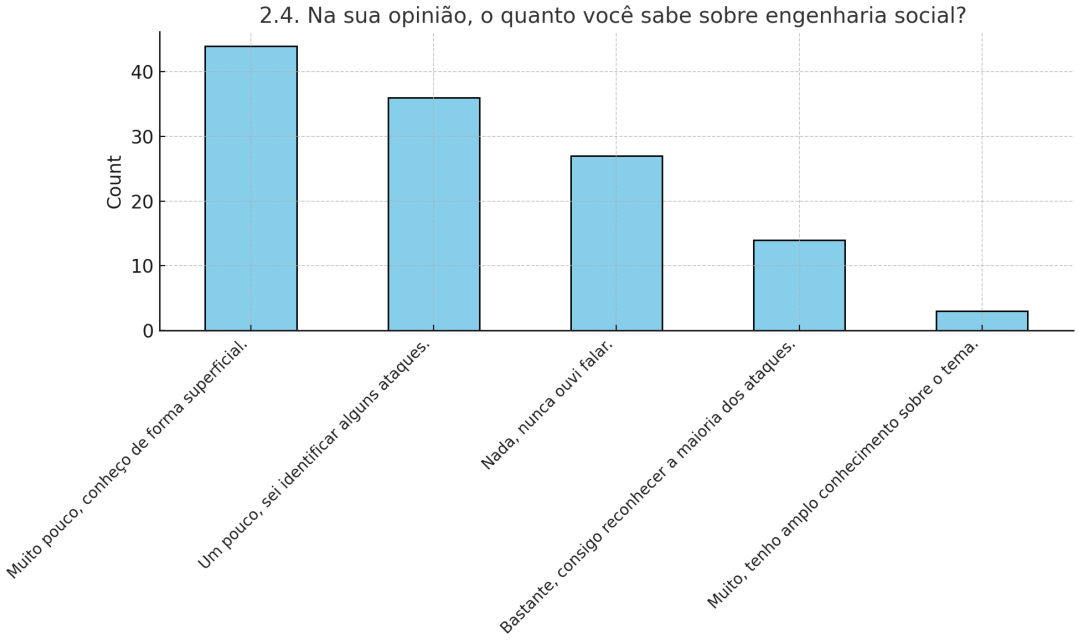


Fonte: Elaborada pela autora.

O questionamento da Figura 10 tem a ver com o nível de conhecimento dos participantes a respeito de engenharia social. Referente a figura temos que 35,5% sabe muito pouco, conhece apenas de forma superficial o termo, 29% que conhece um pouco e sabe identificar alguns ataques, 21,8% que não sabe nada, nunca ouviu falar. Estes indivíduos se tornam alvos fáceis para os atacantes uma vez que não possuem as ferramentas técnicas e cognitivas para identificar mensagens fraudulentas ou outros tipos de ameaças. Houve ainda uma porcentagem de 11,3% que afirma conhecer bastante sobre engenharia social e consegue identificar a maioria dos ataques, e 2,4% diz ter amplo conhecimento no assunto. Esses dados são cruciais para a pesquisa, pois dá indícios de que há necessidade de treinamentos contínuos.

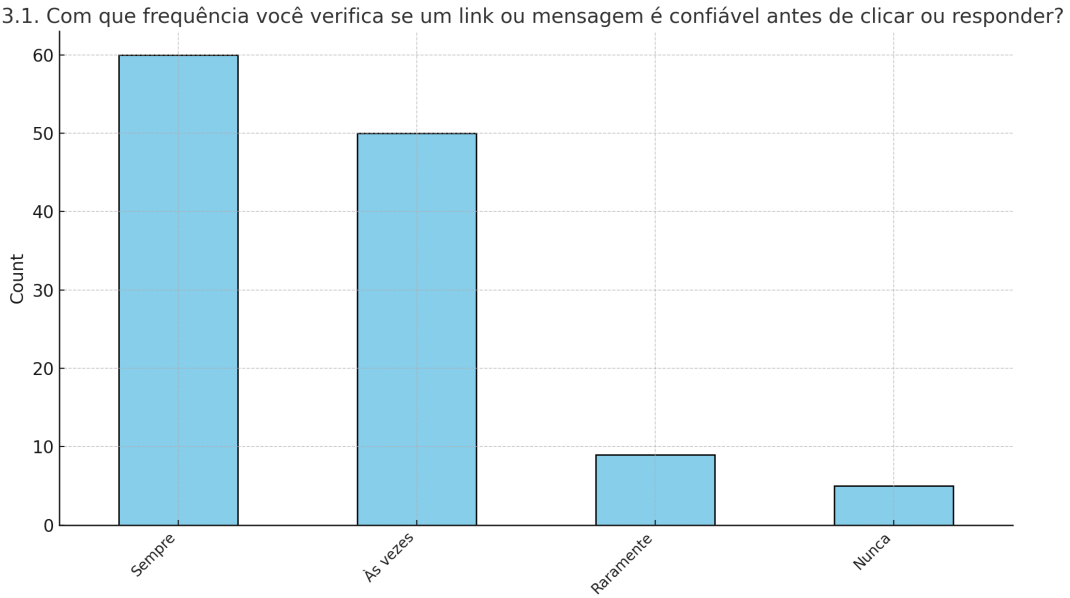
Em relação às questões da terceira seção. O gráfico da Figura 11 representa a frequência em que o participante verifica se um link ou mensagem é confiável antes de clicar, ou responder. Como demostra o gráfico 11, 60 pessoas responderam que verificam sempre a autenticidade de mensagens recebidas, ocupando 48,4% do total, o que significa que a maioria tem um comportamento mais alerta a possíveis ataques. A segunda maior porcentagem de 40,3%

Figura 10 – Nível de conhecimento dos participantes sobre engenharia social



Fonte: Elaborada pela autora.

Figura 11 – Frequência de verificação de autenticidade de mensagens recebidas

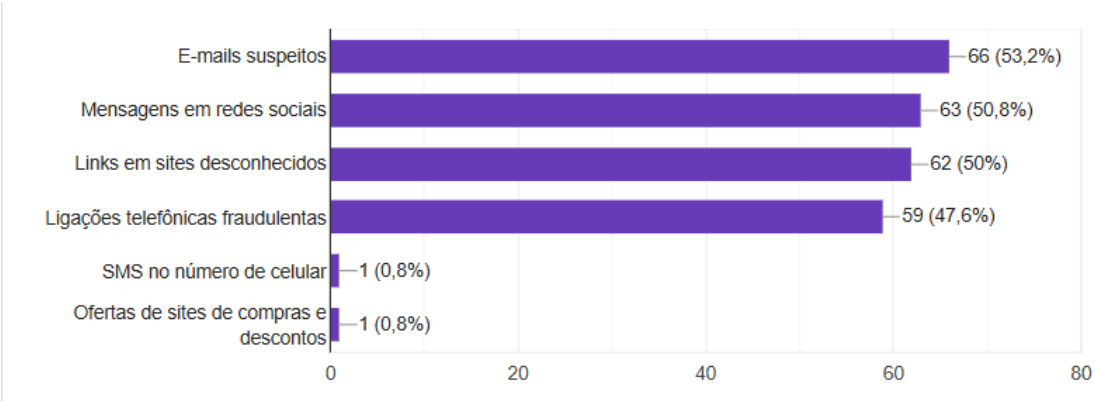


Fonte: Elaborada pela autora.

se refere à 50 dos participantes que dizem verificar se as mensagens ou links são seguros, o dado indica que a maioria do público participante da pesquisa apresenta certa preocupação com os ataques, porém o ato de verificação deve ser rotineiro e não esporádico para que os riscos sejam diminuídos. Há ainda 9 pessoas, 7,3% que dizem verificar apenas raramente e 5 pessoas, 4% que nunca verificam a veracidade de mensagens recebidas ou links compartilhados. Isto indica que ao menos 4 pessoas estão completamente vulneráveis a ataques de engenharia social.

A Figura 12 por sua vez, busca saber do participante qual principal fonte de ataque ele acredita estar exposto. Os dados indicam que 53,2% dos participantes acredita ser por meio de *e-mails* suspeitos, o que demonstra que esse método é o mais comum entre os atacantes, podendo ser reflexo do número de vítimas que é possível obter por meio dele. 50,8% afirma ser por meio de mensagens em redes sociais, ferramenta muito utilizada para ataques como *pretexting* e *baiting*. 50% diz acreditar que seja por links em sites desconhecidos. 47,6% acredita que seja por ligações telefônicas fraudulentas. 0,8% por SMS no número de celular e 0,8% por ofertas de compras e descontos. Vale ressaltar que esta pergunta aceitava mais de uma opção como resposta. A partir da análise das respostas é possível identificar que os participantes em grande maioria estariam expostos há ataques recebidos por meio de ofertas de compras e descontos, esse meio de ataque é um dos mais frequentes no cibercrime, isso reforça a necessidade de treinamentos específicos sobre ataques de engenharia social, não apenas em instituições educacionais.

Figura 12 – Principal fonte de exposição a ataques segundo os participantes

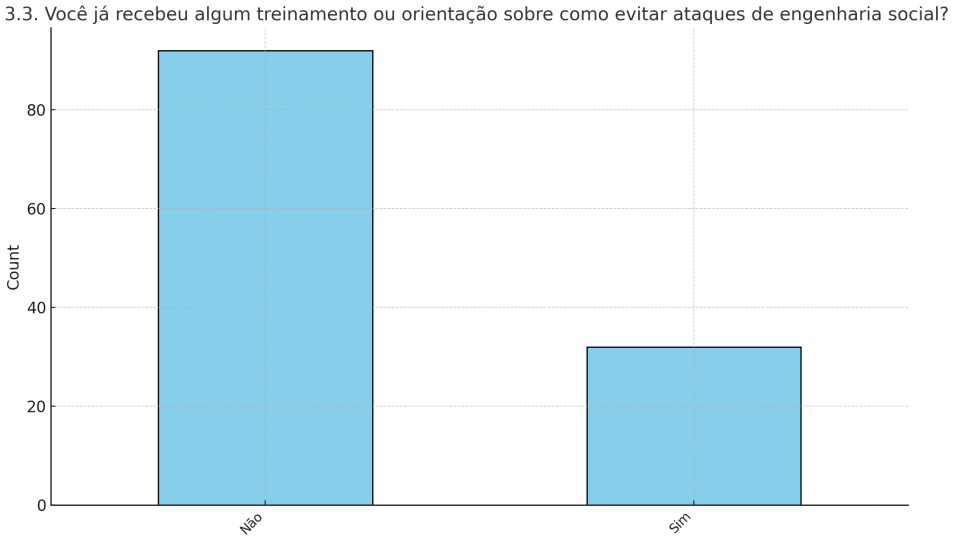


Fonte: Elaborada pela autora.

Para finalizar a seção três, foi questionado se os participantes já haviam recebido algum tipo de treinamento ou orientação sobre como evitar ataques de engenharia social. Os dados da Figura 13 indicam que 92 pessoas, 74,2% dos participantes nunca receberam nenhum tipo de treinamento e 32 pessoas, 25,8% afirmam já terem recebido algum treinamento ou orientação. Esses resultados reforçam a necessidade de aumentar a oferta e a adesão a programas de treinamento e educação sobre segurança em relação ao tema engenharia social, para melhorar a proteção e a capacidade de resposta dos usuários a ameaças como essas.

A quarta seção é iniciada com o questionamento se os participantes acreditam serem capazes de identificar um *e-mail* do ataque de *phishing* facilmente. A maioria com 72 pessoas, 56,1% do total afirma ter capacidade de identificar um *e-mail* com *phishing*, e 52 pessoas, 41,9%

Figura 13 – Relação de participantes que já receberam treinamentos ou orientações sobre engenharia social



Fonte: Elaborada pela autora.

afirma não conseguir identificar um *e-mail* com *phishing*. Isto significa que um grande número de pessoas ainda não possui conhecimento suficiente para identificar os alertas de *e-mails* suspeitos, os tornando possíveis vítimas dependendo da atitude dos mesmos ao se depararem com um *e-mail* incomum.

A Figura 14 representa o gráfico sobre o nível de confiança dos participantes em relação à identificação de ataques de *phishing* em *e-mails*.

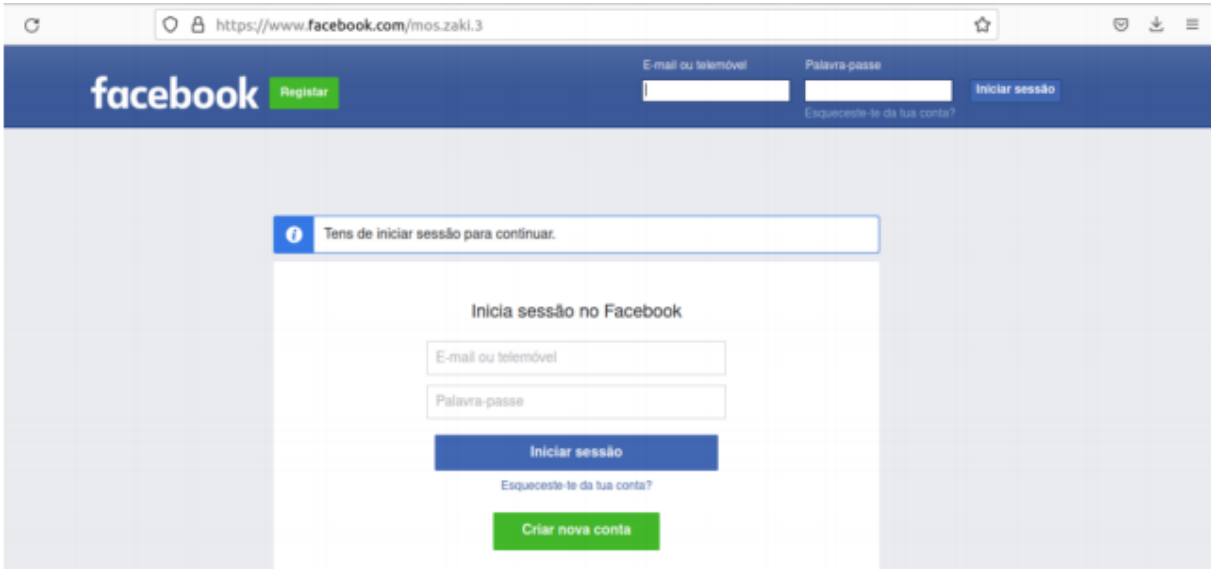
Figura 14 – Nível de confiança dos participantes em relação à identificação de ataques de phishing

Fonte: Elaborada pela autora.

A segunda questão da quarta seção busca verificar as habilidades dos participantes em relação a identificar sinais suspeitos na página de login do Facebook. De acordo com a análise feita pelos participantes da Figura 15, 66 pessoas, 55,6% dos participantes acredita que a imagem apresenta sim sinais que sugerem que o site pode ser falso, e 55 pessoas, 44,4% acredita que não há sinais suspeitos na imagem, como mostra o gráfico da Figura 16.

Levando-se em consideração que a imagem da Figura 15 tem sinais de típicos de ataque de *phishing* como, por exemplo, a mudança de URL, os resultados se tornam um tanto quanto preocupantes. Além da URL incomum, "https:/www.facebook.com/mos.zaki.3"que deveria ser “https:/www.facebook.com/login"a mensagem exposta "Tens de iniciar sessão para continuar"faz parte de um grupo de características usadas nos ataques de *phishing* é uma tática para forçar o usuário a inserir suas credenciais na página.

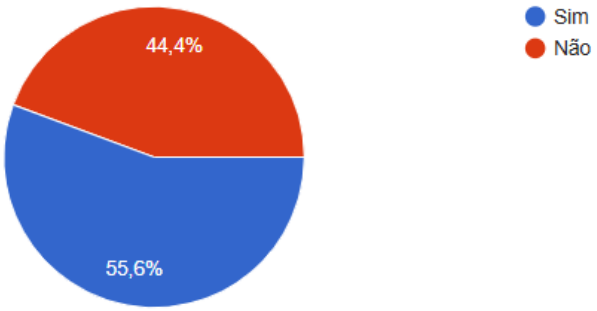
Figura 15 – Pergunta 4.2 do apêndice A



Fonte: Elaborada pela autora.

Por sua vez, na Figura 17 está representada a imagem da questão 4.3 do apêndice A que pede ao participante para analisar se há no *e-mail* recebido algum sinal que indique ser um possível ataque de *phishing*, *pretexting*, *baiting* ou outro. Quanto a identificação do usuário em relação ao *e-mail* recebido 101 pessoas, 81,5% dos participantes afirma que sim, o *e-mail* apresenta sinais de possível ataque. 23 pessoas, 18,5% afirma não ter encontrado possíveis sinais de ataque como ilustra a Figura 18. Por mais que haja uma melhora na identificação dos usuários se comparada com a questão anterior, ainda há uma grande lacuna sobre o nível de conhecimento dos participantes em relação à ataques de engenharia social para ser preenchida.

Figura 16 – Respostas à pergunta 4,2 do apêndice A



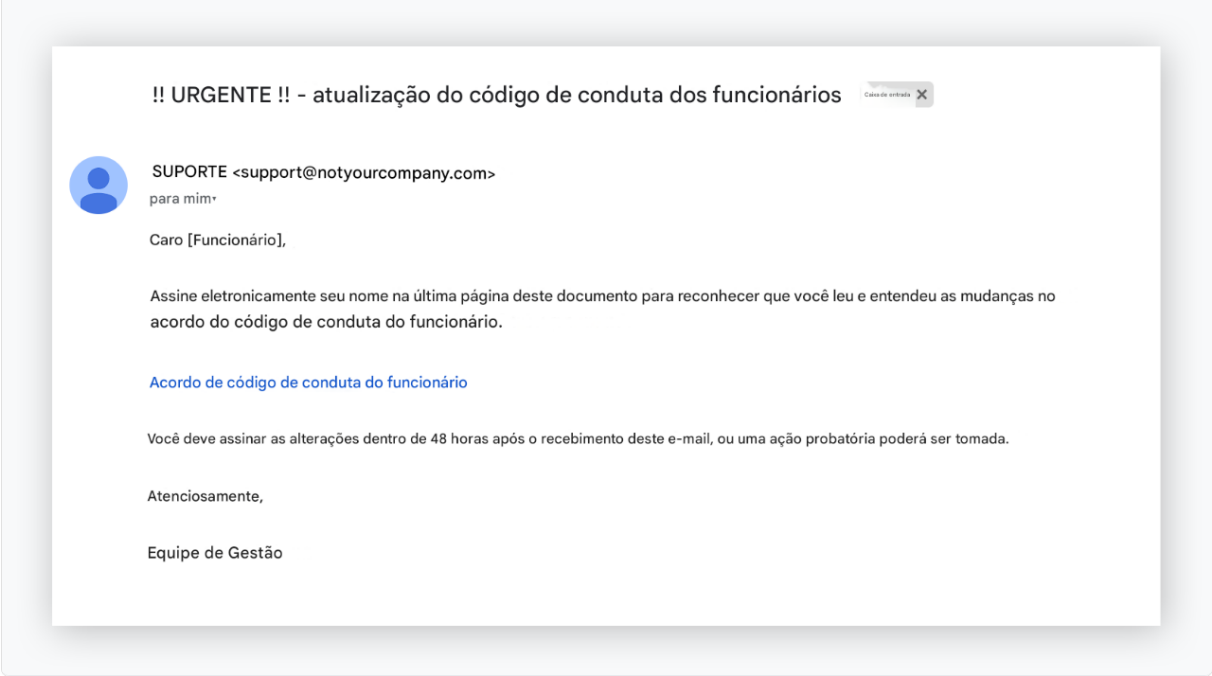
Fonte: Elaborada pela autora.

A imagem na Figura 17 do *e-mail* simulado apresenta características nítidas de um ataque de *pretexting* onde há uso de uma história fabricada, ou pretexto, para ganhar a confiança da vítima e enganá-la ou manipulá-la para prejudicar a si mesma ou à empresas. Na imagem o atacante se passa por uma equipe de "suporte"de uma empresa e pede que o funcionário assine eletronicamente seu nome na última página de um documento disponibilizado por meio de um link para reconhecer que o funcionário leu e concordou com as mudanças no código de conduta dos funcionários. Além da solicitação ele instiga a vítima a assinar em um prazo de no máximo 48 horas ou ações probatórias serão tomadas, isto é usado para causar efeito psicológico na vítima que pode antes de recorrer à gestão para obter informações, responder de imediato para evitar complicações futuras.

A pergunta 4,4 pede ao participante para responder o que ele faria ao receber um *e-mail* como mostra a imagem. A imagem em questão representada na Figura 19 se trata de um suposto *e-mail* dos correios que indica a autorização para a retirada de um objeto, e apresenta seu protocolo BR687674983. No *e-mail* é dito que para realizar a retirada do objeto é obrigatório emitir uma guia, disponibilizada por meio de um link.

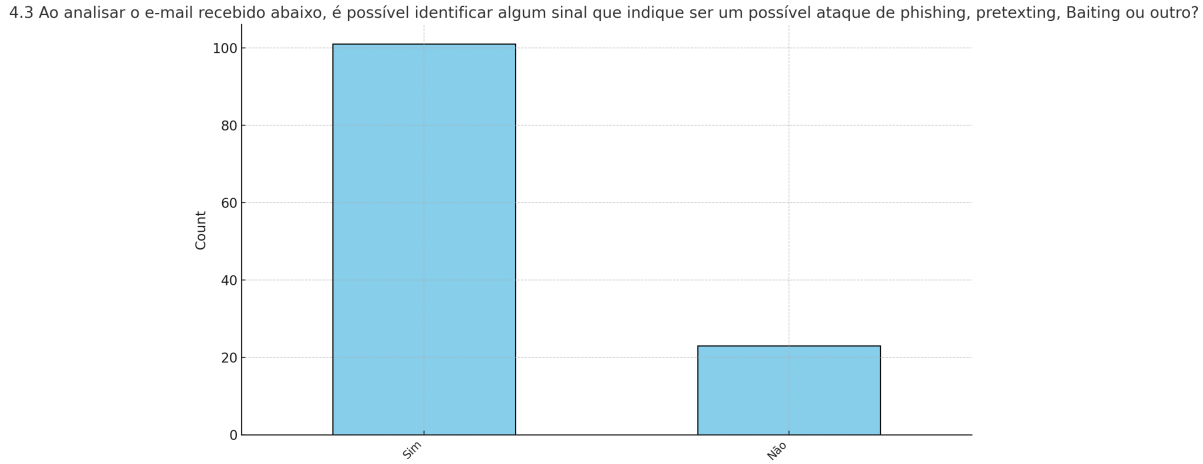
Quanto às respostas dos participantes contidas na Figura 20, 57 dos participantes, 46% diz que ignorariam a mensagem, junto deles também ocupando 46%, 57 pessoas dizem que verificariam com a fonte. 12,1% afirma que relataria o *e-mail*, porém 12,1% também diz que clicaria no link para conferir, o que não é uma atitude indicada em nenhuma hipótese. 10,5% diz que bloquearia o remetente, 4% diz que baixaria o anexo. Outras três pessoas apresentaram respostas diferentes, uma diz que iria até os correios verificar a veracidade caso estivesse esperando alguma entrega, outra diz que verificaria primeiro o site oficial dos correios ou o aplicativo, e por último uma responde que bloquearia o remetente, pois afirma que acredita

Figura 17 – Imagem da pergunta 4,3 do apêndice A



Fonte: Elaborada pela autora.

Figura 18 – Respostas da pergunta 4,3 do apêndice A



Fonte: Elaborada pela autora.

que os correios, não mandaria uma mensagem diretamente ao comprador que por sua vez deve acompanhar a entrega pelo site da loja em questão.

As respostas de maneira geral indicam que os participantes demonstram certa atenção referente a esse tipo de ataque, entretanto o número de pessoas que clicariam no link ou baixariam o anexo para verificar ainda é preocupante, uma vez que apenas esse pequeno passo seria a realização do desejo do atacante.

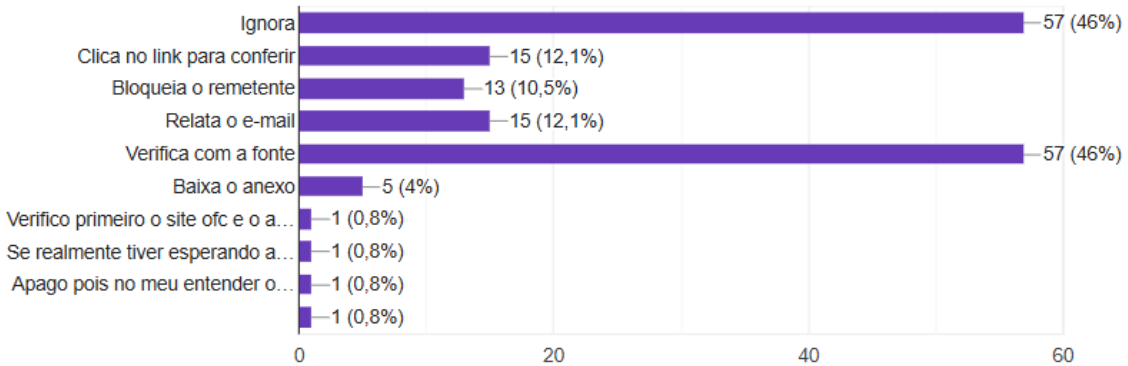
A imagem apresenta as características do ataque de *baiting* que é uma técnica de engenharia social utilizada por cibercriminosos para enganar as vítimas e fazê-las revelar

Figura 19 – Imagem da pergunta 4,4 do apêndice A

Fonte: Elaborada pela autora.

informações confidenciais. Esse tipo de ataque se baseia no desejo das pessoas de obter algo gratuito ou atraente, no caso em questão seria receber um pedido que pode ou não ter sido feito pela vítima recentemente.

Figura 20 – Respostas da pergunta 4,4 do apêndice A



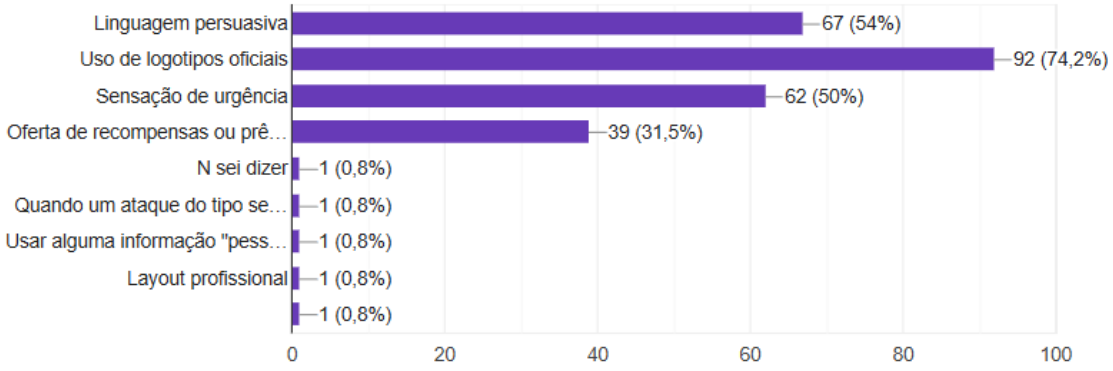
Fonte: Elaborada pela autora.

Já a pergunta 4,5 na Figura 21 que disponibilizava aos participantes a possibilidade

de mais de uma opção de resposta, busca saber o que o participante acha que torna um ataque de engenharia social convincente. Dentre as respostas representadas na figura 20, 92 participantes, 74,2% respondeu que seria o uso de logotipos oficiais, 67 participantes, 54% diz que é o uso de uma linguagem persuasiva, 62 participantes, 50% afirma que é a sensação de urgência, 39 participantes, 31,5% acredita que seja a oferta de recompensas ou prêmios. Há ainda aqueles que falaram ser todas as opções acima, ou usar alguma informação pessoal, layout profissional e ainda uma das pessoas disse não saber dizer o que influencia o ataque a ser convincente.

Conforme a análise destes resultados, é possível concluir que todo material que faça imitação de algo oficial, que use linguagem formal, com conteúdos textuais menos extravagantes e tudo aquilo que imita de forma fiel algum serviço, tende a deixar os ataques de engenharia social mais eficazes. Em seguida, a pergunta 4,6 questiona se o participante se sente confiante em sua capacidade de evitar ser enganado por engenharia social. A Figura 22 representa os dados das respostas dos participantes.

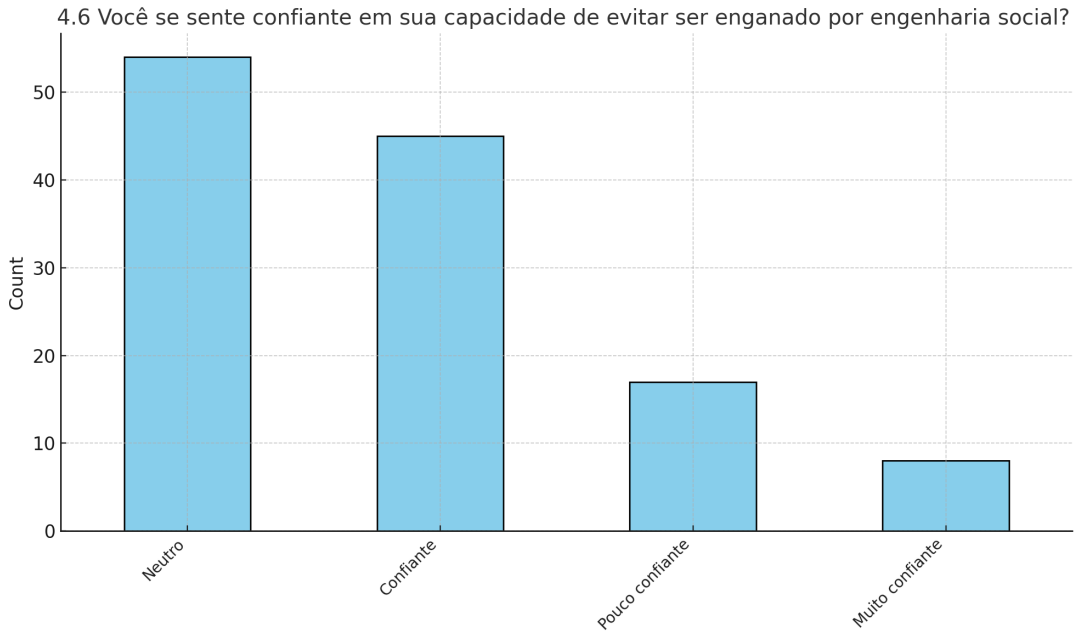
Figura 21 – Fatores que tornam um ataque de engenharia social convincente



Fonte: Elaborada pela autora.

Segundo as respostas, 54 participantes se declaram neutros, o que pode sugerir incerteza ou a percepção de que podem estar vulneráveis dependendo da circunstância. 45 participantes se consideram confiantes, o que indica que quase metade dos participantes acredita possuir um nível satisfatório de habilidade para reconhecer e evitar essas ameaças. 17 participantes demonstram ser pouco confiante, o que indica que representa vulnerabilidade dessa parcela de participantes em relação a sofrer ataques de engenharia social. 8 participantes se sentem muito confiantes, o que indica que estariam totalmente preparados para enfrentar tentativas de *pretexting* por exemplo. Nenhum dos participantes escolheu a opção "nada confiante". O último questionamento feito na seção quatro, pergunta aos participantes qual fator mais importantes

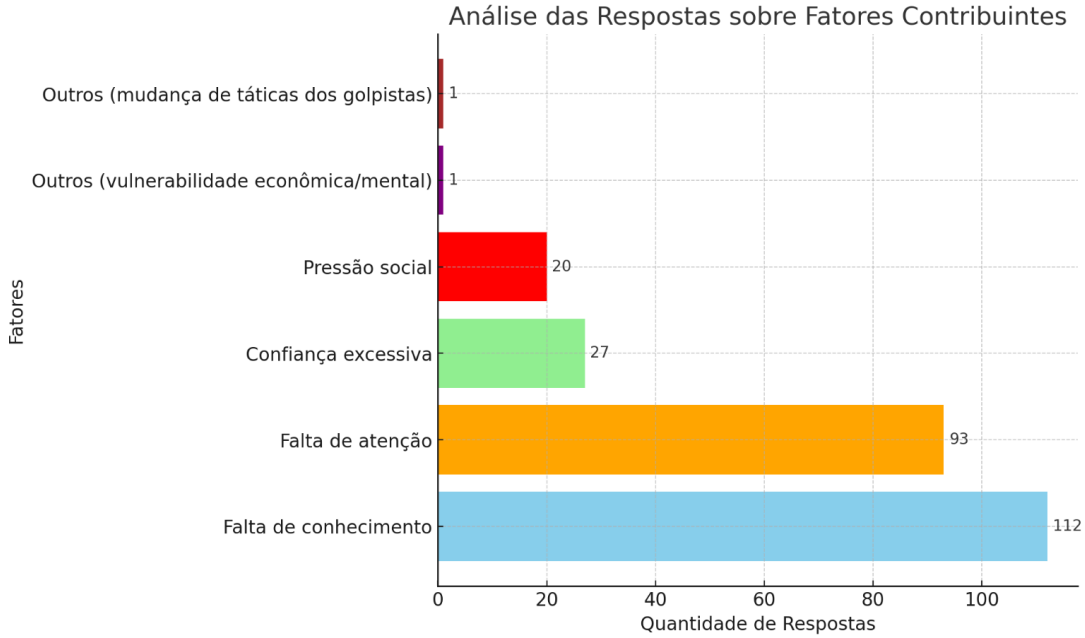
Figura 22 – Capacidades dos participantes de evitar ataques de engenharia social



Fonte: Elaborada pela autora.

que eles consideram que contribui para a vulnerabilidade aos ataques que utilizam engenharia social. A Figura 23 apresenta os resultados deste questionamento, em que o participante poderia escolher mais de uma opção.

Figura 23 – Análise de fatores contribuintes

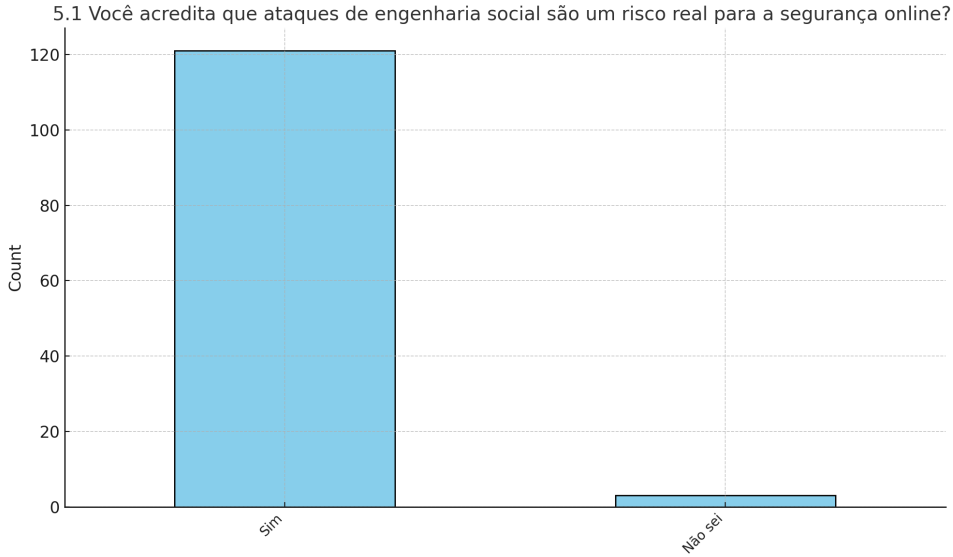


Fonte: Elaborada pela autora.

Segundo a análise das respostas, 112 pessoas acreditam que seja a falta de conhecimento, 93 pessoas acreditam ser falta de atenção, 27 pessoas diz ser confiança excessiva,

20 pessoas enxergam a pressão social como o principal fator. Houve ainda dois comentários diferentes, um deles diz que o fator principal é falta de conhecimento em conjunto da vulnerabilidade econômica ou mental da vítima, e outro que diz ser por conta das mudanças de táticas dos golpistas. A quinta seção será representada a partir da Figura 24 que busca a opinião dos participantes sobre a educação sobre engenharia social ser um risco real para a segurança online.

Figura 24 – Distribuição dos participantes que acreditam que engenharia social é um risco real.



Fonte: Elaborada pela autora.

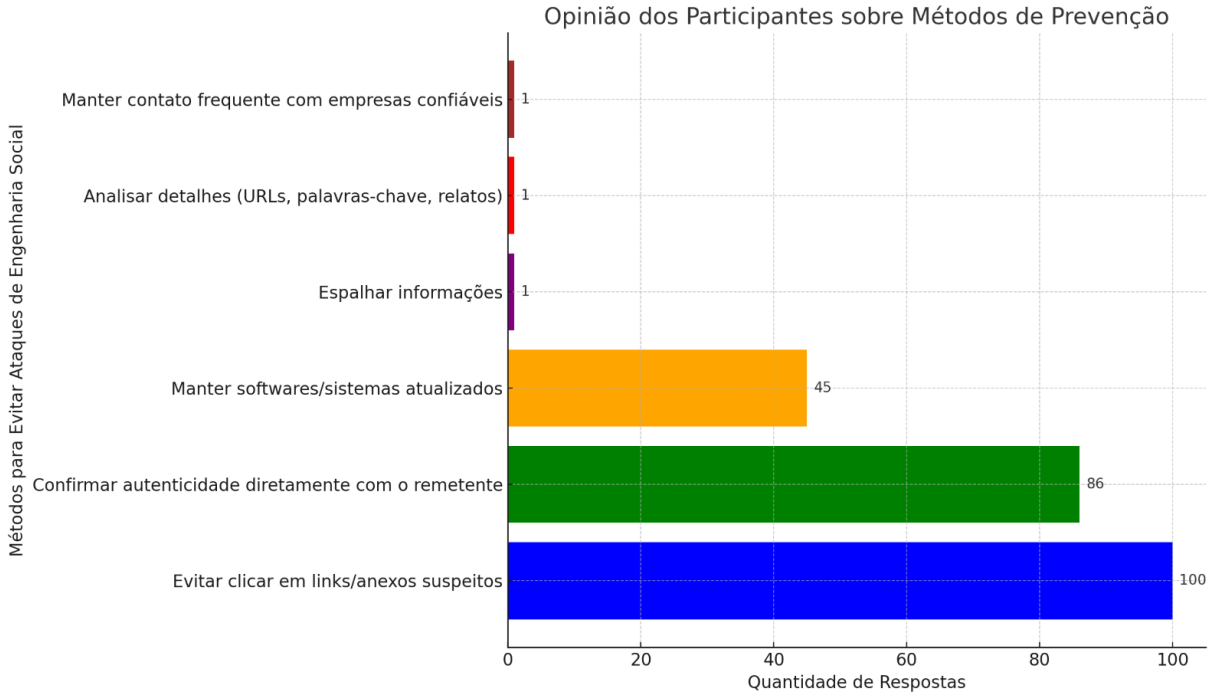
O gráfico da Figura 24 mostra que 121 pessoas, das 124 que responderam o formulário consideram que ataques de engenharia social representam de fato riscos reais para sua segurança, e apenas três afirmaram não ser um risco. A resposta reforça a necessidade de maior exposição dos reais riscos de um ataque de engenharia social e suas consequências, para que todos possam tratar do assunto de forma mais cuidadosa.

A segunda pergunta da quinta seção busca saber a opinião dos participantes sobre qual a melhor maneira de evitar ser vítima de ataques de engenharia social. A Figura 25 representa as respostas dos participantes, suas respostas poderiam ser mais de uma das opções listadas ou outras respostas que não estivessem indicadas na questão.

100 dos participantes, diz que a melhor maneira é evitando clicar em links ou anexos suspeitos, 86 participantes dizem que o ideal é confirmar a autenticidade de mensagens diretamente com o remetente, 45 dos participantes diz que seria manter softwares e sistemas atualizados. Dentre as respostas, ainda é possível analisar três respostas diferentes das dispostas na questão, uma indica que espalhar informações seria a melhor maneira de evitar ser vítima de

um ataque desse tipo, outra afirma que é essencial sempre analisar cada detalhe, principalmente se algo parece muito benéfico, então se deve sempre verificar as URLs, palavras-chave, e procurar por relatos na internet a respeito, e por fim uma das respostas indica que o certo seria manter o contato frequente com as empresas da qual se tenha alguma relação de consumo e que seja confiável.

Figura 25 – Opinião dos participantes sobre métodos de prevenção de ataques de engenharia social

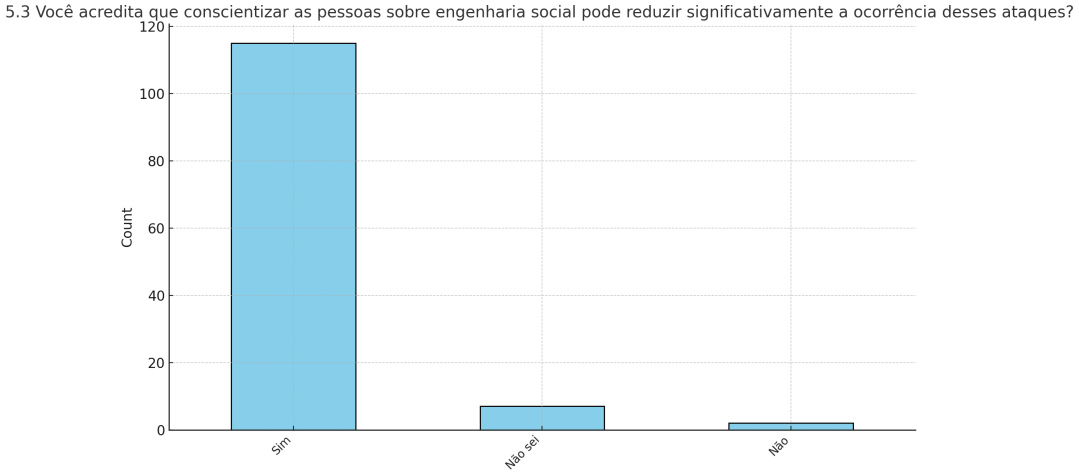


Fonte: Elaborada pela autora.

A pergunta da terceira questão da quinta seção indaga se o participante acredita que conscientizar as pessoas sobre engenharia social pode reduzir significativamente a ocorrência desses ataques. Na Figura 26 se encontram os resultados da pergunta. Segundo o gráfico na Figura 26, 115 pessoas, 92,7% dos participantes acredita que sim, o que significa que a grande maioria está ciente que a aplicação de treinamentos a respeito de engenharia social pode ajudar a evitar os ataques de engenharia social. 7 pessoas, 5,6% afirma não saber se isso ajudaria, e 2 pessoas, 1,6% acredita que não seria útil para evitar cair em ataques como esse. Em seguida foi perguntado aos participantes quais medidas eles consideram mais eficazes para conscientizar as pessoas sobre ataques de engenharia social. A Figura 27 apresenta os resultados da questão.

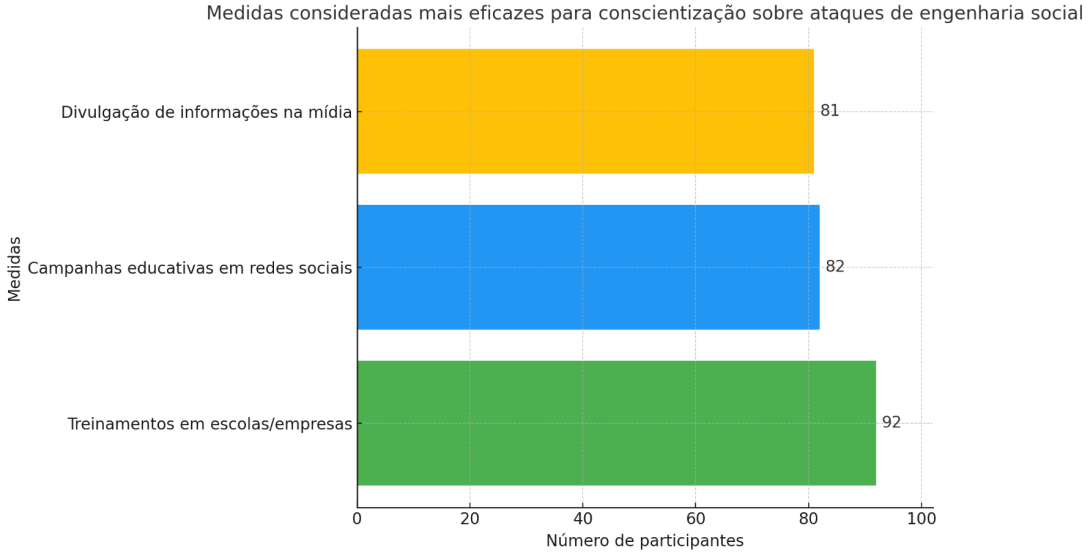
Com a análise dos resultados é possível observar que, 92 participantes acreditam que seja por meio de treinamentos em escolas ou empresas, o que é um dado muito importante para a pesquisa uma vez que se reforça a importância de implementar treinamentos sistemáticos

Figura 26 – A conscientização a cerca de engenharia social como forma de reduzir os ataques



Fonte: Elaborada pela autora.

Figura 27 – Métodos eficazes para a conscientização sobre engenharia social



Fonte: Elaborada pela autora.

em escolas e empresas sobre ataques de engenharia social. Esses treinamentos podem incluir orientações práticas, como identificar links e anexos suspeitos, verificar a autenticidade de mensagens, manter sistemas atualizados e adotar uma postura crítica frente a informações que pareçam muito vantajosas. Além disso, disseminar informações e criar uma cultura de segurança digital são passos fundamentais para mitigar os riscos associados a essas práticas maliciosas.

82 dos participantes acredita que um meio de conscientizar as pessoas seria por meio de campanhas educativas em redes sociais, o que é um bom resultado visto que as redes sociais apresentam-se como uma ferramenta poderosa e eficaz para conscientizar a população sobre ataques de engenharia social. Com bilhões de usuários ativos diariamente, essas plataformas oferecem um alcance massivo e uma capacidade única de disseminar informações de maneira

rápida e acessível. Por meio de campanhas educativas, vídeos explicativos, infográficos e depoimentos de casos reais, é possível sensibilizar os usuários sobre as técnicas utilizadas por golpistas e como se proteger.

Além disso, o formato interativo das redes sociais permite que as pessoas compartilhem experiências, façam perguntas e se engajem em discussões sobre o tema, criando uma rede de apoio e aprendizado colaborativo. Iniciativas como *hashtags* temáticas, lives com especialistas e postagens periódicas podem manter o assunto em evidência e reforçar a importância de adotar práticas seguras no ambiente digital. 81 pessoas, afirmaram que uma maneira eficaz seria divulgação de informações na mídia, esta mídia vai além de redes sociais, o que facilitaria o acesso da maioria das pessoas às informações.

A última pergunta da quinta seção foi realizada uma pergunta aberta que buscava obter sugestões ou comentários sobre como melhorar a prevenção contra engenharia social. Dentre as sugestões obtidas podemos destacar:

> A divulgação constante sobre o tema é fundamental para a conscientização e prevenção contra esses ataques, que ocorrem muitas vezes devido à falta de atenção dos usuários. Manter campanhas educativas contínuas pode ajudar a reforçar a vigilância, tornando as pessoas mais atentas aos sinais de possíveis ameaças e reduzindo a probabilidade de serem vítimas de golpes. [1]

A sugestão está muito bem alinhada com o objetivo do trabalho, uma vez que a divulgação constante do tema é essencial para a prevenção de ataques de engenharia social. Para que essa conscientização seja realmente eficaz, uma boa estratégia seria a implementação de campanhas educativas contínuas dentro das organizações. Essas campanhas poderiam incluir treinamentos periódicos, simulações práticas de ataques, materiais informativos distribuídos regularmente e alertas sobre novas ameaças. Além disso, a criação de uma cultura de segurança, onde os colaboradores sintam-se encorajados a relatar atividades suspeitas e compartilhar boas práticas, ajudaria a reduzir significativamente os riscos. Dessa forma, a atenção dos usuários seria constantemente reforçada, tornando-os mais preparados para identificar e evitar possíveis tentativas de golpe. Outra sugestão dada foi que:

> Dar um foco maior a usuários com 60 anos ou mais é essencial, pois esse grupo representa a maioria das vítimas de ataques de engenharia social. Muitas dessas pessoas não cresceram em um ambiente digital e, por isso, podem ter maior dificuldade em identificar tentativas de fraude, tornando-se alvos frequentes de golpistas. [2]

[1] Entrevista de pesquisa concedida em 11/12/2024, na cidade de Itapajé-CE.
[2] Entrevista de pesquisa concedida em 11/12/2024, na cidade de Itapajé-CE.

Um ponto crucial que merece atenção especial é a vulnerabilidade de usuários com mais de 60 anos, que frequentemente são as principais vítimas de ataques de engenharia social. Muitas dessas pessoas não cresceram em um ambiente digital e, por isso, podem ter mais dificuldade em identificar fraudes e golpes online. Além disso, golpistas exploram a confiança natural desse público e utilizam abordagens persuasivas para enganá-los, seja por *e-mails* fraudulentos, chamadas telefônicas ou mensagens que aparentam ser legítimas. Com a análise de alguns dos resultados do questionário, pôde-se notar que os participantes de 56 anos ou mais todos já ouviram falar de engenharia social, mas apenas um demonstrou confiança sobre sua capacidade de reconhecer um ataque.

Para mitigar esse problema, é essencial que campanhas de conscientização incluam treinamentos específicos voltados para essa faixa etária. Esses treinamentos devem ser didáticos, acessíveis e apresentados de forma clara, com exemplos práticos e simulações de golpes reais para que os idosos aprendam a identificar sinais de fraudes. Além disso, materiais educativos como cartilhas impressas, vídeos explicativos e palestras presenciais podem ser eficazes para alcançar aqueles que têm menos familiaridade com tecnologias digitais.

Outro ponto importante é a participação ativa da família e das comunidades nessa prevenção. Incentivar filhos, netos e cuidadores a orientarem os idosos sobre segurança digital pode fortalecer ainda mais essa proteção. Além dessas sugestões ainda teve um participante que sugere:

> Ampla divulgação em TV e escolas é essencial para alcançar diferentes públicos e reforçar a conscientização sobre ataques de engenharia social. [3]

A sugestão do participante reforça o quanto a educação está diretamente ligada à diminuição do número de pessoas que caem em ataques como o de engenharia social, quanto mais conhecimento se tem sobre qualquer assunto mais facilidade as pessoas tem de lidar com ele quando necessário. A televisão, por ser um meio de comunicação amplamente acessível, especialmente para pessoas mais velhas, pode veicular campanhas educativas com explicações didáticas, simulações de golpes e depoimentos de especialistas, ajudando a tornar o tema mais compreensível.

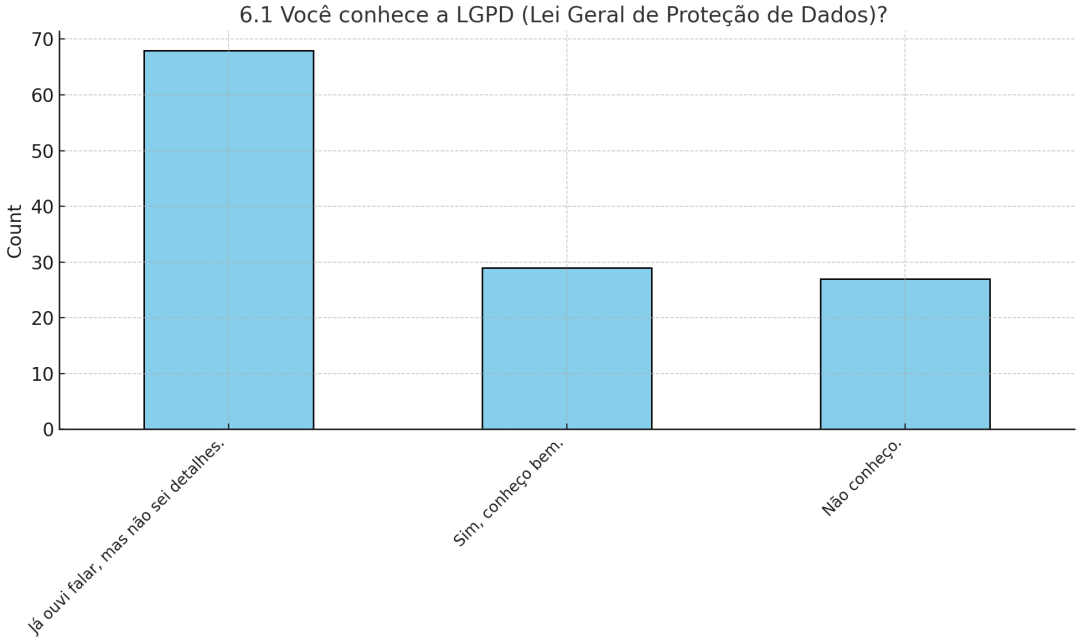
Já nas escolas, a inclusão de noções de segurança digital no currículo pode preparar as novas gerações para identificar tentativas de fraude desde cedo, tornando-as menos vulneráveis no futuro. Além disso, iniciativas como palestras, atividades interativas e a participação de

[3] Entrevista de pesquisa concedida em 11/12/2024, na cidade de Itapajé-CE.

especialistas em tecnologia podem reforçar o aprendizado e incentivar os alunos a compartilharem esse conhecimento com suas famílias, ampliando ainda mais o impacto da prevenção.

Na sexta e última seção do apêndice A, que continha sete perguntas, foi tratado do conhecimento dos direitos perante a lei em casos de ataques de engenharia social. Na primeira pergunta desta seção, foi questionado ao participante se ele já possui conhecimento da Lei Geral de Proteção de Dados a (LGPD). O gráfico da Figura 28 representa as respostas registradas. Conforme o gráfico, 68 dos participantes, já ouviu falar, mas não sabe de detalhes, a segunda maior parte com 29 pessoas diz já possuir conhecimento sobre a LGPD, e 27 pessoas afirmam nunca terem ouvido falar.

Figura 28 – Nível de conhecimento sobre a LGPD

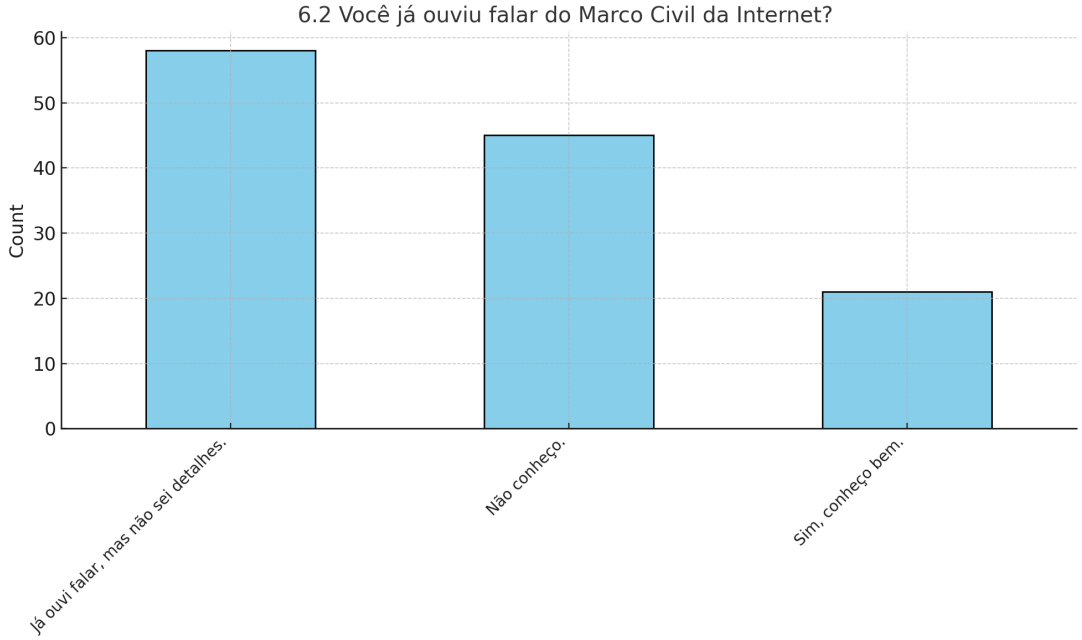


Fonte: Elaborada pela autora.

Os dados indicam que ainda há muitas pessoas que não conhecem a LGPD e algumas até ouviram falar mas não sabem para que servem, esse dado é extremamente preocupante uma vez que a LGPD é uma legislação fundamental que regula o tratamento de dados pessoais no Brasil, garantindo direitos como privacidade e segurança da informação. O fato de a maioria das pessoas não saberem para que serve a LGPD é preocupante por várias razões, dentre elas a vulnerabilidade à abusos, pois quando as pessoas desconhecem seus direitos garantidos pela LGPD, tornam-se mais suscetíveis a abusos por parte de empresas ou indivíduos que tratam seus dados de forma inadequada, como compartilhamento não autorizado ou coleta de informações sem consentimento, semelhante ao que acontece em casos de engenharia social, por exemplo. A

segunda questão por sua vez, pergunta sobre o conhecimento acerca do Marco Civil da Internet que é outro componente importante da legislação brasileira. O gráfico da Figura 29 representa os resultados obtidos.

Figura 29 – Nível de conhecimento sobre o Marco Civil da Internet



Fonte: Elaborada pela autora.

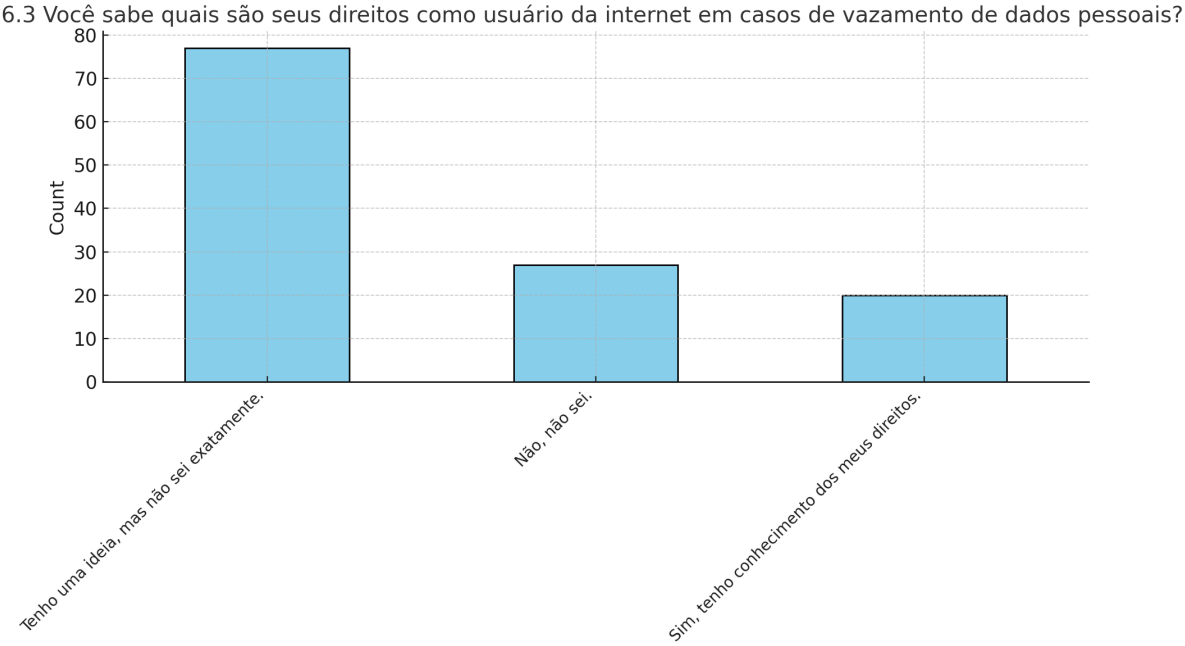
Segundo o analisado a partir da Figura 29, 58 pessoas afirmam já terem ouvido falar do Marco Civil da Internet mas não sabem dos detalhes, a segunda maioria com 45 pessoas, afirmam que não conhecem esta legislação, e apenas 21 pessoas do total de 124 participantes afirma ter conhecimento do Marco civil da internet. O desconhecimento do Marco Civil da Internet pode trazer diversas implicações negativas para essas pessoas, especialmente no contexto de seus direitos e deveres no ambiente digital. O uso de treinamentos sobre engenharia social em escolas e em outras organizações, deve levar em consideração também a apresentação de legislações como a LGPD e o Marco Civil da Internet, uma vez que ambos estão ligados a segurança digital dessas pessoas.

Quem não conhece os detalhes dessa legislação pode estar mais vulnerável a violações de privacidade, uso indevido de dados pessoais ou até mesmo à disseminação de informações falsas sem compreender suas responsabilidades legais. Além disso, essa falta de conhecimento dificulta o exercício da cidadania digital, como o entendimento sobre a neutralidade da rede, a liberdade de expressão e os mecanismos de proteção contra abusos online. Assim, o desconhecimento apontado pelos dados – em que apenas 21 de 124 participantes afirmam ter conhecimento

do Marco Civil da Internet – evidencia a necessidade de maior divulgação e educação sobre essa legislação fundamental para a convivência no meio digital.

A terceira pergunta realizada na seção está representada no gráfico da Figura 30. Os dados apontam que 77 participantes tem uma ideia, mas não sabem exatamente quais são seus direitos como usuários da internet em casos de vazamento de dados pessoais, 27 participantes apresentam não estarem confiantes sobre saberem seus direitos, e apenas 20 responderam que tem conhecimento dos seus direitos perante a lei. Os dados são muito preocupantes, pois expressam a grande desinformação das pessoas sobre seus próprios direitos como cidadãos, o que implica em uma série de negligências que poderiam ser evitadas com a maior exposição de assuntos como este.

Figura 30 – Nível de conhecimento sobre direitos dos participantes perante a lei



Fonte: Elaborada pela autora.

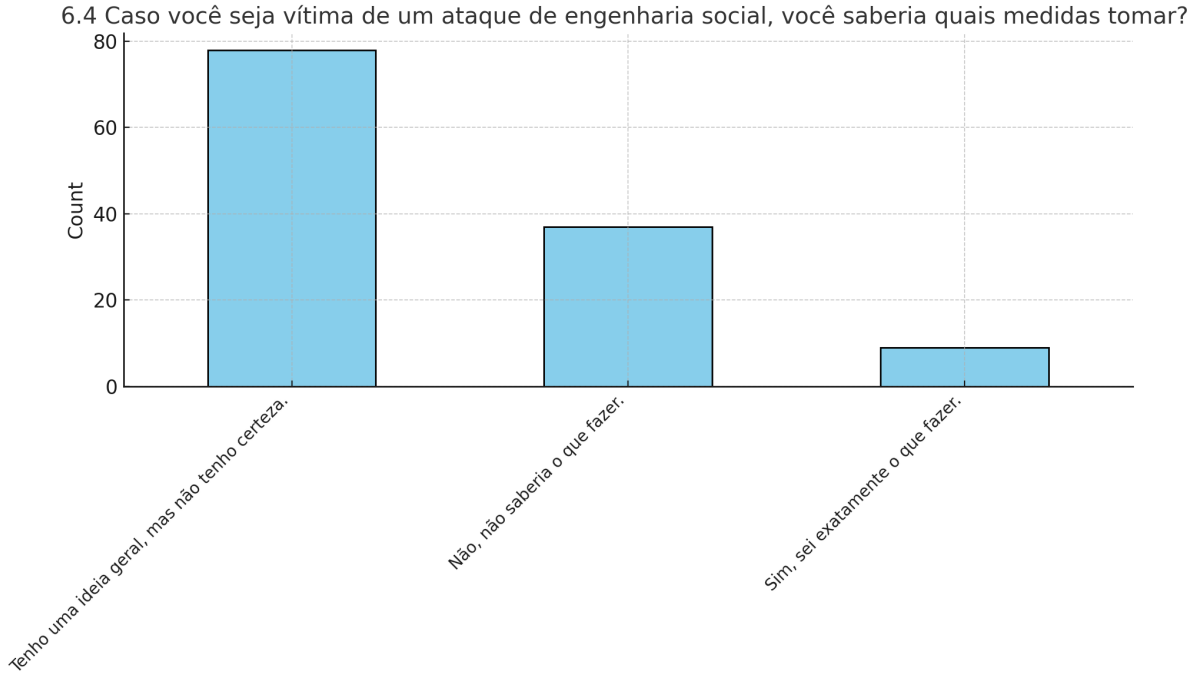
O gráfico da Figura 31 por sua vez, ira apresentar os dados a partir do questionamento ao participante se ele saberia quais medidas tomar em caso de ser vítima de um ataque de engenharia social. Dentre as respostas, a maioria composta por 78 participantes se diz incerto de quais medidas tomar, apesar de ter uma certa noção. 37 dos participantes dizem não saberem quais medidas devem ser tomadas frente a situação, e apenas 9 participantes dizem saberem exatamente quais medidas tomarem.

Os dados apresentam mais um resultado alarmante, o fato de muitas pessoas não saberem quais medidas tomar após serem vítimas de um ataque de engenharia social, uma prática

cada vez mais comum e sofisticada no mundo digital. A falta de informação sobre procedimentos básicos, como notificar autoridades competentes, alterar senhas de contas comprometidas, monitorar atividades financeiras ou buscar suporte especializado, deixa as vítimas desamparadas em um momento crítico. Além disso, muitas pessoas sequer têm consciência de que foram alvos de um ataque, o que impede qualquer reação inicial.

A pergunta representada no gráfico da Figura 32 também influência para ressaltar a urgência de promover a educação digital, conscientizando a população sobre os riscos da engenharia social e capacitando-a para lidar com possíveis incidentes, uma vez que ao questionado sobre conhecerem órgãos ou instituições aos quais se pode recorrer para denunciar um ataque de engenharia social a grande maioria composta por 66 participantes diz não saber a quem recorrer. A segunda maior parte com 41 participantes também demonstra incerteza apesar de ter uma ideia, e somente 17 dos participantes responderam saber onde encontrar ajuda.

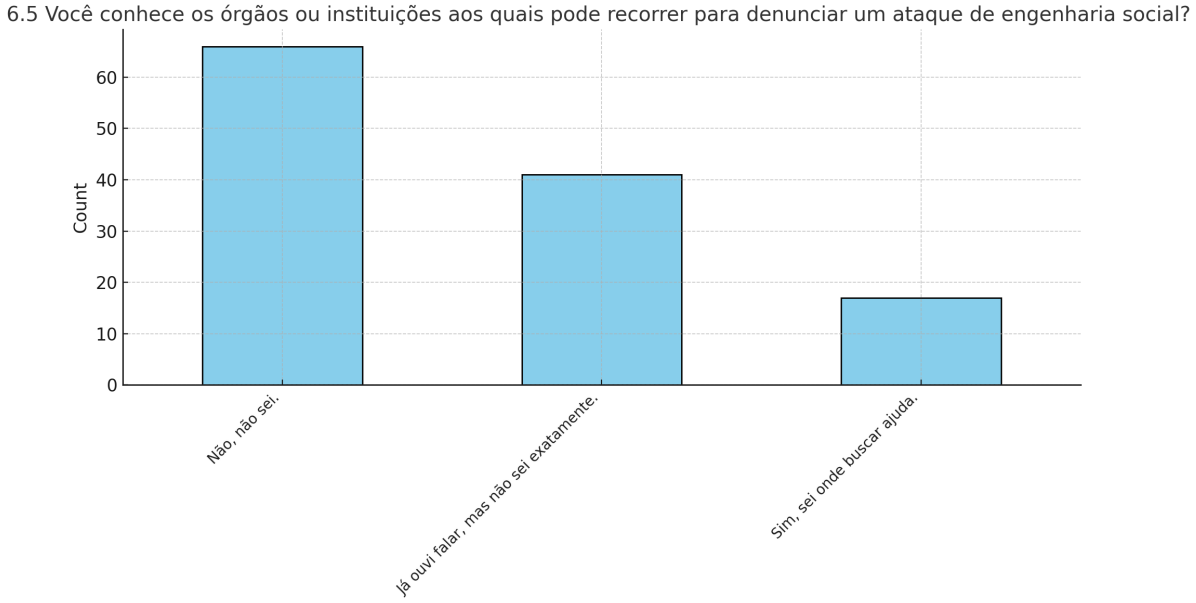
Figura 31 – Nível de conhecimento sobre direitos dos participantes perante a lei



Fonte: Elaborada pela autora.

Em seguida foi indagado ao participante se ele sabe como registrar um boletim de ocorrência em caso de crimes virtuais. O gráfico da Figura 33 apresenta que 49 dos participantes tem uma ideia mas não sabem exatamente como fazer, 42 participantes afirmam não saberem como realizar um boletim de ocorrência neste caso, e 33 dos participantes apresentam estarem cientes de como deve ser feito. Os dados se contradizem se comparados com a questão 6.4 em

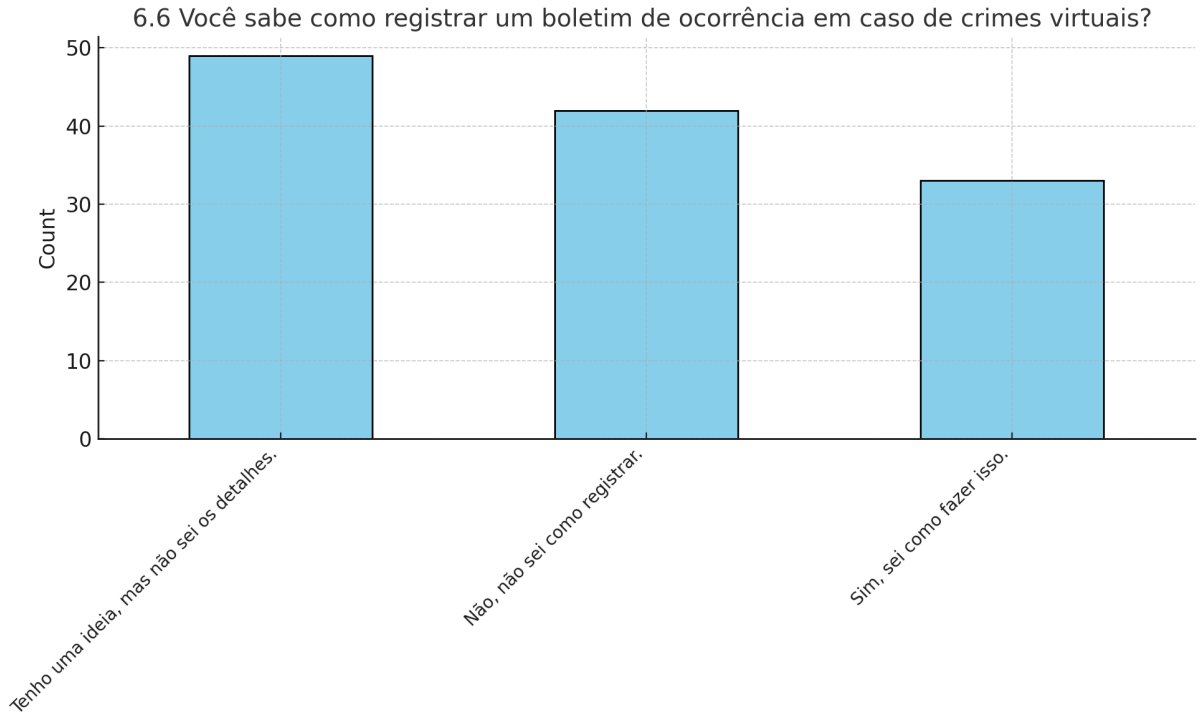
Figura 32 – Conhecimento sobre órgãos ou instituições para efetuar denúncias



Fonte: Elaborada pela autora.

que 78 dos participantes demonstraram incerteza sobre quais medidas tomarem frente a um ataque de engenharia social, que é um crime virtual em sua grande maioria.

Figura 33 – Conhecimento sobre realização de boletins de ocorrência frente a casos de crimes virtuais

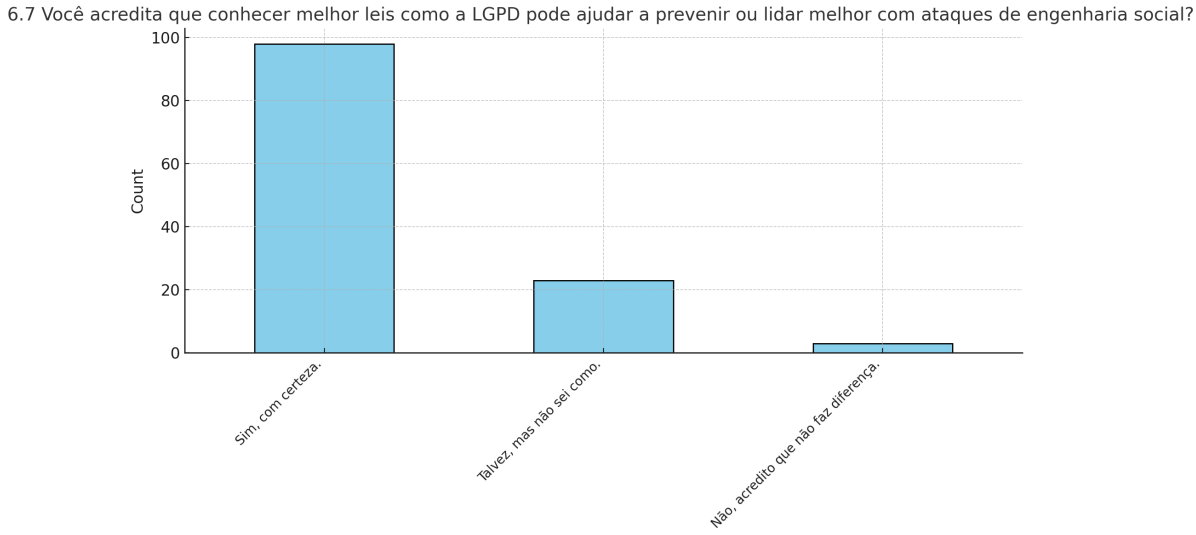


Fonte: Elaborada pela autora.

A última questão da seção, representada na Figura 34 apresenta os resultados obtidos

a partir do questionamento aos participantes quanto a opinião deles conhecer melhor leis como a LGPD como forma de ajuda na prevenção de ataques de engenharia social. Como pode ser observado na figura a grande maioria dos participantes, sendo de 98 pessoas acredita que sim, com certeza isso ajudaria a lidar melhor com ataques de engenharia social. 23 participantes acreditam que talvez seja útil mas não sabem como, e 3 dos participantes acreditam que não faria diferença.

Figura 34 – Opinião dos participantes sobre conhecer melhor leis como método de prevenção



Fonte: Elaborada pela autora.

Dentre os dados obtidos por meio do questionário foi possível identificar que embora a maioria dos participantes possuísse ensino médio completo ou estivesse cursando o ensino superior, os conhecimentos gerais sobre ataques de engenharia social, crimes virtuais e a legislação que protege os direitos das vítimas foram alarmantemente baixos. Essa disparidade sugere que há uma significativa lacuna de informações nas instituições de ensino, o que pode dificultar a conscientização e a capacitação dos indivíduos para enfrentar tais situações. Mesmo entre os participantes que afirmaram ser capazes de identificar um ataque de engenharia social com facilidade, muitos confessaram não saber como buscar ajuda caso fossem vítimas, o que evidencia um problema crítico: o conhecimento teórico não está sendo acompanhado por orientações práticas sobre como agir diante desses crimes.

O fato que um terço dos participantes nunca ouviu falar sobre o assunto e a maioria possui apenas um entendimento superficial evidencia a necessidade urgente de campanhas educativas e treinamentos mais acessíveis. Sem essa conscientização, os indivíduos permanecem vulneráveis a golpes e manipulações, o que pode ter consequências sérias tanto no nível pessoal

quanto organizacional. Isso reforça a importância de investir em estratégias eficazes de educação em segurança digital, tornando o conhecimento sobre engenharia social uma prioridade e não um tema secundário.

Com a pesquisa, foi observado que, embora jovens adultos (19 a 25 anos) tenham sido o grupo com maior representatividade na pesquisa, sua percepção de segurança nem sempre reflete uma proteção efetiva contra esses ataques. Muitos demonstraram excesso de confiança em sua capacidade de reconhecer tentativas de engenharia social, o que pode levar a falhas na adoção de medidas preventivas adequadas. Isto sugere que, mesmo entre aqueles que cresceram em um ambiente digital, a conscientização sobre segurança ainda precisa ser reforçada.

Outro ponto relevante é a disparidade na experiência pessoal com ataques de engenharia social. Enquanto os mais jovens tendem a subestimar sua exposição, muitos participantes mais velhos relataram já terem sido vítimas, muitas vezes sem sequer perceberem a natureza do ataque. Isso reforça a necessidade de estratégias de conscientização personalizadas, que levem em consideração tanto a idade quanto o nível de experiência digital do indivíduo.

Os dados obtidos indicam que, apesar de a maioria dos participantes possuírem ensino médio completo ou estarem cursando o ensino superior, os conhecimentos sobre ataques de engenharia social, crimes virtuais e legislações de proteção de dados ainda são alarmantemente baixos. O que indica que a formação acadêmica, por si só, não garante a capacitação necessária para identificar e lidar com esses tipos de ameaças, evidenciando a lacuna na abordagem educacional sobre segurança digital. Mesmo entre os participantes com ensino superior incompleto ou completo, muitos não sabiam como proceder caso fossem vítimas de um ataque, demonstrando que o conhecimento teórico não está sendo acompanhado por orientações práticas.

Diante disso, se torna evidente que a escolaridade influencia a suscetibilidade a ataques de engenharia social, mas não de forma linear. O simples fato de possuir um nível educacional mais elevado não garante uma proteção eficaz se o conhecimento sobre segurança digital não for enfatizado durante a formação acadêmica. Portanto, é essencial haver esforços para incluir treinamentos práticos e campanhas de conscientização nas instituições de ensino e no ambiente corporativo, garantindo que as pessoas tenham acesso não apenas à teoria, mas também às ferramentas necessárias para se protegerem de ameaças digitais.

5 CONCLUSÕES E TRABALHOS FUTUROS

O estudo realizado sobre engenharia social: Um Estudo sobre o Nível de Conhecimento e Suscetibilidade em Diferentes Faixas Etárias buscou analisar o nível de conscientização e a vulnerabilidade de indivíduos frente a ataques de engenharia social, considerando diferentes faixas etárias e níveis de escolaridade. A pesquisa foi conduzida por meio de um estudo bibliográfico e a aplicação de um formulário aos residentes da cidade de Itapajé, Ceará. Os resultados obtidos revelaram uma série de *insights* importantes sobre o conhecimento, as práticas e as atitudes dos participantes em relação à segurança da informação, especialmente no que diz respeito à engenharia social.

Os resultados deste estudo têm implicações importantes para a segurança da informação, tanto no âmbito pessoal quanto organizacional. A falta de conhecimento e conscientização sobre engenharia social, combinada com a ausência de treinamentos e orientações adequadas, cria um ambiente propício para o sucesso desses ataques. Portanto, é fundamental que instituições educacionais, empresas e órgãos governamentais invistam em programas de educação e conscientização, especialmente voltados para grupos mais vulneráveis, como idosos e pessoas com menor familiaridade com tecnologias digitais.

Além disso, a integração de temas relacionados à segurança da informação nos currículos escolares e universitários pode ajudar a preparar as novas gerações para identificar e evitar ataques de engenharia social desde cedo. Campanhas educativas em redes sociais, mídia e televisão também podem ser eficazes para alcançar um público mais amplo e reforçar a importância de práticas seguras no ambiente digital.

Este estudo abre caminho para pesquisas futuras que possam explorar outras dimensões da engenharia social, como o impacto de diferentes técnicas de ataque em grupos específicos (por exemplo, idosos, crianças, profissionais de determinadas áreas) e a eficácia de diferentes métodos de conscientização e treinamento. Além disso, seria interessante investigar como as mudanças tecnológicas e o surgimento de novas plataformas digitais podem influenciar as táticas utilizadas pelos engenheiros sociais e como os usuários podem se adaptar a essas mudanças.

Outra área de pesquisa relevante seria a análise do impacto da legislação de proteção de dados, como a LGPD, na redução de ataques de engenharia social. Seria importante avaliar se a maior conscientização sobre os direitos dos usuários e as obrigações das empresas em relação ao tratamento de dados pessoais tem contribuído para a diminuição desses crimes.

Em suma, este estudo evidenciou que a falta de conhecimento, a ausência de treina-

mentos e a desinformação sobre direitos legais são fatores que contribuem para a vulnerabilidade dos indivíduos. Portanto, é essencial que haja um esforço conjunto entre governos, instituições educacionais, empresas e a sociedade civil para promover a educação e a conscientização sobre os riscos da engenharia social, capacitando os usuários a se protegerem contra essas ameaças e a agirem de forma proativa em caso de incidentes. Somente com uma abordagem multifacetada e contínua será possível reduzir a incidência desses ataques e garantir um ambiente digital mais seguro para todos.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Engenharia Social: Guia para Proteção de Conhecimentos Sensíveis**. [S.l.], 2021. A reprodução desta cartilha é autorizada, desde que citada a fonte. Disponível em: <https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis>.

ALEROUD, A.; ZHOU, L. Phishing environments, techniques, and countermeasures: A survey. **Computers & Security**, Elsevier, v. 68, p. 160–196, 2017. Acesso em: 3 out. 2024. Disponível em: <https://doi.org/10.1016/j.cose.2017.04.005>.

ALVES, C. B. **Segurança da Informação vs. Engenharia Social: Como se Proteger para Não Ser Mais uma Vítima**. 2. ed. Brasília: Clube de Autores, 2010. Acesso em: 15 out. 2024. Disponível em: <https://clubedeautores.com.br/livro/seguranca-da-informacao-vs-engenharia-social>.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Nbr iso/iec 17799: Tecnologia da informação – código de prática para gestão da segurança da informação. **ABNT**, 2005. Acesso em: 12 nov. 2024. Rio de Janeiro. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=2902>.

BUGHUNT. **O que é engenharia social?** 2022. Acessado em: 07 fev. 2025. Disponível em: <https://blog.bughunt.com.br/o-que-e-engenharia-social/>.

Casa do Desenvolvedor. **Baiting em Cibersegurança: Como Reconhecer e Evitar Armadilhas Digitais**. 2023. Acessado em: 30 jan. 2025. Disponível em: <https://forum.casadodesenvolvedor.com.br/topic/47082-baiting-em-ciberseguran%C3%A7a-como-reconhecer-e-evitar-armadilhas-digitais/>.

CASTRO, R. C. C.; SOUSA, V. L. P. Segurança em cloud computing: Governança e gerenciamento de riscos de segurança. In: **III Congresso Tecnológico de TI e Telecom InfoBrasil**. [s.n.], 2010. Acesso em: 18 out. 2024. Disponível em: <https://example.com>.

CHETIOUI, K.; BAH, B.; ALAMI, A. O.; BAHNASSE, A. Overview of social engineering attacks on social networks. **Procedia Computer Science**, Elsevier, v. 198, p. 656–661, 2022. Acesso em: 15 nov. 2024. Disponível em: <https://doi.org/10.1016/j.procs.2021.12.302>.

CHIEW, K. L.; YONG, K. S. C.; TAN, C. L. A survey of phishing attacks: Their types, vectors and technical approaches. **Expert Systems with Applications**, Elsevier, v. 106, p. 1–20, 2018. Acesso em: 5 jan. 2025. Disponível em: <https://doi.org/10.1016/j.eswa.2018.03.050>.

Claranet. **Engenharia social: o que é e como se proteger**. 2024. Acessado em: 07 fev. 2025. Disponível em: <https://www.claranet.com/br/blog/engenharia-social-o-que-e-e-como-se-proteger>.

COELHO, C. F.; RASMA, E. T.; MORALES, G. Engenharia social: uma ameaça à sociedade da informação. **Exatas & Engenharias**, Institutos Superiores de Ensino do Censa, v. 3, n. 05, 2013. Acesso em: 8 abr. 2024. Disponível em: <https://ojs3.perspectivasonline.com.br/exatas_e_engenharia/article/view/87>.

EIRAS, M. Engenharia social e estelionato eletrônico (monografia (conclusão de curso–lato sensu)). **IBPINET–The internet school e Uni-Rio, Graduação em Segurança da**

Informação na Internet, São Paulo: FGV, 2004. Acesso em: 8 jun. 2024. Disponível em: <https://www.perspectivasonline.com.br/exatas_e_engenharia/article/download/87/59/246.>

FILHO, A. M. S. Entendendo e evitando a engenharia social: Protegendo sistemas e informações. **Revista Espaço Acadêmico**, v. 4, n. 43, dez. 2004. Acesso em: 22 jul. 2012. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm>.

FONSECA, M. **Engenharia Social: Conscientizando o Elo Mais Fraco da Segurança da Informação**. Trabalho de Conclusão de Curso (Pós-Graduação em Especialização em Inteligência em Segurança Pública) — Universidade do Sul de Santa Catarina, Brasília, 2017. Acesso em: 25 mar. 2023. Disponível em: <https://repositorio.animaeducacao.com.br/bitstreams/70e3c981-fab3-40a5-a68c-c64f7f59de78/download>.

FORTINET. **Pretexting**. 2025. Acesso em: 30 jan. 2025. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/pretexting>.

GASPAR, J. E. H. M. **Análise Comportamental sobre Ataques de Engenharia Social**. 77f p. Dissertação (Mestrado em Engenharia Informática) — Escola Superior de Tecnologia e Gestão, 2015. Acesso em: 16 abr. 2024. Disponível em: <https://recipp.ipp.pt/bitstream/10400.22/11096/1/DM_JanaGaspar_MEI_2015.pdf>.

GOMES, L. P. Análise da implementação de treinamentos internos de segurança da informação em conformidade com a lgpd e governança de ti: um estudo de caso. 182, 2023.

HADNAGY, C.; MAXWELL, E. **Social Engineering Defined: Social Engineering Framework**. 2009. Acesso em: 05 abr. 2023. Disponível em: <http://www.socialengineer.org/framework/Social_Engineering_Defined>.

IBM. **O que é pretexting?** 2024. Acessado em: 29 jan. 2025. Disponível em: <https://www.ibm.com/br-pt/topics/pretexting>.

ISO/IEC. **IEC 17799–Tecnologia da informação—Técnicas de segurança—Código de prática para a gestão da segurança da informação**. [S.l.]: ABNT, 2005.

KAVLAC, M. **Conheça os 3 pilares da segurança da informação**. 2023. Acessado em: 24 de janeiro de 2025. Disponível em: <https://psycurity.com.br/conheca-os-3-pilares-da-seguranca-da-informacao/>.

LAFRANCE, Y. Psychology: A precious security tool. **SANS Institute**, p. 27, 2004.

LOHANI, S. Social engineering: Hacking into humans. **International Journal of Advanced Studies of Scientific Research**, v. 4, n. 1, 2019.

LYRA, M. R. Governança da segurança da informação. **Brasília: nd**, 2015. Acesso em: 10 out. 2024. Disponível em: <https://www.amazon.com.br/Governan%C3%A7a-Seguran%C3%A7a-Informa%C3%A7%C3%A3o-Mauricio-Rocha-ebook/dp/B018KED8XS>.

LYRA, M. R. *et al.* Segurança e auditoria em sistemas de informação. **Rio de Janeiro: Ciência Moderna**, p. 20, 2008. Acesso em: 9 out. 2024. Disponível em: <https://www.amazon.com.br/Seguran%C3%A7a-Auditoria-em-Sistemas-Informa%C3%A7%C3%A3o/dp/8573937475>.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar**. 1. ed. São Paulo: Pearson, 2004.

OLIVO, C. K. **Avaliação de características para detecção de phishing de email**. Dissertação (Dissertação (Mestrado)) — Pontifícia Universidade Católica do Paraná, Curitiba, 2010.

OLLMANN, G. **The Phishing Guide – Understanding & Preventing Phishing Attacks**. 2024. <https://www.pt.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems>. Acesso em: 16 fev. 2025.

OOSTERLOO, B. **Managing Social Engineering Risk: Making Social Engineering Transparent**. 130f p. Dissertação (Master in Industrial Engineering and Management) — University of Twente, Enschede, Netherlands, 2008.

PEIXOTO, M. C. P. Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas organizações. **Monografia (Bacharelado)–Curso de Ciência da Computação–Pró-Reitoria de Ensino de Graduação do Centro Universitário do Triângulo. Uberlândia: Unitri**, p. 24, 2004.

PEREIRA, L. A. de S.; VICENTINE, A. L.; RIZO, A. C. Impactos da engenharia social na segurança da informação. **Revista Brasileira em Tecnologia da Informação**, v. 4, n. 1, p. 48–58, 2022.

Phishing.org. **History of phishing**. 2012. Acesso em: 24 abr. 2024. Disponível em: <http://www.phishing.org/historyof-phishing>.

PIOVESAN, L. G.; SILVA, E. R. C.; SOUSA, J. F. de; TURIBUS, S. N. Engenharia social: Uma abordagem sobre phishing. **REVISTA CIENTÍFICA UNIBALSAS**, v. 10, n. 1, p. 45–59, 2019. Acesso em: 22 jul. 2022. Disponível em: <https://revista.unibalsas.edu.br/index.php/unibalsas/article/view/94/87>.

PROOFPOINT. **O que é phishing? Definição, história e mais**. 2022. Acessado em: 24 de janeiro de 2025. Disponível em: <https://www.proofpoint.com/br/threat-reference/phishing>.

RAMZAN, Z. Phishing attacks and countermeasures. **Handbook of information and communication security**, Springer, p. 433–448, 2010. Acesso em: 24 abr. 2023. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-642-04117-4_23>.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. **Future internet**, MDPI, v. 11, n. 4, p. 89, 2019.

SlashNext. **The Human Hacking Report**. 2024. Acessado em: 07 fev. 2025. Disponível em: <https://slashnext.com/the-human-hacking-report/>.

SêMOLA, M. **Curso de educação continuada: gestão de segurança da informação**. [s.l.]: [s.n.], 2006. Acesso em: 9 jan. 2025. Disponível em: <https://example.com>.

THREATLABZ, Z. **Phishing attacks rise 58% year-over-year, AI drives new threats**. 2024. Accessed: 2025-02-06. Disponível em: <https://www.zscaler.com/br/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report>.

TIESO, I. H. de S.; SANTO, F. do E. Ataques de engenharia social. **Revista Interface Tecnológica**, v. 17, n. 2, p. 206–218, 2020.

VENKATESHA, S.; REDDY, K. R.; CHANDAVARKAR, B. R. Social engineering attacks during the covid-19 pandemic. **SN Computer Science**, Springer, v. 2, p. 78, 2021. Acessado em: 29 jan. 2025. Disponível em: <https://link.springer.com/article/10.1007/s42979-020-00443-1>.

ZAGER, M. Who are the hackers? **Infosec News**, 2002. Acesso em: 25 mar. 2022. Disponível em: <https://seclists.org/isn/2002/Sep/78>.

APÊNDICE A – QUESTIONÁRIO: UM ESTUDO SOBRE ENGENHARIA SOCIAL

Prezado(a) participante,

Este questionário faz parte de uma pesquisa realizada para o Trabalho de Conclusão de Curso (TCC) intitulado "Engenharia Social: Um Estudo sobre o Nível de Conhecimento e Suscetibilidade em Diferentes Faixas Etárias", conduzido por Marilene Santos Duarte, aluna do curso de Segurança da Informação, sob a orientação do Prof. Dr. João Henrique Gonçalves Medeiros Corrêa, no Campus de Itapajé.

O objetivo desta pesquisa é analisar o nível de conhecimento das pessoas sobre engenharia social, compreender o comportamento dos usuários diante de ataques desse tipo e formular estratégias eficazes de prevenção e conscientização. Suas respostas são essenciais para a obtenção de dados relevantes que apoiarão a elaboração de diretrizes e recomendações práticas para melhorar a segurança contra ataques como *phishing, pretexting, baiting*, entre outros, que utilizam técnicas de engenharia social.

Agradecemos sua participação e garantimos que todas as informações fornecidas serão tratadas de forma confidencial e anônima.

Muito obrigado(a)!

++

O participante da pesquisa terá um questionário contendo questões sobre dados demográficos, conhecimento e experiência com ataques de engenharia social, comportamento e atitude, percepção e conhecimento, educação e conscientização, opiniões adicionais de um projeto de pesquisa intitulado "Engenharia Social: Um Estudo sobre o Nível de Conhecimento e Suscetibilidade em Diferentes Faixas Etárias", conduzido por Marilene Santos Duarte sob a orientação do Prof. Dr. João Henrique Gonçalves Medeiros Corrêa no Campus de Itapajé. O objetivo é analisar o conhecimento a cerca de ataques de engenharia social a fim de desenvolver estratégias de prevenção e conscientização. Se você aceitar participar, será solicitado a responder a um questionário online sobre seu conhecimento e comportamento em relação a engenharia social. A participação é voluntária, confidencial e anônima, podendo ser interrompida a qualquer momento. Para dúvidas ou mais informações, entre em contato com a pesquisadora através do email: Marilenesantosduarte@alu.ufc.br. Ao assinar este termo, você concorda em participar do estudo.

- Seção 0: Concordo em participar da pesquisa

☐ Li o Termo de Consentimento Livre e Esclarecido (TCLE) e aceito responder.

- Seção 1: Informações pessoais

Questão 1. 1.1. Idade:

(a) 15-18 anos

(b) 19-25 anos

(c) 26-35 anos

(d) 36-45 anos

(e) 46-55 anos

(f) 56 anos ou mais

Questão 2. 1.2. Gênero:

(a) Masculino

(b) Feminino

(c) Prefiro não dizer

(d) Outros

Questão 3. 1.3. Nível de Escolaridade:

(a) Ensino Fundamental incompleto

(b) Ensino Fundamental completo

(c) Ensino Médio incompleto

(d) Ensino Médio completo

(e) Ensino Superior incompleto

(f) Ensino Superior completo

(g) Nenhuma das alternativas

- Seção 2: Conhecimento sobre engenharia social

Questão 4. 2.1. Você já ouviu falar sobre o termo "engenharia social"?

(a) Sim

(b) Não

Questão 5. 2.2. Você acredita que já foi vítima de algum ataque de engenharia social?

(a) Sim, tenho certeza.

(b) Talvez, não tenho certeza

(c) Não, nunca fui vítima

Questão 6. 2.3. Se você respondeu "sim"à pergunta anterior, qual foi o tipo de ataque?

(a) *Phishing* (mensagens fraudulentas pedindo informações pessoais ou financeiras).

(b) *Pretexting* (situações onde alguém se faz passar por outra pessoa para obter informações).

(c) *Baiting* (ofertas falsas que atraem vítimas com algo de interesse, como downloads gratuitos).

(d) Não sei identificar.

(e) Outros

Questão 7. 2.4. Na sua opinião, o quanto você sabe sobre engenharia social?

(a) Nada, nunca ouvi falar.

(b) Muito pouco, conheço de forma superficial.

(c) Um pouco, sei identificar alguns ataques.

(d) Bastante, consigo reconhecer a maioria dos ataques.

(e) Muito, tenho amplo conhecimento sobre o tema.

- Seção 3: Como lida com a situação

Questão 8. 3.1. Com que frequência você verifica se um link ou mensagem é confiável antes de clicar ou responder?

(a) Sempre

(b) Às vezes

(c) Raramente

(d) Nunca

Questão 9. 3.2. Na sua rotina, qual é a principal fonte de ataques que você acredita estar exposto(a)?

☐ E-mails suspeitos

☐ Mensagens em redes sociais

☐ Links em sites desconhecidos

☐ Ligações telefônicas fraudulentas

☐ Outros

Questão 10. 3.3. Você já recebeu algum treinamento ou orientação sobre como evitar ataques de engenharia social?

(a) Sim

(b) Não

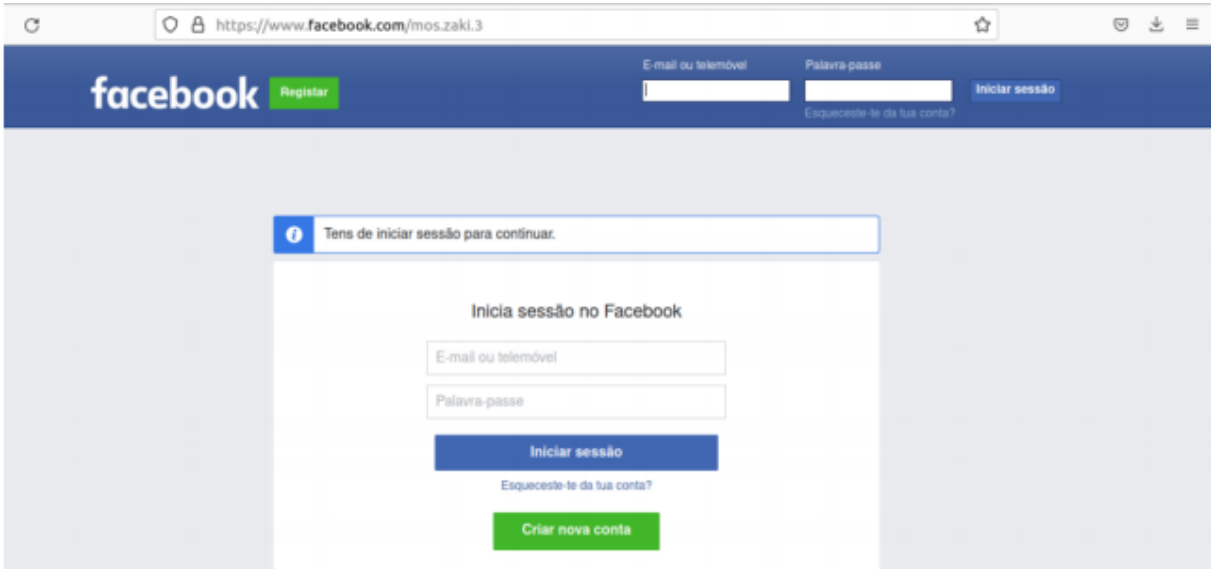
- Seção 4: Percepção de ataques de engenharia social

Questão 11. 4.1 Você acredita que pode identificar um e-mail de *phishing* facilmente?

(a) Sim

(b) Não

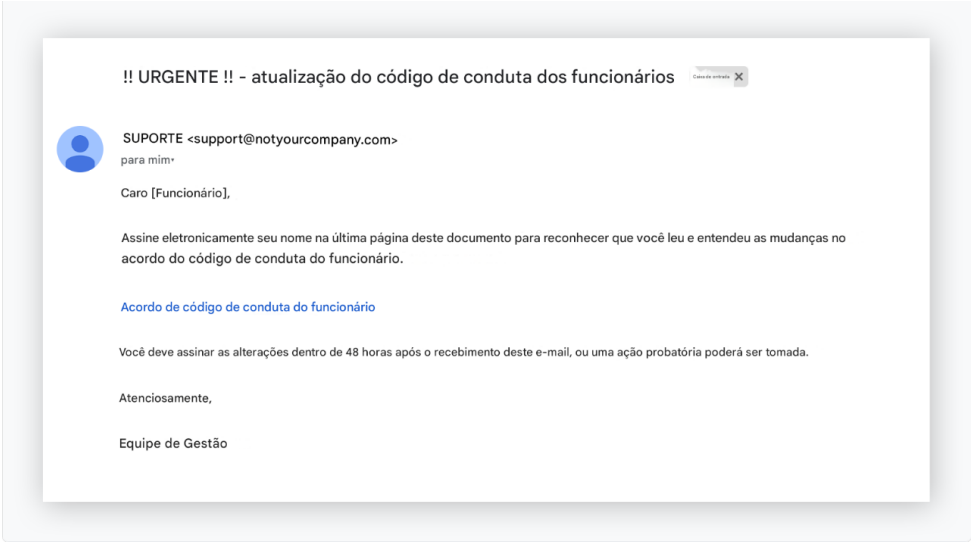
Questão 12. 4.2 O Facebook é uma das redes sociais mais populares e acessadas globalmente. Ao analisar cuidadosamente a imagem e os elementos visuais disponíveis, há algum sinal que sugira que este site possa ser falso ou representar um risco para a segurança na transmissão de dados?



(a) Sim

(b) Não

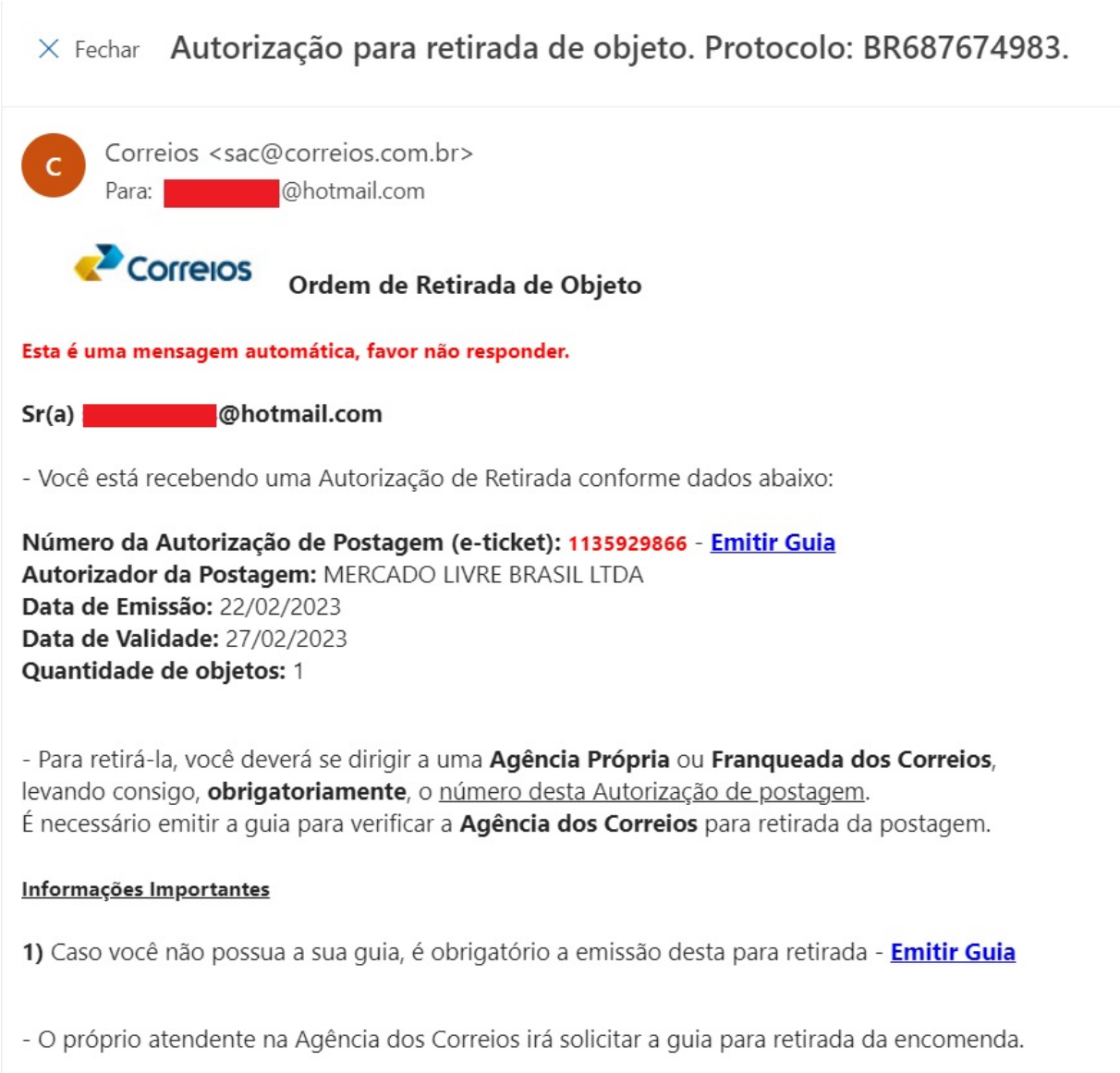
Questão 13. 4.3 Ao analisar o e-mail recebido abaixo, é possível identificar algum sinal que indique ser um possível ataque de phishing, pretexting, Baiting ou outro?



(a) Sim

(b) Não

Questão 14. 4.4 Ao receber um e-mail como mostra a imagem, o que você faz?



Fechar Autorização para retirada de objeto. Protocolo: BR687674983.

C Correios <sac@correios.com.br>
Para: [redacted]@hotmail.com

Correios **Ordem de Retirada de Objeto**

Esta é uma mensagem automática, favor não responder.

Sr(a) [redacted]**@hotmail.com**

- Você está recebendo uma Autorização de Retirada conforme dados abaixo:

Número da Autorização de Postagem (e-ticket): 1135929866 - **Emitir Guia**
Autorizador da Postagem: MERCADO LIVRE BRASIL LTDA
Data de Emissão: 22/02/2023
Data de Validade: 27/02/2023
Quantidade de objetos: 1

- Para retirá-la, você deverá se dirigir a uma **Agência Própria** ou **Franqueada dos Correios**, levando consigo, **obrigatoriamente**, o número desta Autorização de postagem.
É necessário emitir a guia para verificar a **Agência dos Correios** para retirada da postagem.

Informações Importantes

1) Caso você não possua a sua guia, é obrigatório a emissão desta para retirada - **Emitir Guia**

- O próprio atendente na Agência dos Correios irá solicitar a guia para retirada da encomenda.

☐ Ignora

☐ Clica no link para conferir

☐ Bloqueia o remetente

☐ Relata o e-mail

☐ Verifica com a fonte

☐ Baixa o anexo

☐ Outros

Questão 15. 4.5 O que você acha que torna um ataque de engenharia social convincente?

☐ Linguagem persuasiva

☐ Uso de logotipos oficiais

☐ Sensação de urgência

☐ Oferta de recompensas ou prêmios

☐ Outros

Questão 16. 4.6 Você se sente confiante em sua capacidade de evitar ser enganado por engenharia social?

(a) Muito confiante

(b) Confiante

(c) Neutro

(d) Pouco confiante

(e) Nada confiante

Questão 17. 4.7 Em sua opinião, qual é o fator mais importante que contribui para a vulnerabilidade aos ataques que utilizam engenharia social?

☐ Falta de conhecimento

☐ Falta de atenção

☐ Confiança excessiva

☐ Pressão social

☐ Outros

- Seção 5: Conscientização

Questão 18. 5.1 Você acredita que ataques de engenharia social são um risco real para a segurança online?

(a) Sim

(b) Não

(c) Não sei

Questão 19. 5.2 Na sua opinião, qual é a melhor maneira de evitar ser vítima de ataques de engenharia social?

☐ Não clicar em links ou anexos suspeitos

☐ Confirmar a autenticidade de mensagens diretamente com o remetente.

☐ Manter softwares e sistemas atualizados.

☐ Outros

Questão 20. 5.3 Você acredita que conscientizar as pessoas sobre engenharia social pode reduzir significativamente a ocorrência desses ataques?

(a) Sim

(b) Não

(c) Não sei

Questão 21. 5.4 Qual medida você considera mais eficaz para conscientizar as pessoas sobre ataques de engenharia social?

☐ Campanhas educativas em redes sociais.

☐ Treinamentos em escolas ou empresas.

☐ Divulgação de informações na mídia.

☐ Outros

Questão 22. 5.5 Você tem alguma sugestão ou comentário sobre como melhorar a prevenção contra ataques de engenharia social? _____

- Seção 6: Conhecimento dos direitos perante a lei em caso de ataques

Questão 23. 6.1 Você conhece a LGPD (Lei Geral de Proteção de Dados)?

(a) Sim, conheço bem.

(b) Já ouvi falar, mas não sei detalhes.

(c) Não conheço.

Questão 24. 6.2 Você já ouviu falar do Marco Civil da Internet?

(a) Sim, conheço bem.

(b) Já ouvi falar, mas não sei detalhes.

(c) Não conheço.

Questão 25. 6.3 Você sabe quais são seus direitos como usuário da internet em casos de vazamento de dados pessoais?

(a) Sim, tenho conhecimento dos meus direitos.

(b) Tenho uma ideia, mas não sei exatamente.

(c) Não, não sei.

Questão 26. 6.4 Caso você seja vítima de um ataque de engenharia social, você saberia quais medidas tomar?

(a) Sim, sei exatamente o que fazer.

(b) Tenho uma ideia geral, mas não tenho certeza.

(c) Não, não saberia o que fazer.

Questão 27. 6.5 Você conhece os órgãos ou instituições aos quais pode recorrer para denunciar um ataque de engenharia social?

(a) Sim, sei onde buscar ajuda.

(b) Já ouvi falar, mas não sei exatamente.

(c) Não, não sei.

Questão 28. 6.6 Você sabe como registrar um boletim de ocorrência em caso de crimes virtuais?

(a) Sim, sei como fazer isso.

(b) Tenho uma ideia, mas não sei os detalhes.

(c) Não, não sei como registrar.

Questão 29. 6.7 Você acredita que conhecer melhor leis como a LGPD pode ajudar a prevenir ou lidar melhor com ataques de engenharia social?

(a) Sim, com certeza

(b) Talvez, mas não sei como.

(c) Não, acredito que não faz diferença.

- Muito obrigado por participar deste questionário!