

UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE ITAPAJÉ

CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

LÍVIA MARIA MOTA BRANDÃO

PSICOLOGIA POR TRÁS DOS ATAQUES DE ENGENHARIA SOCIAL

ITAPAJÉ

2025

LÍVIA MARIA MOTA BRANDÃO

PSICOLOGIA POR TRÁS DOS ATAQUES DE ENGENHARIA SOCIAL

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

Orientador: Prof. Dr. Israel Eduardo de Barros Filho

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)

B818p Brandão, Lívia Maria Mota.
Psicologia por trás dos ataques de Engenharia social / Lívia Maria Mota Brandão. – 2025.
50 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. Israel Eduardo de Barros Filho.

1. Engenharia social. 2. Psicologia. 3. Segurança da informação. 4. Ataques. I. Título.
CDD 005.8

LÍVIA MARIA MOTA BRANDÃO

PSICOLOGIA POR TRÁS DOS ATAQUES DE ENGENHARIA SOCIAL

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

Aprovada em: 27/02/2025.

BANCA EXAMINADORA

_____
Prof. Dr. Israel Eduardo de Barros Filho (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Aminadabe Barbosa de Sousa
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Juan Sebastian Toquica Arenas
Universidade Federal do Ceará (UFC)

Dedico este trabalho a Deus, que me sustentou em cada desafio, e à minha família, que sempre acreditou em mim.

"O Senhor é a minha força e o meu escudo; nele o meu coração confia, e dele recebo ajuda." (Salmos 28:7)"

AGRADECIMENTOS

Ao concluir esta etapa tão importante da minha vida, não poderia deixar de expressar minha gratidão a todos que, de alguma forma, contribuíram para o conhecimento adquirido e para a realização deste trabalho.

Em primeiro lugar, minha gratidão a Deus, por ser minha fortaleza e refúgio em todos os momentos. Sem Ele, nada disso seria possível. Em cada dificuldade, encontrei forças n'Ele para seguir em frente, e em cada conquista, reconheci Sua graça e fidelidade. Agradeço por me guiar, por renovar minhas energias quando o cansaço e a dúvida tentaram me desmotivar, e por me conceder sabedoria para concluir esta jornada com êxito.

À minha família, meu alicerce, meu porto seguro, que sempre esteve ao meu lado, me encorajando, acreditando em mim e celebrando cada pequena vitória ao longo dessa caminhada. À minha mãe, Márcia, exemplo de amor, dedicação e força, que com seu carinho e palavras de incentivo me motivou nos momentos mais difíceis. Ao meu pai, Metusalém, por sua paciência, por seu apoio incondicional e por me ensinar o valor da perseverança. Aos meus avós, Salete e Teobaldo, que sempre demonstraram orgulho de mim e me incentivaram a seguir meus sonhos com determinação. Sem vocês, essa caminhada teria sido muito mais árdua. Obrigada por cada palavra de apoio, por cada gesto de carinho e por sempre acreditarem no meu potencial.

Aos meus colegas de turma, que compartilharam comigo esta trajetória acadêmica, tornando-a mais significativa. Foram anos de aprendizado, desafios e crescimento, e cada um de vocês fez parte dessa história. Agradeço por cada risada nos momentos de descontração, por cada dúvida compartilhada e por cada desafio que enfrentamos juntos. O companheirismo de vocês foram fundamentais para tornar essa jornada mais enriquecedora.

Aos meus professores e orientador, que desempenharam um papel essencial na minha formação acadêmica e profissional. Em especial, ao Dr. Israel Eduardo de Barros Filho, por sua orientação precisa, paciência e dedicação ao longo do desenvolvimento deste trabalho. Sua sabedoria, incentivo e disponibilidade foram cruciais para que este estudo pudesse ser concluído com qualidade e consistência. Agradeço não apenas pelo suporte técnico, mas também pelo incentivo e pelas palavras motivadoras que me ajudaram a manter o foco e a determinação.

Aos professores participantes da banca examinadora, Prof. Aminadabe e Prof. Juan Sebastian, pela disponibilidade e atenção em avaliar este trabalho. Desde já, agradeço

suas considerações e contribuições, que certamente agregarão valor à minha formação acadêmica e profissional.

À Universidade Federal do Ceará – Campus Jardins de Anita, por proporcionar um ambiente acadêmico de excelência, onde pude desenvolver meus conhecimentos, aprimorar minhas habilidades e amadurecer tanto pessoal quanto profissionalmente. Oportunidades e desafios foram colocados diante de mim, e cada um deles contribuiu para minha evolução. Agradeço aos técnicos administrativos e servidores do campus, que desempenham um papel fundamental para o funcionamento da instituição, e em especial à Bruna, Angélica e Igor Bruno, por toda a ajuda, paciência e comprometimento.

A todos os autores citados neste trabalho, cujas pesquisas e conhecimentos foram essenciais para a fundamentação teórica deste estudo. Seu esforço e dedicação à ciência possibilitaram a construção de novos saberes e enriqueceram significativamente este trabalho.

Aos participantes da pesquisa, que gentilmente se dispuseram a colaborar, disponibilizando seu tempo e conhecimento para contribuir com este trabalho. A contribuição de cada um de vocês foi essencial para que os objetivos deste estudo fossem alcançados.

À minha igreja, Comunidade Nova Vida, por ser um espaço de fortalecimento da minha fé e renovação da minha esperança. A cada irmão em Cristo que orou por mim, que me incentivou e que me ajudou a permanecer firme, minha eterna gratidão. Saber que havia pessoas intercedendo por mim e me apoiando espiritualmente foi um dos maiores sustentos durante essa caminhada.

Agradeço também a todos que, direta ou indiretamente, contribuíram para a realização deste trabalho e para minha formação. Cada palavra de incentivo, cada gesto de apoio e cada ensinamento recebido ao longo desta caminhada foram fundamentais para que eu chegasse até aqui.

Por fim, deixo aqui o meu profundo e sincero agradecimento a todos que fizeram parte dessa jornada. Este trabalho é fruto de um esforço coletivo, e cada um de vocês contribuiu de maneira significativa para que eu alcançasse mais essa conquista.

“A percepção é a chave que determina nossas respostas ao mundo.” (BARON, 2014, p. 37).

RESUMO

A engenharia social é um conjunto de técnicas utilizadas para manipular pessoas, aproveitando-se de suas vulnerabilidades psicológicas e sociais, a fim de obter informações confidenciais ou realizar ações fraudulentas. Este trabalho busca analisar os aspectos psicológicos envolvidos nos ataques de engenharia social. A pesquisa incluiu uma revisão bibliográfica e um questionário aplicado a estudantes dos cursos de Segurança da Informação, Ciência de Dados e Análise e Desenvolvimento de Sistemas da UFC, Campus Jardins de Anita. Os resultados revelaram que 81,6% dos entrevistados consideram a engenharia social um tema essencial para a área de segurança da informação e acreditam que deveria ser tratado de maneira mais aprofundada. Esse dado reforça a necessidade de revisar e atualizar os currículos acadêmicos, incluindo abordagens que vão além da segurança técnica e abrangem fatores psicológicos e comportamentais. Com base nesses achados, uma das principais recomendações deste estudo é a implementação de estratégias educacionais mais imersivas, como laboratórios de simulação de ataques, onde os alunos possam vivenciar, na prática, as táticas utilizadas por engenheiros sociais e desenvolver técnicas de defesa mais eficazes. Além disso, a criação de campanhas institucionais de conscientização pode contribuir significativamente para a disseminação do conhecimento sobre os riscos da engenharia social, tanto dentro quanto fora do ambiente acadêmico.

Palavras-chave: engenharia social; psicologia; segurança da informação; ataques.

ABSTRACT

Social engineering is a set of techniques used to manipulate people, taking advantage of their psychological and social vulnerabilities, in order to obtain confidential information or carry out fraudulent actions. This study aims to analyze the psychological aspects involved in social engineering attacks. The research included a literature review and a questionnaire administered to students of the Information Security, Data Science, and Systems Analysis and Development courses at UFC, Jardins de Anita Campus. The results revealed that 81.6% of the interviewees consider social engineering an essential topic for the area of information security and believe that it should be addressed in more depth. This data reinforces the need to review and update academic curricula, including approaches that go beyond technical security and encompass psychological and behavioral factors. Based on these findings, one of the main recommendations of this study is the implementation of more immersive educational strategies, such as attack simulation laboratories, where students can experience, in practice, the tactics used by social engineers and develop more effective defense techniques. Furthermore, the creation of institutional awareness campaigns can significantly contribute to the dissemination of knowledge about the risks of social engineering, both within and outside the academic environment.

Keywords: social engineering; psychology; information security; attacks.

LISTA DE FIGURAS

Figura 1 – Ataque de *phishing*..... 17
Figura 2 – Faixa etária dos estudantes 30
Figura 3 – Distribuição dos estudantes por curso……..... 30
Figura 4 – Distribuição dos estudantes por semestre……..…… 31
Figura 5 – Nível de familiaridade dos participantes …….…. 32
Figura 6 – Percepção dos alunos sobre o uso de princípios psicológicos…….. 33
Figura 7 – Emoções mais exploradas pelos atacantes 34
Figura 8 – Experiência pessoal dos estudantes……..... 34
Figura 9 – Medidas que os estudantes adotam para se proteger dos ataques..... 35
Figura 10 –Frequência de verificação dos estudantes……..... 36
Figura 11 –Exposição dos estudantes a mensagens suspeitas solicitando informações…… 36
Figura 12 – Plataformas consideradas pelos estudantes…….…….. 37
Figura 13 – Nível de treinamento dos estudantes……..... 38
Figura 14 – Abordagem do tema na UFC……..……..... 39
Figura 15 – Iniciativas consideradas mais eficazes……..... 39

SUMÁRIO

1	**INTRODUÇÃO**	12
2	**REVISÃO DA LITERATURA**	14
2.1	**Engenharia Social**	14
2.1.1	***Tipos de ataques***	14
2.1.1.2	Técnicas comuns de engenharia social	15
2.1.1.3	*Phishing*	15
2.1.1.4	*Pretexting*	18
2.1.1.5	*Baiting*	19
2.1.1.6	*Tailgating*	20
2.2	**Princípios psicológicos aplicados na Engenharia Social**	21
2.2.1	***Teoria da Persuasão (Robert Cialdini)***	21
2.2.2	***Vieses Cognitivos e Tomada de decisão***	22
2.3	Casos Reais de Engenharia Social	23
2.3.1	***Análise de Incidentes Famosos***	24
3	**METODOLOGIA**	27
4	**RESULTADOS**	29
5	**CONCLUSÃO E TRABALHOS FUTUROS**	41
	REFERÊNCIAS	44
	APÊNDICE	46

1 INTRODUÇÃO

A segurança da informação é um dos pilares essenciais para a proteção de dados em ambientes digitais e corporativos, sendo responsável por garantir a confidencialidade, integridade e disponibilidade das informações. Com o avanço das tecnologias de defesa, diversas camadas de proteção foram desenvolvidas, incluindo *firewalls*, sistemas de detecção e prevenção de intrusão, autenticação multifator e criptografia avançada. No entanto, apesar dessas evoluções, um dos pontos mais vulneráveis na segurança de qualquer sistema continua sendo o fator humano. A Engenharia Social explora exatamente essa fragilidade, utilizando estratégias de manipulação psicológica para persuadir indivíduos a divulgar informações sigilosas ou realizar ações prejudiciais sem perceber que estão sendo enganados.

Diferentemente de ataques puramente técnicos, que exploram falhas em *softwares* e infraestruturas, a Engenharia Social se baseia em princípios da psicologia e do comportamento humano para atingir seus objetivos. Técnicas como *pretexting*, *phishing*, *baiting* e *tailgating* exploram fatores psicológicos como a confiança, o medo, a autoridade, a reciprocidade e a urgência, tornando-se eficazes até mesmo contra usuários treinados. De acordo com Mitnick e Simon (2002), a Engenharia Social pode ser definida como "a arte de enganar pessoas para obter informações, acesso ou realizar ações que comprometam a segurança de um sistema". Essa abordagem transforma os próprios usuários em vetores de ataque, tornando a proteção da informação um desafio ainda maior.

Neste contexto, o presente trabalho tem como objetivo analisar os aspectos psicológicos subjacentes aos ataques de Engenharia Social, investigando como os agentes mal-intencionados exploram vulnerabilidades cognitivas e emocionais para alcançar seus objetivos. A pesquisa abordará os principais fatores que influenciam a suscetibilidade das vítimas. Além disso, serão discutidas as estratégias mais comuns utilizadas pelos atacantes, destacando como essas técnicas podem ser reconhecidas e prevenidas. Para reforçar a compreensão do tema, serão apresentados estudos de caso que exemplificam a eficácia da Engenharia Social em diferentes contextos, desde ataques direcionados a indivíduos até grandes violações de segurança em empresas e instituições governamentais.

A relevância deste estudo reside na crescente necessidade de conscientização e capacitação de indivíduos e organizações para reconhecer e mitigar as ameaças relacionadas à

Engenharia Social. Em um cenário no qual a cibersegurança não depende exclusivamente de barreiras tecnológicas, mas também do preparo dos usuários, torna-se essencial compreender a psicologia por trás desses ataques. Com base nessa compreensão, é possível desenvolver estratégias mais eficazes para reduzir a vulnerabilidade humana, promovendo treinamentos, campanhas de conscientização e políticas de segurança mais robustas. Dessa forma, este trabalho contribuirá para o campo da segurança da informação ao aprofundar a interseção entre psicologia e cibersegurança, fornecendo *insights* valiosos para o desenvolvimento de programas de treinamento mais eficazes e políticas de defesa que levem em consideração o fator humano como um elemento crítico na proteção da informação.

Esta monografia está organizada da seguinte forma: no capítulo 1, é apresentada a introdução ao tema, destacando a importância do estudo, a questão de pesquisa, os objetivos e os resultados esperados. O capítulo 2 compreende a revisão da literatura, abordando conceitos fundamentais sobre engenharia social, incluindo os tipos de ataques, técnicas comuns, princípios psicológicos aplicados, teoria da persuasão de Robert Cialdini e vieses cognitivos. Além disso, são analisados casos reais de engenharia social e incidentes famosos. No capítulo 3, é descrita a metodologia utilizada para o desenvolvimento da pesquisa. O capítulo 4 apresenta os resultados obtidos a partir da aplicação dos métodos descritos. Por fim, o capítulo 5 traz a conclusão do estudo, destacando as principais contribuições e sugerindo possíveis direções para trabalhos futuros.

2 REVISÃO DA LITERATURA

Esta seção aborda conceitos fundamentais relacionados à Engenharia Social, explorando as técnicas utilizadas por agentes maliciosos, os princípios psicológicos que sustentam esses ataques e casos reais que demonstram a relevância desse tema para a Segurança da Informação.

2.1 Engenharia Social

Conforme Mitnick e Simon (2002), Engenharia Social é "a arte de enganar pessoas para obter informações, acesso ou realizar ações que comprometam a segurança de um sistema". O ataque se baseia na exploração de características humanas, como sentimentos e comportamentos, por exemplo: confiança, medo, ou curiosidade, para manipular vítimas a revelar informações sensíveis ou a executar ações prejudiciais.

De acordo com uma definição contemporânea, a engenharia social é centrada na exploração das interações humanas, focando nas fraquezas cognitivas e comportamentais dos indivíduos ao invés de falhas técnicas (IEEE, 2023).

> As fraquezas cognitivas referem-se a limitações ou distorções no processo de pensamento, como a tendência a tomar decisões precipitadas devido à falta de análise crítica ou à influência de preconceitos mentais. As fraquezas comportamentais envolvem padrões de ação ou reação que podem ser manipulados, como a busca por gratificação instantânea ou a conformidade social.[...] (ANDERSON, 2020, p. 250)

2.1.1 Tipos de Ataques

Os ataques de Engenharia Social podem ser classificados em várias categorias, de acordo com os métodos utilizados e os objetivos do invasor. Esses ataques ocorrem tanto no ambiente online quanto no presencial, baseando-se em técnicas para enganar e influenciar as pessoas, explorando fraquezas emocionais, psicológicas ou comportamentais para alcançar seus propósitos.

Os ataques diretos envolvem a interação imediata com a vítima, seja por meio de telefonemas, mensagens, *e-mails*, ou até mesmo abordagens presenciais. O agente malicioso finge ser alguém confiável para obter informações sigilosas ou acesso a sistemas críticos.

Exemplo: Um indivíduo se passa por um técnico de TI da empresa e solicita que a vítima revele sua senha para "atualização de segurança".

Os ataques indiretos não exigem interação direta com a vítima no primeiro momento, mas utilizam artifícios como links maliciosos, arquivos infectados ou dispositivos físicos comprometidos.

Exemplo: O envio de um pendrive infectado é levado de propósito na recepção de uma empresa, esperando que um funcionário curioso conecte-o ao sistema interno.

2.1.1.2 Técnicas comuns de engenharia social

A Engenharia Social engloba uma variedade de técnicas que exploram falhas cognitivas e comportamentais humanas para alcançar seus objetivos. As principais técnicas utilizadas incluem:

2.1.2.3 Phishing

O *phishing* é uma das estratégias mais frequentes e ameaçadoras no campo da engenharia social. Ele aproveita a confiança e a falta de cautela das vítimas para enganá-las e obter dados confidenciais, como senhas, informações financeiras ou detalhes pessoais. Por ser uma técnica simples de implementar e com alta taxa de eficácia, é amplamente adotada por criminosos virtuais atualmente.

Segundo a *Microsoft* (2023), *phishing* é “uma tentativa de obter informações confidenciais ou induzir uma ação perigosa por meio de comunicações fraudulentas, geralmente em e-mails, mensagens de texto ou sites falsos que imitam fontes legítimas.”

De acordo com *Jakobsson e Myers* (2007), o *phishing* é "uma forma de engenharia social que usa táticas de dissimulação e falsificação para roubar informações pessoais das vítimas". Os criminosos se aproveitam de uma aparência legítima para enganar as vítimas, criando um cenário onde a urgência, a escassez ou a autoridade são exploradas.

O *phishing* opera por meio de um processo relativamente simples, mas altamente eficaz. Ele se inicia com o envio de uma mensagem falsa, cuidadosamente projetada para parecer legítima. O criminoso digital simula ser uma instituição confiável, como um banco, uma plataforma de redes sociais ou uma loja online. Para enganar a vítima, a mensagem é elaborada com atenção aos detalhes, incluindo o uso de logotipos, nomes de remetentes e endereços de *e-mail* que imitam os das organizações verdadeiras.

Dentro da mensagem, o criminoso geralmente cria um senso de urgência, induzindo a vítima a agir rapidamente sem tempo para avaliar criticamente a situação. Exemplos típicos incluem alertas como: "Sua conta será bloqueada se você não confirmar suas informações" ou "Detectamos uma atividade suspeita na sua conta. Clique aqui para verificar." Essas declarações são projetadas para explorar o medo e a ansiedade, dois fatores emocionais que reduzem a capacidade da vítima de tomar decisões racionais.

O próximo passo envolve o redirecionamento da vítima para um *site* falso, que imita quase perfeitamente o site legítimo da instituição mencionada na mensagem. Esse *site* é controlado pelo atacante e contém formulários que solicitam informações sensíveis, como nome de usuário, senha, número de cartão de crédito ou CPF. A vítima, acreditando estar interagindo com uma plataforma confiável, insere esses dados sem suspeitar que está sendo enganada.

Uma vez coletadas, as informações são imediatamente transmitidas para o atacante, que pode utilizá-las de diversas formas. Entre as ações mais comuns estão o roubo de dinheiro de contas bancárias, a realização de compras fraudulentas, o acesso não autorizado a sistemas corporativos e até a venda dos dados pessoais na *dark web*. Em muitos casos, as vítimas só percebem que foram alvo de um ataque quando já é tarde demais e os danos financeiros ou reputacionais já ocorreram.

Portanto, o *phishing* representa uma ameaça significativa à segurança da informação, especialmente em um mundo cada vez mais digitalizado. A conscientização dos usuários sobre as técnicas utilizadas nesses ataques e a adoção de práticas de segurança, como verificar cuidadosamente a autenticidade de mensagens suspeitas e evitar clicar em *links* não verificados, são fundamentais para mitigar esse tipo de ameaça. A Figura 1 mostra uma tentativa de *phishing*.

Figura 1 – Ataque de *phishing*



Fonte: Elaborada por Blog usecure (2024).

A conscientização dos usuários sobre as técnicas utilizadas nesses ataques e a adoção de práticas de segurança, como verificar cuidadosamente a autenticidade de mensagens suspeitas e evitar clicar em *links* não verificados, são fundamentais para mitigar esse tipo de ameaça.

A Figura 1 ilustra um exemplo típico de *e-mail* de *phishing*, destacando elementos fundamentais que visam enganar o destinatário e induzi-lo a tomar ações prejudiciais, como fornecer informações pessoais ou clicar em *links* maliciosos. A mensagem, que aparenta ser de uma instituição legítima, contém características que exploram a confiança da vítima, como o uso de logotipos, nomes de remetentes confiáveis e um *layout* profissional, simulando uma comunicação oficial.

Um dos principais aspectos identificados na Figura 1 é a criação de um senso de urgência. Frases como "Sua conta será suspensa em 24 horas" ou "Atividade suspeita detectada" são utilizadas para induzir o destinatário a agir rapidamente, sem questionar a autenticidade da mensagem. Esse gatilho psicológico, conforme discutido por Cialdini (1984), explora o princípio da urgência e do medo, reduzindo a capacidade de julgamento crítico do usuário.

Além disso, a figura mencionada anteriormente apresenta um *link* inserido no corpo do e-mail que direciona a vítima para um site fraudulento. Esse site, muitas vezes, é uma réplica visual de uma página oficial, projetada para capturar credenciais de *login*, dados bancários ou outras informações sensíveis. Jakobsson e Myers (2007) destacam que essa

técnica é uma das mais eficazes formas de *phishing*, devido à aparência de legitimidade do site falso.

O *e-mail* pode conter erros gramaticais ou ortográficos sutis, o que, embora possa parecer um sinal óbvio de fraude para usuários experientes, ainda passa despercebido por muitos usuários menos atentos ou mais vulneráveis. Esses detalhes, conforme evidenciado na figura, são comuns em ataques de *phishing* e reforçam a importância da educação e da conscientização como medidas preventivas.

2.1.1.4. Pretexting

O *pretexting* é uma técnica de engenharia social em que o atacante cria um cenário fictício ou "pretexto" para enganar a vítima e obter informações confidenciais. Ao contrário do *phishing*, que frequentemente depende de um ataque massivo e impessoal, o *pretexting* é caracterizado pela construção de uma história personalizada, muitas vezes muito convincente, que leva a vítima a acreditar que está interagindo com uma autoridade legítima ou com alguém em quem confia (MITNICK; SIMON, 2002).

O atacante, nesse caso, cria um cenário falso, muitas vezes se passando por alguém que a vítima considera confiável ou uma autoridade legítima. Por exemplo, o criminoso pode se passar por um funcionário de uma empresa, solicitando informações para "verificar" ou "atualizar" os dados da vítima, ou por um investigador de segurança que precisa confirmar informações sensíveis. Esse tipo de ataque explora a credibilidade e a autoridade percebida da pessoa ou instituição fictícia que o atacante representa (MITNICK & SIMON, 2002).

O *pretexting* não acontece só em mensagens ou *e-mails*; ele também pode acontecer por ligação ou até pessoalmente. O golpista cria uma história bem elaborada para ganhar a confiança da pessoa e convencê-la a entregar informações importantes. Por exemplo, alguém pode fingir ser do suporte de TI e pedir que a vítima confirme dados como o número de segurança ou outras credenciais, dizendo que é para uma "verificação de rotina". Antes de aplicar o golpe, eles geralmente pesquisam sobre a vítima, usando redes sociais e outras fontes, para deixar a abordagem mais realista e difícil de desconfiar.

De acordo com Mitnick e Simon (2002), um dos maiores especialistas em segurança e ex-criminoso de engenharia social, o *pretexting* é eficaz porque os atacantes geralmente se aproveitam da disposição humana para confiar em figuras de autoridade ou em cenários que

parecem legítimos. Isso, combinado com a personalização do ataque, faz com que as vítimas muitas vezes revelem dados críticos sem questionar a legitimidade da solicitação.

A principal diferença entre o *pretexting* e outras formas de ataque de engenharia social, como o *phishing*, é a natureza do engano. Enquanto o *phishing* depende de mensagens fraudulentas e impessoais enviadas para um grande número de pessoas, o *pretexting* envolve uma abordagem mais direcionada e focada na construção de um relacionamento de confiança entre o atacante e a vítima. O criminoso muitas vezes investe tempo na construção de um pretexto convincente, o que pode levar a uma maior taxa de sucesso.

2.1.1.5. Baiting

O *baiting* é um tipo de ataque de engenharia social que se caracteriza pela oferta de um "isca" tentadora para atrair a vítima a realizar uma ação que resultará na instalação de malware ou no comprometimento de dados sensíveis. O termo "*baiting*" deriva da analogia com a pesca, em que a vítima é atraída sem perceber que ela está sendo levada para um perigo iminente. Diferente de outros ataques, como o *phishing* e o *pretexting*, que dependem da manipulação psicológica e da criação de confiança, o *baiting* apela diretamente para os desejos e a curiosidade da vítima, oferecendo algo aparentemente valioso ou desejável (Mitnick, 2002).

O ataque de *baiting* pode se manifestar de várias formas, tanto digitais quanto físicas. Em seu formato mais comum, o *baiting* envolve a promessa de conteúdo gratuito, como filmes, músicas, *software* ou até mesmo prêmios, de modo que a vítima seja atraída por algo que lhe pareça vantajoso. No ambiente digital, o criminoso pode criar sites falsos ou anúncios oferecendo *downloads* de conteúdo popular ou pirata. Quando a vítima clica no *link*, um arquivo infectado com *malware* ou um programa malicioso é baixado para o dispositivo, podendo comprometê-lo completamente.

No contexto físico, o *baiting* também pode envolver a distribuição de dispositivos de armazenamento, como *pendrives* ou cartões de memória, contendo o *malware*. O criminoso deixa esses dispositivos em locais públicos ou próximos a áreas de tráfego intenso, esperando que a vítima os encontre e os conecte a seu computador ou rede. Ao fazer isso, o *malware* é instalado sem o conhecimento da vítima (Brown, 2020).

Outro risco associado ao *baiting* é o roubo de credenciais. Em ataques *online*, por exemplo, o *baiting* pode ser usado para redirecionar a vítima para *sites* falsos, onde informações confidenciais, como números de cartões de crédito ou dados bancários, podem ser roubadas (Brown, 2020).

Um exemplo clássico de *baiting* ocorre quando o atacante oferece um arquivo ou programa que parece ser de interesse da vítima, como um jogo, um *software* de edição ou um arquivo multimídia. Ao tentar baixar e executar o arquivo, o *malware* é instalado no sistema da vítima, podendo roubar informações sensíveis ou dar acesso remoto ao computador (Stallings, 2013).

2.1.1.6. Tailgating

O *tailgating* é uma técnica de engenharia social voltada para o acesso físico não autorizado a ambientes restritos. Nesse ataque, o criminoso explora a confiança e a distração de indivíduos que são autorizados a acessar determinadas áreas para aproveitar e invadir essas zonas protegidas. Ao contrário de outras formas de engenharia social que ocorrem em plataformas digitais, como o *phishing* ou o *pretexting*, o *tailgating* é um ataque no mundo físico, onde o criminoso se aproveita do comportamento humano para ganhar acesso a locais de forma furtiva (Hadnagy, 2018).

O processo do *tailgating* é relativamente simples, mas eficiente. O atacante observa a rotina das vítimas e se posiciona de forma a entrar fisicamente no local quando alguém autorizado estiver acessando o ambiente restrito. Normalmente, o criminoso segue uma pessoa enquanto ela utiliza seus privilégios para abrir uma porta ou acessar um controle de entrada, e aproveita-se dessa brecha para entrar sem ser notado (Bishop, 2018).

Em muitas situações, o atacante pode tentar parecer estar acompanhando alguém da mesma equipe ou se passar por um colaborador da organização, com o intuito de evitar ser questionado. O atacante, ao observar o comportamento do funcionário autorizado, se aproxima logo após a entrada do outro e entra, muitas vezes sem levantar suspeitas.

Um exemplo clássico de *tailgating* ocorre em edifícios corporativos, onde o controle de acesso é realizado por cartões magnéticos ou crachás. O atacante, ao perceber que um funcionário vai acessar o prédio, segue-o de perto e entra sem ser detectado.

Outro cenário comum é em empresas ou órgãos governamentais onde há grande circulação de pessoas. Um criminoso pode facilmente aproveitar-se de um momento em que uma porta automática é aberta para uma pessoa e seguir logo atrás, entrando sem que ninguém perceba.

2.2 Princípios psicológicos aplicados na engenharia social

A engenharia social explora vulnerabilidades cognitivas e emocionais humanas, utilizando estratégias psicológicas para manipular comportamentos e decisões. Essas estratégias são eficazes porque aproveitam padrões universais de pensamento e reação, muitas vezes levando as vítimas a agir rapidamente e sem questionar. Dois conceitos fundamentais nesse contexto são a Teoria da Persuasão, proposta por Robert Cialdini, e os Vieses Cognitivos, amplamente discutidos por Daniel Kahneman. Juntos, esses princípios ajudam a explicar como indivíduos são induzidos a cair em ataques de engenharia social.

2.2.1 Teoria da Persuasão

Robert Cialdini, em sua obra Influência: A Psicologia da Persuasão, detalha como comportamentos humanos podem ser influenciados por gatilhos psicológicos universais. Um desses gatilhos é o princípio da reciprocidade, onde o desejo de retribuir favores pode ser explorado por criminosos. Por exemplo, como um "brinde gratuito", pode levar a vítima a sentir-se inclinada a compartilhar informações confidenciais. Outro princípio é a autoridade, que utiliza a propensão humana de obedecer figuras que parecem possuir conhecimento ou poder superior. Ataques de *phishing* frequentemente simulam e-mails de autoridades para legitimar suas solicitações.

A escassez também é um fator persuasivo frequentemente aplicado. Esse princípio explora a percepção de valor em algo que está "em falta". Um *e-mail* fraudulento pode informar que uma oferta é válida por "tempo limitado", encorajando decisões impulsivas sem análise crítica. Além disso, a simpatia desempenha um papel fundamental, especialmente em ataques onde o criminoso tenta estabelecer uma relação de confiança, como em esquemas de *pretexting*. Ao demonstrar compreensão ou empatia, os atacantes conseguem obter informações que não seriam fornecidas em um contexto formal.

Um dos outros princípios é a aprovação social, que é a tendência humana de adotar comportamentos que são vistos como comuns ou aceitos por um grupo. Em situações de incerteza, as pessoas muitas vezes buscam sinais no comportamento dos outros para decidir como agir, o que faz desse princípio uma poderosa ferramenta de persuasão. O conceito de aprovação social se baseia no desejo intrínseco dos indivíduos de serem aceitos e validados pelos outros, o que frequentemente leva à conformidade com padrões observados em seu círculo social ou em contextos maiores, e esse princípio é bastante explorado pelos atacantes.

Os criminosos frequentemente utilizam mensagens que transmitem a ideia de que outras pessoas já tomaram uma determinada ação, levando as vítimas a acreditar que devem fazer o mesmo para não ficar de fora ou perder uma oportunidade. Em uma estratégia de *phishing*, por exemplo, um atacante pode criar um senso de urgência, informando que "milhares de usuários já atualizaram suas informações", incentivando a vítima a agir rapidamente, sem questionar a autenticidade da mensagem.

Estudos de Cialdini (2006) demonstram que as pessoas tendem a seguir a multidão, especialmente em situações em que elas não têm certeza sobre o que fazer. Isso é amplamente utilizado em técnicas de *marketing* e, claro, também é explorado por cibercriminosos. Em um estudo de Goldstein, Cialdini e Griskevicius (2008), foi observado que a simples exibição de comportamentos comuns em um grupo pode ser suficiente para induzir indivíduos a adotar atitudes ou ações semelhantes, mesmo sem uma pressão direta para isso. Isso é exemplificado em sites de *e-commerce* fraudulentos que mostram números falsos de "clientes que compraram recentemente" ou comentários de "usuários satisfeitos", criando uma ilusão de validação social.

2.2.2 Vieses cognitivos e tomadas de decisão

Os vieses cognitivos são padrões sistemáticos de pensamento que afetam a maneira como tomamos decisões. Esses atalhos mentais, também conhecidos como heurísticas, foram amplamente discutidos por Daniel Kahneman em sua obra "Rápido e Devagar: Duas Formas de Pensar" (2012). Kahneman descreve que nossa mente opera em dois sistemas: o primeiro sistema, rápido, automático e emocional, e o segundo sistema, mais lento, deliberado e lógico. Muitas vezes, o primeiro sistema domina, levando a julgamentos influenciados por vieses que podem ser explorados por atacantes na engenharia social.

Um dos vieses mais comuns é o viés da confirmação, que ocorre quando as pessoas tendem a buscar, interpretar ou lembrar informações de maneira que confirme suas crenças pré-existentes. Na prática, um atacante pode enviar uma mensagem que reforce uma crença já existente na vítima, como a ideia de que há um problema com sua conta bancária. A vítima, ao invés de questionar, aceita a informação, pois ela se encaixa no que já acredita ser possível.

Outro viés significativo é o efeito de ancoragem, no qual as pessoas se baseiam fortemente na primeira informação que recebem ao tomar decisões. Por exemplo, em um ataque de *phishing*, um *e-mail* pode mencionar um valor monetário falso como "débito pendente", ancorando a vítima a essa ideia e incentivando-a a agir rapidamente para consertar o suposto problema.

A aversão à perda também é frequentemente explorada. Como seres humanos, temos uma tendência inata a evitar perdas mais intensamente do que buscar ganhos. Essa inclinação pode ser usada para criar um senso de urgência em ataques, como mensagens que afirmam: "Sua conta será suspensa se você não agir agora". Isso provoca medo às pessoas de perder algo valioso para a vítima, levando a ações precipitadas.

O efeito de familiaridade é outro viés relevante. Ele ocorre quando as pessoas tendem a confiar em informações ou situações que lhes são familiares. Um atacante pode usar logotipos, tons de mensagem e outros elementos que imitam comunicações legítimas para criar uma falsa sensação de confiança. Essa familiaridade pode levar a vítima a agir sem verificar a autenticidade do pedido.

Como ressaltado por Kahneman (2012), nossa propensão a confiar no pensamento rápido e nos atalhos mentais é uma característica intrínseca do cérebro humano, mas também uma vulnerabilidade que pode ser explorada por aqueles com intenções maliciosas.

2.3 Casos reais de engenharia social

Tendo em vista que a engenharia social tem sido um dos métodos mais eficazes utilizados por atacantes para acessar sistemas e dados sensíveis, pois ocorre porque o alvo principal desses ataques é o comportamento humano, frequentemente descrito como o elo mais fraco da segurança da informação. Para compreender melhor como esses ataques se desenrolam e quais os seus impactos, é essencial analisar incidentes reais que demonstram a aplicabilidade prática das técnicas de engenharia social. Esses casos mostram como

criminosos têm usado o conhecimento do comportamento humano para alcançar seus objetivos, muitas vezes causando danos financeiros, reputacionais e operacionais a indivíduos e organizações.

A seguir, serão apresentados e analisados incidentes famosos que ilustram as diversas formas como a engenharia social tem sido empregada. A análise desses casos permitirá identificar padrões, compreender os fatores que contribuem para o sucesso desses ataques e oferecer *insights* sobre como mitigar os riscos associados a essa ameaça.

2.3.1 Análise de Incidentes Famosos

Em 2020, o Banco Central do Brasil enfrentou um ataque de *phishing* que resultou na transferência indevida de aproximadamente R$3 milhões para contas controladas por criminosos. Neste caso, e-mails fraudulentos foram enviados a funcionários do banco, induzindo-os a acreditar que precisavam atualizar suas credenciais de *login* em um sistema interno.

A eficácia desse ataque baseou-se no viés cognitivo da autoridade, pois os *e-mails* aparentavam ter sido enviados por superiores hierárquicos ou departamentos oficiais, gerando uma sensação de urgência e obediência. Além disso, a pressão de cumprir rapidamente a solicitação contribuiu para que as vítimas negligenciaram a análise detalhada do conteúdo das mensagens, um comportamento frequentemente explorado em golpes dessa natureza.

O uso de um site falso que imitava fielmente o sistema interno do banco reforçou a ilusão de legitimidade, desencadeando o viés da familiaridade. A familiaridade com o *design* e *layout* do site fez com que os funcionários acreditassem que estavam acessando o sistema verdadeiro, levando-os a inserir suas credenciais. Este caso evidencia a importância do treinamento contínuo para que funcionários possam identificar sinais de *phishing*, como *URLs* suspeitas, erros gramaticais ou solicitações incomuns.

Outro exemplo significativo ocorreu em outubro de 2020, quando o Interbank, uma das principais instituições financeiras do Peru, sofreu um ataque cibernético que expôs dados de mais de 3 milhões de clientes. O invasor, identificado pelo pseudônimo *kzoldiyck*, obteve acesso a servidores internos por meio de credenciais comprometidas de um parceiro terceirizado.

Esse incidente demonstra como atacantes utilizam a estratégia de porta dos fundos (*backdoor*), explorando brechas em terceiros que têm acesso privilegiado à infraestrutura da organização. Psicologicamente, o atacante explorou a negligência humana em relação à verificação de permissões e controles de segurança no uso de serviços externos.

O vazamento incluiu informações sensíveis, como nomes completos, números de telefone, documentos de identidade e detalhes financeiros. O atacante usou a pressão psicológica da extorsão, exigindo um resgate de US$ 4 milhões sob ameaça de divulgar os dados publicamente. A recusa do banco em atender à demanda destacou a importância de resiliência organizacional e de estratégias de comunicação para lidar com crises dessa natureza.

No Brasil, em 2024, uma mulher de 79 anos foi vítima de um golpe emocionalmente devastador em Toledo, Paraná. O criminoso, fingindo ser o empresário Elon Musk, estabeleceu um relacionamento virtual com a vítima, induzindo-a a acreditar que estava em um relacionamento amoroso com ele.

Neste caso, o golpista explorou sentimentos de solidão e carência emocional, criando uma narrativa envolvente que gerou confiança e apego emocional na vítima. A promessa de um futuro financeiro estável e a devolução do dinheiro "em dólares" exacerbaram o viés da ganância, um fator psicológico que frequentemente leva as pessoas a agir de maneira impulsiva.

A vítima foi levada a comprar cartões de presente da Apple e enviar os códigos via *WhatsApp*, acreditando que estaria ajudando seu suposto parceiro. A intervenção de funcionários do supermercado, que identificaram a compra atípica, foi crucial para mitigar o impacto financeiro do golpe. Este incidente ilustra como a engenharia social pode explorar a fragilidade emocional das pessoas, especialmente em grupos mais vulneráveis, como idosos.

Em 2020, um golpe relacionado ao sistema de pagamentos instantâneos Pix afetou centenas de moradores de Fortaleza e outras cidades do estado do Ceará. *Hackers* usaram uma técnica de engenharia social para criar um esquema de *phishing*, enviando *e-mails* e mensagens de texto falsas que se passavam por comunicados de bancos de grande porte, como Banco do Brasil e Caixa Econômica Federal. As mensagens informavam sobre supostas pendências ou bloqueios no sistema de pagamentos Pix, induzindo as vítimas a acreditar que suas contas estavam em risco e precisavam ser "corretamente configuradas".

O golpista utilizou a técnica de falsa urgência, um elemento psicológico eficaz em ataques de engenharia social. Ao clicar nos *links* fornecidos nas mensagens, as vítimas eram redirecionadas para páginas falsas que imitavam com precisão os sites oficiais dos bancos. Nessas páginas, as vítimas eram solicitadas a fornecer dados pessoais sensíveis, como senhas de acesso, números de conta, e *tokens* de segurança (gerados por sistemas de autenticação de dois fatores). O uso do viés da autoridade foi crucial, pois os golpistas se passaram por instituições financeiras confiáveis, o que gerou confiança nas vítimas.

Ao fornecer suas credenciais, os usuários estavam permitindo que os criminosos tivessem acesso completo às suas contas bancárias, e em muitos casos, os criminosos realizaram transferências rápidas para contas controladas por eles, esvaziando as contas em questão de minutos.

Centenas de pessoas foram afetadas pelo golpe, com perdas financeiras significativas. Os criminosos conseguiram transferir grandes quantias de dinheiro, deixando muitas vítimas com sérios prejuízos financeiros. Esse incidente é um exemplo claro de como a engenharia social pode ser utilizada em ataques ao sistema financeiro, explorando vulnerabilidades tanto tecnológicas quanto humanas. As vítimas, em sua maioria, relataram não ter percebido imediatamente o golpe, pois os *sites* falsificados eram extremamente semelhantes aos originais, o que reforçou a confiança e a sensação de segurança.

Esse ataque de engenharia social exemplifica como os criminosos exploraram os viés cognitivos de urgência e autoridade, bem como a familiaridade que os clientes têm com os comunicados institucionais dos bancos. A falsa urgência gerada pela mensagem, combinada com o temor de bloqueio das contas bancárias, fez com que as vítimas agissem impulsivamente, sem considerar os riscos ou verificar a autenticidade da mensagem.

Além disso, a manipulação de sentimentos de medo e insegurança levou os usuários a tomarem decisões precipitadas, sem refletir sobre a possível falsidade da comunicação. A combinação desses fatores psicológicos com a aparência convincente dos sites falsos aumentou significativamente as chances de sucesso do golpe.

3 METODOLOGIA

A metodologia deste estudo descreve os procedimentos adotados para a coleta e análise dos dados, garantindo a confiabilidade dos resultados. O objetivo é investigar os fatores psicológicos que influenciam ataques de engenharia social, combinando pesquisa bibliográfica e questionário online que se encontra no apêndice A. A pesquisa é voltada para os alunos da Universidade Federal do Ceará Campus Jardim de Anita e utiliza abordagens qualitativa e quantitativa para uma compreensão ampla do tema.

Esta pesquisa caracteriza-se como qualitativa e quantitativa, uma vez que busca compreender a psicologia por trás dos ataques de engenharia social por meio de uma análise aprofundada e de dados coletados junto ao público-alvo. A abordagem qualitativa é essencial para interpretar as motivações e comportamentos dos indivíduos expostos a ataques de engenharia social, enquanto a quantitativa possibilita a mensuração estatística das respostas dos participantes.

A coleta de dados foi realizada por meio de pesquisa bibliográfica e questionário online, aplicado aos alunos da Universidade Federal do Ceará (UFC). A pesquisa bibliográfica abrangeu obras, publicações de artigos científicos e estudos que tratam da psicologia da persuasão, influência social e vulnerabilidades humanas exploradas em ataques de engenharia social. O questionário online foi estruturado com perguntas para obter dados quantitativos e qualitativos sobre o conhecimento, experiências e percepção dos estudantes em relação a esses ataques, ficando disponíveis para respostas por um período de um mês.

Os critérios de seleção dos participantes incluíram estudantes regularmente matriculados na UFC que se dispuseram a responder ao questionário. O questionário foi divulgado por meio de redes sociais e na universidade para alcançar o máximo de respondentes. A pesquisa foi conduzida ao longo de um período de quase quatro semanas, garantindo tempo para uma amostragem representativa.

Os instrumentos utilizados para a coleta de dados incluíram um questionário online, desenvolvido para captar percepções, conhecimentos e experiências dos alunos dos cursos Segurança da Informação, Análise e Desenvolvimento de Sistemas e Ciência de Dados da UFC em relação à engenharia social. O questionário foi elaborado com base em estudos prévios sobre o tema, garantindo que os itens avaliassem corretamente os principais aspectos investigados. A pesquisa bibliográfica foi realizada com base em artigos científicos, livros e

publicações acadêmicas sobre psicologia e engenharia social, permitindo um embasamento teórico robusto para a análise dos dados coletados.

A pesquisa seguiu os princípios éticos estabelecidos pela UFC, garantindo o consentimento informado dos participantes, a confidencialidade dos dados e o respeito à privacidade. Todos os respondentes foram informados sobre os objetivos da pesquisa e foi assegurado que a participação era voluntária, permitindo que os participantes desistissem a qualquer momento sem prejuízo. Os dados coletados foram anonimizados para evitar qualquer possibilidade de identificação dos respondentes, e os resultados foram utilizados exclusivamente para fins acadêmicos. Todas as diretrizes para pesquisas envolvendo seres humanos foram rigorosamente seguidas, garantindo conformidade com os princípios da ética em pesquisa.

4 RESULTADOS

Do dia vinte e dois de janeiro até dezesseis de fevereiro, foi aplicado um questionário com o propósito de avaliar o nível de conhecimento e as percepções dos alunos sobre ataques de engenharia social. O público-alvo da pesquisa incluiu estudantes dos cursos de Segurança da Informação, Análise e Desenvolvimento de Sistemas e Ciência de Dados da Universidade Federal do Ceará (UFC), no Campus de Itapajé. Ao final da coleta de dados, foi obtido um espaço amostral de 38 respostas válidas, que compõem a base de análise deste estudo.

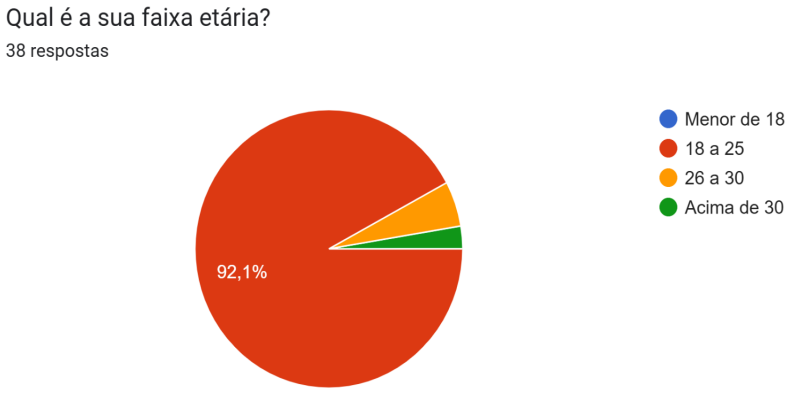
A pesquisa foi conduzida em conformidade com os aspectos legais relacionados à coleta, armazenamento e uso de dados dos participantes, seguindo os princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD). Antes da participação, foi garantido que os respondentes recebessem informações claras sobre os objetivos do estudo, os tipos de dados coletados e o uso dessas informações, garantindo seu consentimento informado.

Além disso, medidas de segurança foram adotadas para assegurar a confidencialidade dos dados durante todo o processo de pesquisa, prevenindo acessos não autorizados e possíveis vazamentos. A anonimização das respostas foi aplicada como forma de minimizar riscos de identificação dos participantes e preservar sua privacidade.

A primeira Seção do questionário teve como objetivo traçar o perfil dos estudantes que participaram da pesquisa, fornecendo um panorama essencial para a análise dos demais resultados. Essa etapa foi composta por três questões que abordaram a faixa etária, o curso no qual os alunos estão matriculados e o período em que se encontram. Compreender essas características é fundamental para interpretar os níveis de conhecimento e percepção sobre ataques de phishing dentro de um contexto acadêmico específico.

O gráfico da Figura 2 apresenta a classificação dos estudantes por faixa etária. Os dados indicam que 92,1% dos participantes possuem entre 18 e 25 anos, demonstrando que a grande maioria é composta por jovens adultos em início de carreira acadêmica e profissional. Esse resultado sugere que a familiaridade com tecnologia pode ser um fator relevante na análise, uma vez que essa faixa etária cresceu em um ambiente digitalizado e, possivelmente, já teve contato prévio com conceitos de segurança da informação.

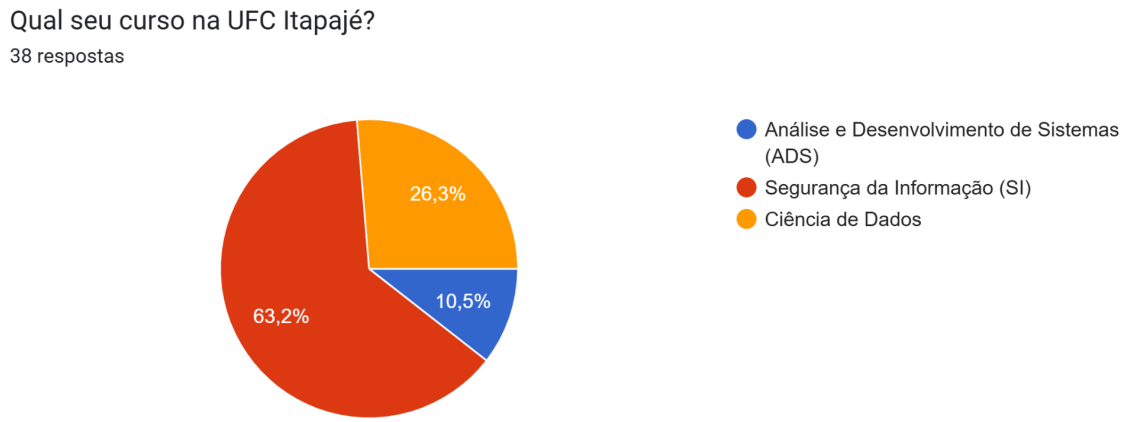
Figura 2 – Faixa etária dos estudantes



Fonte: Elaborada pela autora.

Na sequência, a Figura 3 exibe a distribuição dos estudantes por curso, mostrando que 63,2% estão matriculados no curso de Segurança da Informação, 26,3% em Ciência de Dados e 10,5% em Análise e Desenvolvimento de Sistemas. Esses números refletem um público majoritariamente voltado para a área de tecnologia e segurança, o que pode impactar os níveis de conhecimento sobre phishing, uma vez que os alunos dessas áreas tendem a ter maior exposição a temas relacionados à cibersegurança. A predominância de estudantes de Segurança da Informação também pode indicar um maior nível de conscientização sobre ataques cibernéticos, o que será analisado nas próximas seções do estudo.

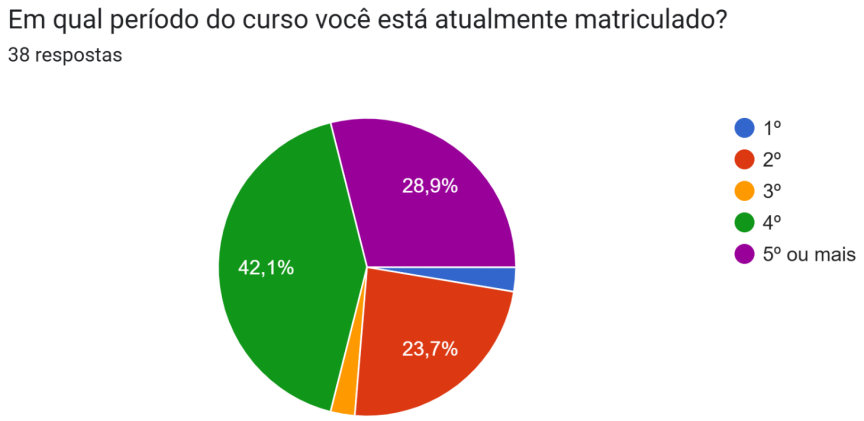
Figura 3 – Distribuição dos estudantes por curso



Fonte: Elaborada pela autora.

A Figura 4 demonstra a distribuição dos participantes com base no período em que estão matriculados. Observa-se que a maior parte dos estudantes está no 4º semestre do curso, representando 42,1% da amostra (16 alunos). Esse dado é significativo, pois sugere que boa parte dos respondentes já teve contato com disciplinas mais avançadas relacionadas à segurança e pode possuir um nível de conhecimento mais consolidado sobre o tema.

Figura 4 – Distribuição dos estudantes por semestre



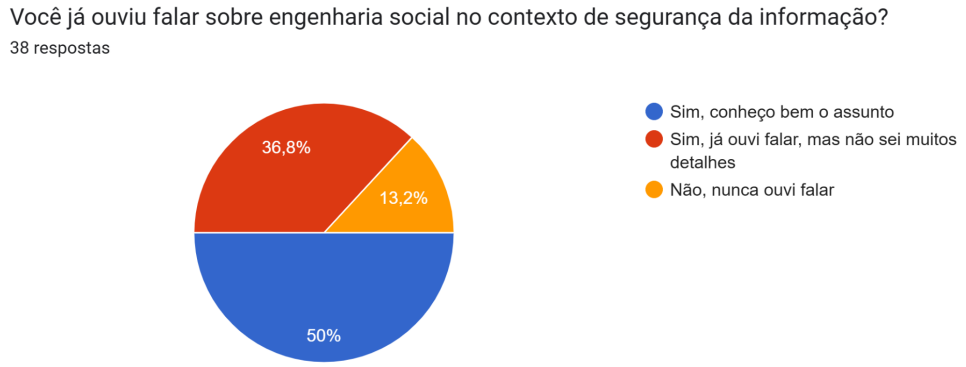
Fonte: Elaborada pela autora.

A coleta desses dados iniciais é essencial para contextualizar os resultados subsequentes, uma vez que diferentes fatores, como idade, curso e tempo de estudo, podem influenciar no nível de conscientização e preparo dos alunos diante de ameaças cibernéticas. A análise dessas variáveis permitirá uma compreensão mais precisa da relação entre o perfil acadêmico e o conhecimento sobre engenharia social, contribuindo para identificar possíveis lacunas na formação e oportunidades de aprimoramento educacional na área de segurança da informação.

A segunda Seção da pesquisa teve como objetivo explorar a experiência dos estudantes em segurança da informação, com um foco específico na engenharia social. O intuito dessa abordagem foi avaliar o nível de conscientização dos alunos sobre ataques cibernéticos baseados na manipulação psicológica, além de identificar possíveis vulnerabilidades e áreas que demandam maior aprofundamento em termos de capacitação.

Dentre as questões abordadas, a primeira, representada na Figura 5, buscou compreender o nível de familiaridade dos participantes com o conceito de engenharia social. Os resultados revelaram que 50% dos estudantes afirmaram conhecer bem o tema, enquanto 36,8% declararam já ter ouvido falar sobre ele, mas sem um conhecimento aprofundado. Por outro lado, 13,12% dos entrevistados relataram nunca ter ouvido falar sobre engenharia social.

Figura 5 – Nível de familiaridade dos participantes



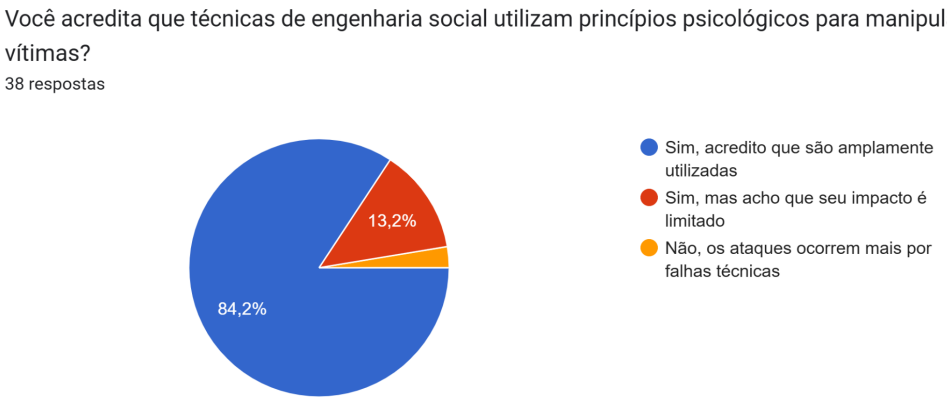
Fonte: Elaborada pela autora.

Esses dados indicam que, apesar de uma parcela significativa dos alunos possuir alguma noção sobre o assunto, ainda há uma quantidade considerável que desconhece completamente o conceito ou possui apenas um entendimento superficial. Essa lacuna de conhecimento pode representar um risco à segurança digital dos usuários, visto que indivíduos menos informados são mais suscetíveis a ataques baseados em manipulação psicológica. Assim, promover campanhas educativas e treinamentos específicos pode ser uma estratégia essencial para fortalecer a segurança dos estudantes contra ameaças desse tipo.

A percepção dos alunos sobre o uso de princípios psicológicos em ataques de engenharia social foi abordada na questão representada pela Figura 6. Os resultados apontam que 84,2% dos respondentes acreditam que essas técnicas são amplamente utilizadas para manipular as vítimas, enquanto 13,2% reconhecem a existência desse fator, mas acreditam que seu impacto seja limitado. Apenas 1% dos participantes considera que os ataques ocorrem mais devido a falhas técnicas do que à manipulação psicológica. Esses achados reforçam a ideia de que a engenharia social se aproveita majoritariamente de vulnerabilidades humanas, explorando aspectos emocionais e cognitivos para enganar as vítimas. Esse conhecimento evidencia a importância da conscientização e do treinamento contínuo em segurança da

informação, capacitando os estudantes a reconhecerem e evitarem armadilhas criadas por cibercriminosos.

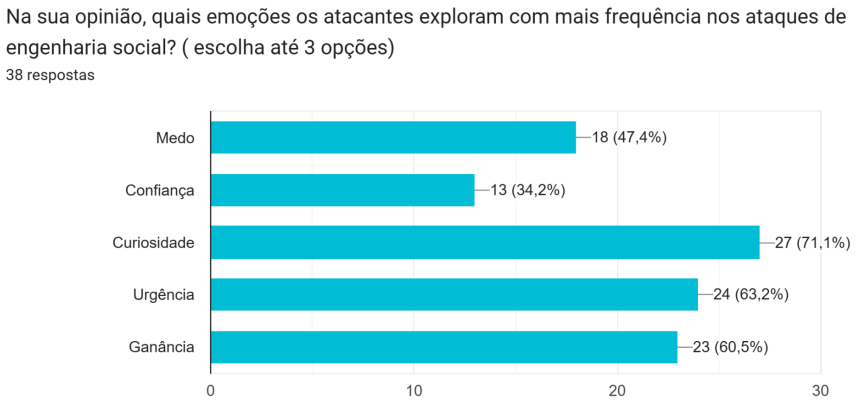
Figura 6 – Percepção dos alunos sobre o uso de princípios psicológicos.



Fonte: Elaborada pela autora.

Uma das perguntas centrais da pesquisa buscou identificar quais emoções são mais exploradas pelos atacantes nos golpes de engenharia social. Conforme ilustrado na Figura 7, as emoções mais mencionadas foram medo e confiança. Além disso, outras emoções frequentemente utilizadas em ataques incluem urgência, curiosidade e ganância. Esses dados confirmam que a engenharia social frequentemente se baseia na criação de cenários que induzem reações emocionais impulsivas, comprometendo a capacidade da vítima de analisar a situação com racionalidade. Por exemplo, *e-mails* fraudulentos podem simular situações de urgência para induzir um usuário a fornecer informações sigilosas ou realizar pagamentos sem verificar a autenticidade da solicitação. Dessa forma, o conhecimento sobre a exploração dessas emoções pode ser aplicado no desenvolvimento de treinamentos de segurança voltados para a identificação de situações suspeitas e para o fortalecimento da tomada de decisão racional frente a possíveis ataques.

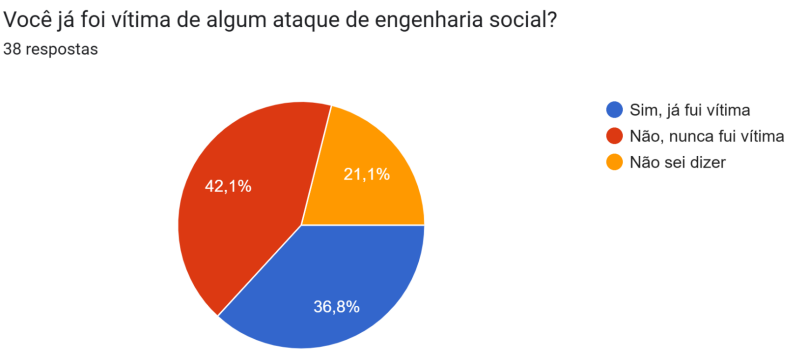
Figura 7 – Emoções mais exploradas pelos atacantes



Fonte: Elaborada pela autora.

A experiência pessoal dos estudantes com ataques de engenharia social foi analisada na questão representada pela Figura 8. Os resultados indicam que 36,8% dos participantes afirmaram já ter sido vítimas desse tipo de ataque, enquanto 42,1% relataram nunca terem passado por essa experiência. No entanto, 21,1% dos entrevistados afirmaram não saber dizer se já foram vítimas de engenharia social, o que pode indicar uma falta de compreensão sobre como esses ataques ocorrem e quais são seus sinais. Esse percentual reforça a necessidade de iniciativas educativas que abordem não apenas os conceitos teóricos da engenharia social, mas também exemplos práticos e estudos de caso que ajudem os estudantes a reconhecerem tentativas de ataques. A incerteza sobre a exposição a golpes cibernéticos pode tornar os indivíduos mais vulneráveis, uma vez que aqueles que não percebem que foram alvo de ataques podem acabar comprometendo suas informações sem perceber.

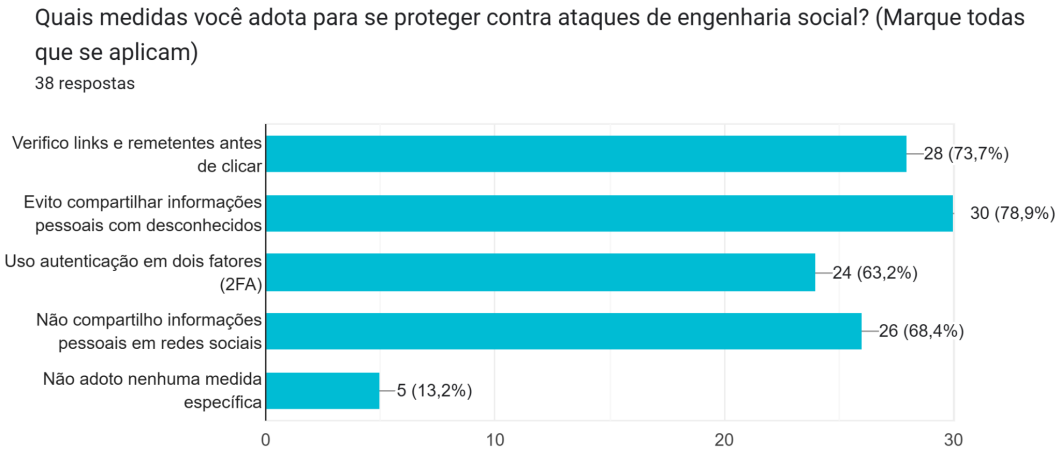
Figura 8 – Experiência pessoal dos estudantes com ataques de engenharia social



Fonte: Elaborada pela autora.

A pesquisa também investigou quais medidas os estudantes adotam para se proteger contra ataques de engenharia social, conforme representado na Figura 9, onde os participantes poderiam marcar mais de uma opção. Os resultados mostram que os participantes evitam compartilhar informações pessoais com desconhecidos, verificam *links* e remetentes antes de clicar. Além disso, afirmam não compartilhar informações pessoais em redes sociais e utilizam autenticação em dois fatores (2FA). No entanto, um dado preocupante é que 13,2% dos estudantes relataram não adotar nenhuma medida específica para se proteger contra esse tipo de ameaça, o que pode aumentar sua vulnerabilidade a ataques cibernéticos.

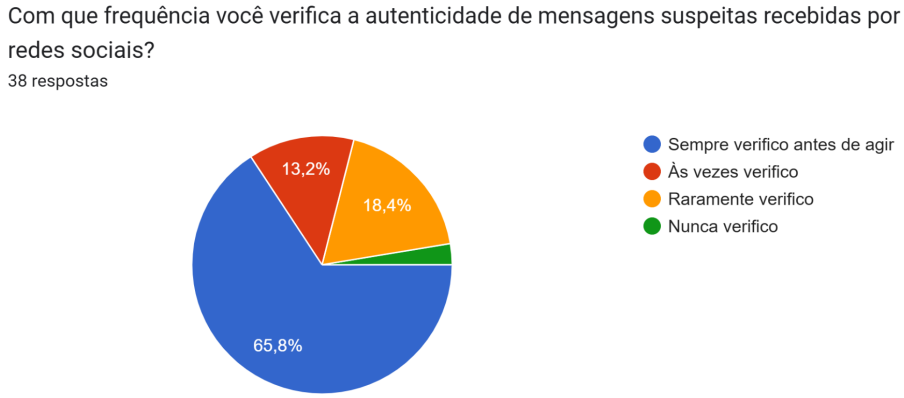
Figura 9 – Medidas que os estudantes adotam para se proteger dos ataques



Fonte: Elaborada pela autora.

A frequência com que os estudantes verificam a autenticidade de mensagens suspeitas recebidas por e-mail ou redes sociais foi analisada na Figura 10. Os resultados indicam que 65,8% dos participantes sempre verificam antes de agir, enquanto 13,2% verificam às vezes. Em contrapartida, 18,4% raramente verificam e 2,6% nunca verificam, demonstrando que ainda há um percentual significativo de indivíduos que não adotam essa prática essencial de segurança.

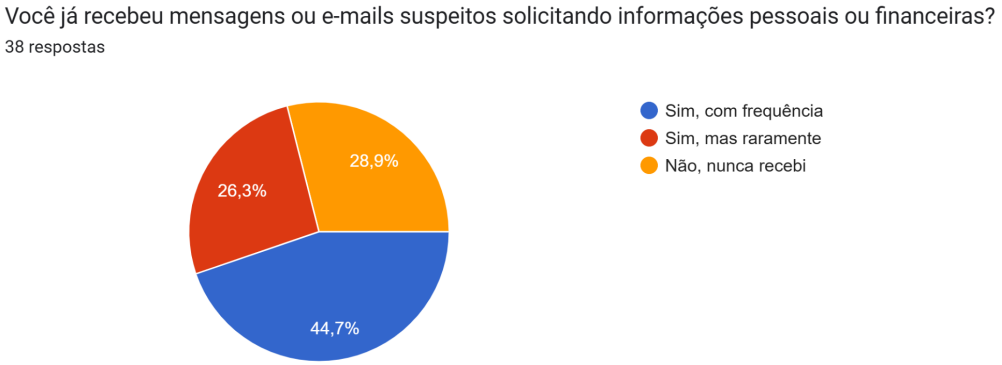
Figura 10 – Frequência que os estudantes verificam a autenticidade de mensagens suspeitas



Fonte: Elaborada pela autora.

A exposição dos estudantes a mensagens ou *e-mails* suspeitos solicitando informações pessoais ou financeiras foi abordada na Figura 11. Os resultados revelam que 44,7% dos entrevistados recebem esse tipo de mensagem com frequência, enquanto 26,3% afirmam recebê-las raramente. Por outro lado, 28,9% relataram nunca ter recebido tais mensagens. Esses dados destacam a relevância de campanhas de conscientização sobre técnicas de engenharia social, visto que a maioria dos estudantes já teve algum contato com esse tipo de ameaça.

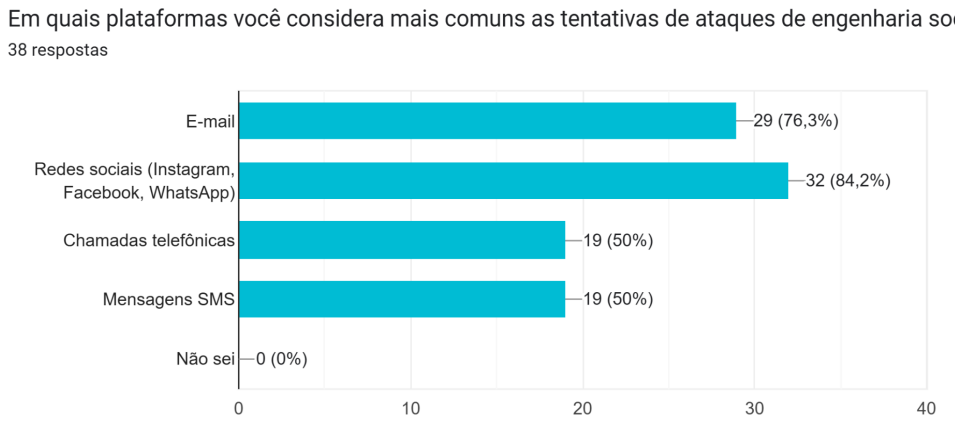
Figura 11 – Exposição dos estudantes a mensagens ou e-mails suspeitos solicitando informações



Fonte: Elaborada pela autora.

Por fim, a pesquisa analisou quais plataformas são consideradas pelos estudantes como as mais comuns para tentativas de ataques de engenharia social, onde poderiam marcar mais de uma opção de plataforma. (Figura 12). As redes sociais (*Instagram, Facebook, WhatsApp*) foram mencionadas e também foram apontadas as chamadas telefônicas como um meio recorrente. Além disso, mensagens *SMS* foram citadas por 50% dos entrevistados. Esses achados reforçam a necessidade de medidas preventivas em diferentes canais de comunicação, destacando a importância de boas práticas de segurança digital para evitar ataques.

Figura 12 – Plataformas consideradas pelos estudantes como as mais comuns para tentativas de ataques de engenharia social



Fonte: Elaborada pela autora.

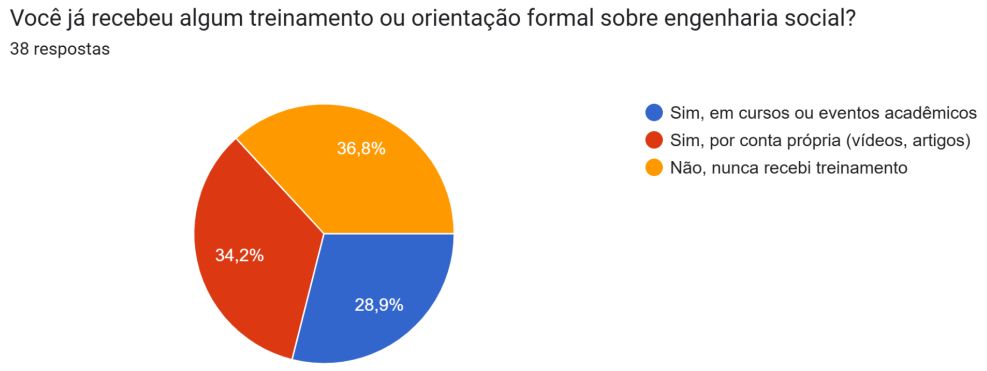
Em suma, os resultados dessa Seção da pesquisa revelam que, embora muitos estudantes tenham um conhecimento básico sobre engenharia social, ainda existem lacunas significativas na conscientização sobre esse tipo de ameaça. A falta de certeza sobre a própria exposição a ataques e o desconhecimento sobre práticas de segurança indicam a necessidade de programas educacionais contínuos. Capacitações específicas podem contribuir significativamente para a redução da vulnerabilidade dos estudantes frente a ataques cibernéticos baseados em manipulação psicológica, tornando-os mais preparados para identificar e evitar possíveis ameaças.

A terceira Seção da pesquisa teve como objetivo investigar o nível de treinamento dos participantes sobre engenharia social, com foco na experiência prévia de treinamento e na percepção da importância de aprofundar esses temas na formação acadêmica. O intuito dessa abordagem foi avaliar a familiaridade dos estudantes com as ameaças cibernéticas mais

comuns, identificar possíveis lacunas de conhecimento e explorar a necessidade de programas educacionais específicos para fortalecer a segurança digital no campus.

A pergunta representada pela Figura 13, buscou saber se os participantes já haviam realizado algum curso ou treinamento sobre engenharia social. Os resultados indicaram que 36,8% dos participantes nunca haviam feito esse tipo de treinamento, enquanto 14,9% participantes haviam participado de cursos específicos ou eventos acadêmicos. Esse dado revela uma deficiência significativa na formação dos alunos, pois a falta de treinamento sobre engenharia social pode deixá-los mais vulneráveis a ataques. Portanto, a ausência de treinamento pode comprometer a segurança dos usuários, tornando-os mais propensos a cair em golpes. Esse resultado destaca a necessidade urgente de incluir mais programas de treinamento sobre segurança cibernética para capacitar os alunos a reconhecerem e evitarem tais ameaças.

Figura 13 – Nível de treinamento dos estudantes sobre engenharia social



Fonte: Elaborada pela autora.

A Figura 14 abordou a percepção dos alunos sobre a importância do tema engenharia social ser abordada de forma mais detalhada na UFC. A maioria dos participantes (81,6%) concorda que é um tema essencial para a área e deve ser tratado de forma mais aprofundada, enquanto 15,8% acham que deveria ser tratado de maneira mais breve e apenas 1% não vê necessidade. Esses dados refletem uma forte demanda dos alunos por mais educação sobre como a engenharia social pode ser usada para manipular as pessoas e como se proteger dessas ameaças.

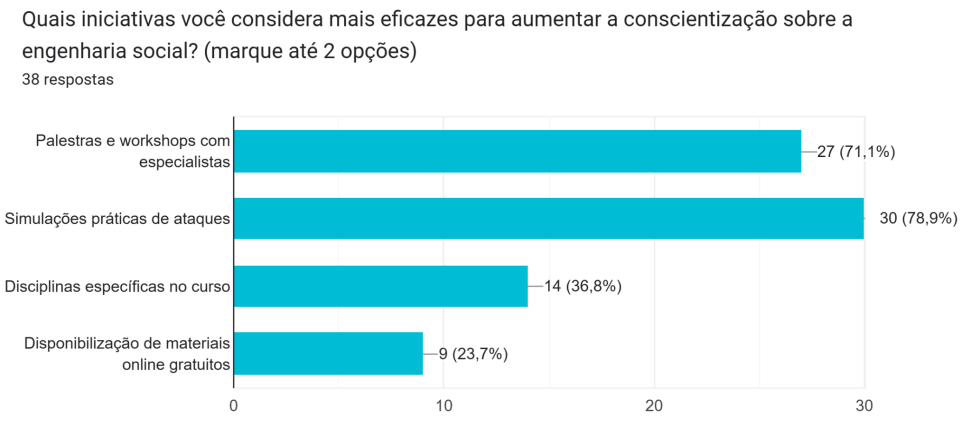
Figura 14 – Abordagem do tema na UFC



Fonte: Elaborada pela autora.

Por fim, a Figura 15 questionou quais iniciativas os participantes consideram mais eficazes para aumentar a conscientização sobre engenharia social. As opções mais votadas foram: simulações práticas de ataques e palestras/*workshops* com especialistas. Isso sugere que os alunos preferem métodos de ensino mais interativos e práticos, que simulem cenários reais de ataques, permitindo que eles vivenciem a situação e aprendam como reagir a ela. As simulações práticas de ataques e *workshops* com especialistas têm o potencial de fornecer uma experiência de aprendizado mais eficaz do que aulas teóricas ou materiais online, pois os alunos podem aplicar o que aprenderam em um ambiente controlado. Esse dado destaca a importância de integrar métodos de ensino ativos, como simulações e *workshops*, para aprimorar a educação sobre segurança cibernética.

Figura 15– Iniciativas consideradas mais eficazes para aumentar a conscientização



Fonte: Elaborada pela autora.

Em conclusão, os resultados desta seção da pesquisa evidenciam que, embora os participantes demonstrem algum grau de conscientização sobre engenharia social, há uma clara necessidade de intensificar os programas de treinamento e a conscientização sobre esses tópicos. As lacunas no conhecimento e a falta de treinamento formal indicam que os alunos estão em risco de se tornarem vítimas de ataques cibernéticos, tornando essencial a implementação de programas educativos focados em práticas interativas, como simulações de ataques e palestras com especialistas, para melhorar a segurança e preparação dos estudantes. Além disso, os dados mostram que os alunos consideram a abordagem de temas como engenharia social uma prioridade e que a inclusão desses tópicos nas currículas acadêmicas pode contribuir significativamente para a formação de profissionais mais preparados para lidar com as ameaças cibernéticas.

5 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho buscou explorar a psicologia por trás dos ataques de engenharia social, evidenciando que as vulnerabilidades humanas desempenham um papel tão significativo quanto as falhas técnicas na segurança da informação. A pesquisa utilizou uma abordagem qualitativa e quantitativa para compreender como os estudantes dos cursos de Segurança da Informação, Ciência de Dados e Análise e Desenvolvimento de Sistemas do campus UFC Jardim de Anita percebem e lidam com ameaças dessa natureza.

Os resultados obtidos reforçaram a importância das emoções no processo de manipulação empregado por atacantes de engenharia social. Foi possível identificar que sentimentos como medo, urgência, curiosidade e até mesmo o desejo de ajudar podem levar um indivíduo a se tornar vítima de um ataque. Esses achados corroboram a literatura da área, que aponta que técnicas como *pretexting, phishing e baiting* exploram aspectos emocionais para enganar as vítimas e obter informações sigilosas.

Outro ponto relevante identificado na pesquisa foi a lacuna existente na capacitação acadêmica sobre o tema. A análise dos dados revelou que 36,8% dos participantes nunca haviam recebido treinamento específico sobre engenharia social, enquanto apenas 14,9% tiveram contato com cursos especializados ou eventos acadêmicos. Essa estatística indica uma deficiência educacional, pois a ausência de treinamento adequado pode deixar futuros profissionais da área mais suscetíveis a ataques e menos preparados para atuar na proteção de sistemas e dados.

Além disso, a pesquisa revelou que 81,6% dos entrevistados consideram a engenharia social um tema essencial para a área de segurança da informação e acreditam que deveria ser tratado de maneira mais aprofundada. Esse dado reforça a necessidade de revisar e atualizar os currículos acadêmicos, incluindo abordagens que vão além da segurança técnica e abrangem fatores psicológicos e comportamentais. Entre os métodos de ensino preferidos pelos estudantes, destacam-se simulações práticas de ataques e palestras ministradas por especialistas, demonstrando que métodos interativos e aplicados tendem a ser mais eficazes para o aprendizado do tema.

Com base nesses achados, uma das principais recomendações deste estudo é a implementação de estratégias educacionais mais imersivas, como laboratórios de simulação de ataques, onde os alunos possam experimentar, na prática, as táticas utilizadas por

engenheiros sociais e desenvolver técnicas de defesa mais eficazes. Além disso, a criação de campanhas institucionais de conscientização pode contribuir significativamente para a disseminação do conhecimento sobre os riscos da engenharia social, tanto dentro quanto fora do ambiente acadêmico.

A adoção da gamificação no ensino de segurança cibernética também pode ser uma estratégia promissora. Jogos interativos e desafios que simulem ataques reais podem tornar o aprendizado mais dinâmico e incentivar a participação ativa dos alunos, promovendo uma melhor assimilação do conteúdo. Da mesma forma, a inserção de treinamentos obrigatórios em cursos de tecnologia da informação poderia garantir que todos os estudantes adquirissem um conhecimento mínimo necessário sobre engenharia social e suas implicações.

Outro aspecto que merece destaque é a necessidade de colaboração entre universidades e empresas do setor de segurança cibernética. Parcerias com organizações especializadas podem proporcionar oportunidades para que os alunos tenham contato direto com cenários reais de ataques, participem de programas de capacitação avançada e interajam com profissionais experientes da área. Essa troca de conhecimento pode ser fundamental para preparar futuros especialistas para os desafios do mercado de trabalho.

Por fim, este estudo reforça a ideia de que a segurança da informação não pode ser tratada apenas como uma questão técnica, mas deve considerar aspectos psicológicos e sociais para ser verdadeiramente eficaz. A vulnerabilidade humana continuará sendo explorada por atacantes enquanto não houver uma abordagem mais abrangente para mitigar esse risco. Dessa forma, espera-se que esta pesquisa sirva como um ponto de partida para futuras investigações sobre a interseção entre psicologia e segurança cibernética, contribuindo para o desenvolvimento de estratégias mais eficientes na proteção contra ataques de engenharia social.

Em um mundo cada vez mais conectado, onde a informação se tornou um dos ativos mais valiosos, compreender e mitigar os riscos da engenharia social é essencial para garantir a segurança digital. O aprimoramento das práticas educacionais e a ampliação da conscientização sobre o tema são passos fundamentais para a formação de profissionais mais preparados e para a construção de um ambiente digital mais seguro para todos. Com isso, espera-se que este trabalho possa inspirar novas abordagens no ensino da segurança da

informação e contribuir para o fortalecimento da cultura de cibersegurança no meio acadêmico e profissional.

Como sugestão para trabalhos futuros, recomenda-se a realização de estudos mais aprofundados sobre a eficácia das campanhas de conscientização em segurança da informação, avaliando o impacto real dessas iniciativas na redução de ataques de engenharia social. Além disso, seria interessante analisar o comportamento dos usuários diante de diferentes cenários de ataque, utilizando experimentos controlados para compreender quais barreiras podem ser mais bem exploradas na prevenção desses ataques. Outra possibilidade é investigar a aplicação de testes de simulação de ataques de engenharia social em ambientes corporativos para avaliar a resposta dos funcionários e a eficácia das contramedidas adotadas.

REFERÊNCIAS

ANDERSON, Ross. *Security Engineering:* ***A Guide to Building Dependable Distributed Systems.*** 3. ed. Wiley, 2020.

ARIELY, Dan. ***Previsivelmente Irracional: As forças ocultas que moldam nossas decisões.*** Rio de Janeiro: Elsevier, 2008.

BANCO CENTRAL DO BRASIL. ***Ataque de phishing compromete a segurança de funcionários.*** Brasília: Banco Central, 2020. Disponível em: https://www.bcb.gov.br. Acesso em: 10 jan. 2025.

BANCO DO BRASIL; CAIXA ECONÔMICA FEDERAL. ***Alerta sobre golpes envolvendo o Pix.*** Brasília: Banco do Brasil e Caixa, 2020. Disponível em: https://www.bb.com.br e https://www.caixa.gov.br. Acesso em: 11 jan. 2025.

BISHOP, Matt. ***Introduction to Computer Security.*** Addison-Wesley, 2018.

BROWN, John. ***Baiting Attacks and How to Avoid Them.*** Cybersecurity Weekly, 2020.

CIALDINI, Robert. ***Influência: a psicologia da persuasão.*** 4. ed. Rio de Janeiro: Sextante, 1984.

CIALDINI, Robert. ***Influence: The Psychology of Persuasion.*** Harper Business, 2006.

G1. ***Mulher perde dinheiro após cair em golpe envolvendo Elon Musk.*** G1, 2024. Disponível em: https://g1.globo.com. Acesso em: 11 jan. 2025.

GOLDMAN, Eric. ***The Pretexting Problem: Exploring the Ethics of Deception in Cybersecurity.*** Journal of Cybersecurity, 2013.

GOLDSTEIN, Noah J.; CIALDINI, Robert B.; GRISKEVICIUS, Vladas. ***A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels.*** Journal of Consumer Research, 2008.

GROSS, Jonah; HERNANDEZ-CASTRO, Julio. ***Exploring Psychological Triggers in Cybercrime: A Cognitive Bias Perspective.*** Journal of Cybersecurity Research, 2022.

HADNAGY, Christopher. ***Social Engineering: The Science of Human Hacking.*** Wiley, 2018.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. ***Social Engineering: Exploitation of Cognitive and Behavioral Weaknesses in Human Interactions.*** IEEE, 2023.

INTERBANK. ***Relatório oficial sobre o ataque cibernético de 2020.*** Lima: Interbank, 2020. Disponível em: https://www.interbank.pe. Acesso em: 10 jan. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022 –* ***Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements.*** Genebra: ISO, 2022.

JAKOBSSON, Markus; MYERS, Steven. ***Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft.*** Hoboken: John Wiley & Sons, 2007.

KAHNEMAN, Daniel. ***Rápido e Devagar: Duas Formas de Pensar.*** Tradução de Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2012.

KASPERSKY. **Engenharia social e ataques de phishing: Relatório global de ameaças.** Moscou: Kaspersky Lab, 2020. Disponível em: https://securelist.com. Acesso em: 12 jan. 2025.

KASPERSKY. ***IT Threat Evolution Report.*** Moscou: Kaspersky Lab, 2024.

MCALANEY, John; TAYLOR, Helen; FENICI, Patryk. ***Social Influence and Cybersecurity: Understanding and Preventing Online Manipulation.*** Palgrave Macmillan, 2021.

MCGUIRE, Michael; DOWLING, Samantha. ***Cybercrime: Understanding the Online Business of Illicit Markets.*** Springer, 2020.

MICROSOFT CORPORATION. ***Detect and prevent phishing attacks.*** 2023.

MITNICK, Kevin D.; SIMON, William L. ***The Art of Deception: Controlling the Human Element of Security.*** Wiley, 2002.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). ***Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.*** Gaithersburg: NIST, 2018.

ROSS, Lee; NISBETT, Richard E. ***The Person and the Situation: Perspectives of Social Psychology.*** McGraw-Hill, 1991.

STALLINGS, William. ***Network Security Essentials: Applications and Standards.*** Pearson, 2013.

THALER, Richard H.; SUNSTEIN, Cass R. *Nudge:* ***Improving Decisions About Health, Wealth, and Happiness.*** Penguin Books, 2008.

TVERSKY, Amos; KAHNEMAN, Daniel. ***Judgment under Uncertainty: Heuristics and Biases.*** Cambridge University Press, 1982.

APÊNDICE – Questionário: A psicologia por trás dos ataques de engenharia social

QUESTIONÁRIO

Este questionário faz parte de uma pesquisa acadêmica em andamento na Universidade Federal do Ceará (UFC). O objetivo desse questionário é compreender o nível de conscientização e percepção dos alunos da UFC Campus Itapajé sobre os ataques de engenharia social, bem como avaliar as práticas de segurança adotadas. Sua participação é essencial e muito valiosa para o desenvolvimento deste trabalho.

Todas as respostas serão voluntárias, anônimas e confidenciais, sendo utilizadas exclusivamente para fins acadêmicos. O tempo estimado para a conclusão do questionário é de 3 minutos. Agradeço a sua colaboração!

TERMO DE CONSENTIMENTO

Eu declaro que fui devidamente informado(a) sobre a pesquisa intitulada “A psicologia por trás dos ataques de engenharia social”, conduzida por Lívia Maria Mota Brandão, no âmbito do Trabalho de Conclusão de Curso da Universidade Federal do Ceará (UFC). Fui esclarecido(a) sobre os objetivos do estudo. Compreendo que minha participação é voluntária e que posso desistir a qualquer momento sem prejuízo ou necessidade de justificativa.

Os dados coletados serão utilizados exclusivamente para fins acadêmicos e serão anonimizados para garantir a minha privacidade, impedindo qualquer possibilidade de identificação. A pesquisa segue os princípios éticos estabelecidos pela UFC, garantindo o sigilo e a confidencialidade das informações fornecidas. Fui informado(a) de que os resultados poderão ser divulgados em trabalhos acadêmicos, artigos científicos e eventos da área, sempre resguardando minha identidade.

Ao concordar em participar, afirmo que estou ciente dos aspectos da pesquisa e autorizo o uso das informações fornecidas para os fins mencionados.

- ☐ Eu li o Termo de consentimento livre e esclarecido e aceito responder esta pesquisa.

PRIMEIRA SEÇÃO - Perfil do participante

1. Qual sua faixa etária?

( ) Menor de 18 anos

( ) 18 a 25 anos

( ) 26 a 30 anos

( ) Acima de 30 anos

2. Em qual curso você está matriculado?

( ) Segurança da Informação

( ) Ciência de Dados

( ) Análise e Desenvolvimento de Sistemas

3. Em qual período do curso você está atualmente matriculado?

( ) 1º semestre

( ) 2º semestre

( ) 3º semestre

( ) 4º semestre

( ) 5º ou mais

SEGUNDA SEÇÃO - Experiência e Percepção sobre Engenharia Social

4. Você já ouviu falar sobre engenharia social?

( ) Sim, conheço bem o tema

( ) Sim, já ouvi falar, mas não sei muitos detalhes

( ) Não, nunca ouvi falar

5. Você acredita que ataques de engenharia social utilizam princípios psicológicos para manipular as vítimas?

( ) Sim, acredito que são amplamente utilizadas

( ) Sim, mas acho que seu impacto é limitado

( ) Não, os ataques ocorrem mais por falhas técnicas

6. Quais emoções você acredita que são mais exploradas em ataques de engenharia social? (Marque todas as que se aplicam)

( ) Medo

( ) Confiança

( ) Curiosidade

( ) Urgência

( ) Ganância

( ) Outra. Qual? _____

7. Você já foi vítima de um ataque de engenharia social?

( ) Sim, já fui vítima

( ) Não, nunca fui vítima

( ) Não sei dizer

8. Quais medidas você adota para se proteger contra ataques de engenharia social? (Marque todas as que se aplicam)

( ) Verifico links e remetentes antes de clicar

( ) Evito compartilhar informações pessoais com desconhecidos

( ) Utilizo autenticação em dois fatores (2FA)

( ) Não compartilho informações pessoais em redes sociais

( ) Nenhuma medida específica

9. Com que frequência você verifica a autenticidade de mensagens suspeitas recebidas por e-mail ou redes sociais?

( ) Sempre verifico antes de agir

( ) Às vezes verifico

( ) Raramente verifico

( ) Nunca verifico

10. Você já recebeu mensagens ou e-mails suspeitos solicitando informações pessoais ou financeiras?

( ) Sim, com frequência

( ) Sim, mas raramente

( ) Não, nunca recebi

11. Quais plataformas você considera mais comuns para tentativas de ataques de engenharia social? (Marque todas as que se aplicam)

( ) E-mails

( ) Redes sociais (Instagram, Facebook, WhatsApp)

( ) Chamadas telefônicas

( ) Mensagens SMS

( ) Não sei

12. Você já realizou algum curso ou treinamento sobre engenharia social?

( ) Sim, participei de cursos ou eventos acadêmicos sobre o tema

( ) Sim, por conta própria (vídeos, artigos)

( ) Não, nunca recebi nenhum treinamento

TERCEIRA SEÇÃO - Lacunas de Conhecimento

13. Você acredita que a engenharia social deveria ser abordada de forma mais detalhada na UFC?

( ) Sim, é um tema essencial para a área e deve ser aprofundado

( ) Sim, mas de forma mais breve

( ) Não vejo necessidade

14. Você considera importante que o tema "engenharia social" seja abordado de forma mais detalhada no seu curso ou na instituição em que estuda?

( ) Sim, é um tema essencial para a área

( ) Sim, mas de forma mais breve

( )Não vejo necessidade

15. Quais iniciativas você considera mais eficazes para aumentar a conscientização sobre a engenharia social? (marque até 2 opções)

( ) Palestras e workshops com especialistas

( ) Simulações práticas de ataques

( ) Disciplinas específicas no curso

( ) Disponibilização de materiais online gratuitos

Obrigada por sua participação!