UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE ITAPAJÉ

CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

LARISSE CRUZ LUCAS

COMPREENDENDO A PSICOLOGIA DO *PHISHING*: UMA ABORDAGEM PRÁTICA CENTRADA NO USUÁRIO

ITAPAJÉ

2024

LARISSE CRUZ LUCAS

COMPREENDENDO A PSICOLOGIA DO *PHISHING*: UMA ABORDAGEM PRÁTICA CENTRADA NO USUÁRIO

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. João Henrique Gonçalves Medeiros Corrêa

ITAPAJÉ

2024

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)

L966c Lucas, Larise Cruz.
Compreendendo a psicologia do pishing : uma abordagem prática centrada no usuário / Larise Cruz Lucas. – 2024.
61 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Itapajé, Curso de Segurança da Informação, Fortaleza, 2024.
Orientação: Prof. Dr. João Henrique Gonçalves Medeiros Corrêa.

1. Segurança da informação. 2. Engenharia social. 3. Phishing. I. Título.

CDD 005.8

LARISSE CRUZ LUCAS

COMPREENDENDO A PSICOLOGIA DO *PHISHING*: UMA ABORDAGEM PRÁTICA CENTRADA NO USUÁRIO

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: 26/09/2024

BANCA EXAMINADORA

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

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

Prof. Me. Artur de Oliveira da Rocha Franco
Universidade Federal do Ceará (UFC)

Dedico este trabalho a minha mãe, que sob muito sol, fez-me chegar até aqui, na sombra.

AGRADECIMENTOS

Ao chegar ao fim desta jornada, é com gratidão que dedico este espaço a todos aqueles que, de alguma forma, contribuíram para que este trabalho se tornasse realidade.

A Deus, por ser minha fonte de força e sabedoria, guiando meus passos e acalmando meu coração nos momentos mais desafiadores.

A minha mãe, Marinete, que sempre esteve ao meu lado com amor, paciência e apoio. Você é o alicerce de todas as minhas conquistas. Tudo o que sou e o que alcancei é fruto dos valores que me ensinou.

Aos meus amigos de longa data, Ewerton, Janily Késsia, Viviane, que estiveram em todas as minhas graduações. Sou imensamente grata por ter amigos tão especiais e queridos ao meu lado durante todo esse tempo. Agradeço pela paciência e compreensão, e peço desculpas pela ausência ocasionada pelos compromissos acadêmicos. A amizade de cada um de vocês foi uma fonte constante de apoio e encorajamento, e sem dúvida, tornou minha jornada muito mais rica e significativa.

À Tatá, que entrou na minha vida como amiga durante a graduação e se tornou uma companheira incrível. Agradeço profundamente pelo apoio constante, pela compreensão e por estar ao meu lado em todos os momentos, tanto nos desafios quanto nas conquistas. Sou grata por cada momento compartilhado.

Aos meus amigos que fiz durante este período, que se tornaram uma parte importante desta jornada acadêmica. Agradeço por cada risada compartilhada, pelas conversas que me ajudaram a enfrentar os desafios do curso.

Aos meus professores e orientador, em especial Dr. João Henrique Corrêa, pelo apoio, paciência e orientação. Sua dedicação ao longo deste processo foi essencial para a concretização deste trabalho, e sou profundamente grata por sua sabedoria.

À Universidade Federal do Ceará Campus Jardins de Anita por proporcionar um ambiente acadêmico estimulante e enriquecedor. Sou grata por todas as oportunidades de aprendizado e desenvolvimento que a instituição ofereceu ao longo da minha jornada.

Aos técnicos administrativos e servidores do campus que sempre estiveram disponíveis para auxiliar com eficiência e cordialidade. Seus trabalhos muitas vezes invisíveis, mas essenciais, foi fundamental para que eu pudesse focar em meus estudos. Em especial, agradeço à Angélica, que além de ser uma amiga de longa data, contribuiu de maneira significativa para o sucesso deste trabalho. Agradeço também à técnica Bruna, cuja ajuda e apoio foram igualmente

valiosos.

A todos os participantes da pesquisa por dedicarem seu tempo e compartilharem suas experiências e percepções. Sua colaboração foi essencial para a realização deste trabalho e para a obtenção de resultados significativos. A contribuição de cada um é apreciada e fundamental para o sucesso deste trabalho.

Aos meus conhecidos e agregados, pessoas que, mesmo não estando diariamente em minha vida, ofereceram um olhar de compreensão, uma conversa breve, mas significativa, ou uma ajuda inesperada. Cada interação foi valiosa e me ajudou a manter a fé na minha caminhada.

A todos que, de alguma forma, ajudaram a abrir os caminhos para que eu pudesse seguir.

A todos, meu profundo e sincero agradecimento.

“A melhor maneira de ficar em segurança é nunca se sentir seguro.”

(Benjamin Franklin)

RESUMO

A segurança da informação tem se tornado mais relevante com o crescimento dos ataques cibernéticos, como engenharia social. *Phishing* é uma técnica de manipulação psicológica usada para enganar e convencer outras pessoas a revelar dados relevantes. Este trabalho busca analisar os aspectos psicológicos envolvidos nos ataques de *phishing* para entender o comportamento dos usuários. A pesquisa incluiu uma revisão bibliográfica e um questionário aplicado a estudantes de Análise e Desenvolvimento de Sistemas, Ciência de Dados e Segurança da Informação da UFC do Campus Jardins de Anita, abordando seu conhecimento, experiências e medidas preventivas em relação ao *phishing*. Os resultados mostram que, apesar de 94% identificarem sinais de *phishing*, 84% nunca receberam treinamento específico, demonstrando vulnerabilidades. Os ataques têm crescido globalmente em tempos de avanços tecnológicos, e a escolha deste tema é relevante para o desenvolvimento de estratégias de proteção e para melhorar a segurança cibernética. Sugere-se a realização de simulações e programas de educação contínua para melhorar a conscientização e a segurança digital dos usuários.

Palavras-chave: segurança da informação. engenharia social. *phishing*.

ABSTRACT

Information security has become more relevant with the growth of cyber attacks, such as social engineering. Phishing is a psychological manipulation technique used to deceive and convince other people to reveal relevant data. This work seeks to analyze the psychological aspects involved in phishing attacks in order to understand user behavior. The research included a literature review and a questionnaire applied to students of Systems Analysis and Development, Data Science and Information Security at UFC's Jardins de Anita Campus, addressing their knowledge, experiences and preventive measures in relation to phishing. The results show that although 94% identify signs of phishing, 84% have never received specific training, demonstrating vulnerabilities. Attacks have grown globally in times of technological advances, and the choice of this topic is relevant for developing protection strategies and improving cyber security. Simulations and ongoing education programs are suggested to improve users' awareness and digital security.

Keywords: information security. social engineering. phishing.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação vem ganhado relevância ao passo que os indivíduos se tornam mais dependentes de tecnologias digitais. Mesmo com os avanços tecnológicos tenham aprimorado as medidas de proteção, os ataques cibernéticos continuam a evoluir. Nesse sentido, a engenharia social destaca-se como uma técnica de manipulação psicológica usada para enganar e persuadir pessoas a revelar informações confidenciais.

Entre as maneiras mais usuais de enganar as pessoas está o *phishing*, um tipo de golpe onde criminosos na internet disfarçam mensagens falsas como se fossem verdadeiras, fazendo as pessoas darem dados importantes ou clicar em *links* perigosos. Esses golpes usam não só problemas com tecnologia, mas também a falta de conhecimento e percepção das vitimas sobre os riscos que existem.

O *phishing* é um ataque de engenharia social em que criminosos usam mensagens de e-mail falsas para enganar as pessoas a compartilhar informações confidenciais ou instalar *malware* em seus computadores. As vítimas percebem essas mensagens como sendo associadas a uma marca confiável, mas, na realidade, são o trabalho de golpistas. Os ataques de *phishing* contornam a maioria das medidas de segurança, tornando-os mais difundidos e sofisticados. Eles se espalharam além do e-mail para incluir VOIP, SMS, mensagens instantâneas, sites de redes sociais e jogos. Os criminosos também mudaram do envio de mensagens de e-mail em massa para ataques mais seletivos de "*spear-phishing*"que usam informações contextuais relevantes para enganar vítimas específicas (HONG, 2012).

O *phishing* é uma maneira fácil e muito usada de enganar, onde os atacantes imitam mensagens reais, como e-mails ou textos de instituições conhecidas para confundir as pessoas e pegar dados úteis como senhas e informações do banco.

O impacto de um ataque de *phishing* pode ser prejudicial tanto para indivíduos quanto para organizações. Quando uma pessoa é vítima em um golpe de *phishing*, isso leva ao roubo de dados pessoais e financeiros; portanto, a vítima pode sofrer com o pior cenário de roubo de identidade, fraude financeira e até mesmo danos à reputação. Em um nível organizacional, o ato de *phishing* pode levar a violações, resultando na perda de informações confidenciais, valor monetário perdido e destruição da confiança do cliente, além de penalidades legais e regulatórias que pode ser aplicado de acordo do impacto do *phishing*(RODRIGUES, 2023; SANTOS; MOREIRA, 2023).

Em uma pesquisa realizada pela *Kaspersky*, o Brasil foi o país mais atacado por

phishing via *WhatsApp* em 2022, com mais de 76 mil tentativas de fraude (KASPERSKY, 2022). Entre junho de 2022 até julho de 2023, houve aumento de 617% nas tentativas de golpe de *phishing*. No Brasil, representou um aumento de cinco vezes mais ataques (KASPERSKY, 2024).

Os ataques têm crescido globalmente ao longo dos anos. De acordo com o APWG (2024), no segundo trimestre de 2024, correspondente aos meses de abril, maio e junho, foram observados 877.536 ataques de *phishing*, embora o número geral de ataques relatados tenha permanecido relativamente estável. *Phishing* por meio de chamadas telefônicas e mensagens de texto tem sido cada vez mais utilizado para atacar clientes de bancos e usuários de serviços de pagamento (APWG, 2024b). As plataformas de mídia social foram mais uma vez o setor mais frequentemente atacado, representando 32,9% de todos os ataques de *phishing*. O valor médio de transferência eletrônica solicitado em ataques de BEC no primeiro trimestre de 2024 foi de US$ 89.520, um aumento em relação ao trimestre anterior. Contas do *Google Gmail* foram usadas em 72,4% de todos os golpes de comprometimento de e-mail comercial (BEC) (APWG, 2024b).

No segundo trimestre de 2023, o Relatório de *Phishing* de Marca revelou o *ranking* das marcas mais imitadas em ataques de *phishing*. A *Microsoft* liderou a lista, estando relacionada a 29% de todos os ataques de *phishing* globalmente. Em seguida, o *Google* ocupou a segunda posição com 19,5%, seguido pela *Apple* com 5,2%. As marcas *Wells Fargo* e *Amazon* vieram em seguida, representando 4,2% e 4% dos ataques, respectivamente. *Walmart* (3,9%), *Roblox* (3,8%), *LinkedIn* (3%), *Home Depot* (2,5%) e *Facebook* (2,1%) completaram a lista das dez marcas mais imitadas no trimestre (ADVISOR, 2023).

Phishing é um problema relevante para os usuários finais porque explora vulnerabilidades humanas, levando as pessoas a revelar informações sensíveis, como credenciais bancárias, senhas e dados pessoais. Este tipo de ataque afeta diretamente as pessoas de várias maneiras: perda financeira, roubo de identidade, perda de dados pessoais e privacidade e até mesmo comprometimento de contas corporativas.

O objetivo central deste trabalho busca analisar os aspectos psicológicos envolvidos em ataques de *phishing*, visando compreender o comportamento dos usuários diante dessas ameaças. Além disso, busca-se identificar padrões comportamentais desses estudantes de tecnologia da UFC Campus Jardim de Anita em situações de *phishing*, com o intuito de entender suas respostas e prever possíveis vulnerabilidades diante dessas ameaças.

Diante disso, a escolha deste tema decorre do aumento alarmante de ataques de

phishing, que exploram não só vulnerabilidades técnicas, mas também aspectos psicológicos dos utilizadores. Compreender esses fatores é importante para o desenvolvimento de estratégias de proteção eficazes. Além disso, a pesquisa contribuirá para estabelecer uma base teórica sólida sobre o tema, permitindo melhorias na segurança cibernética.

O restante deste trabalho está organizado da seguinte forma: na Seção 2 serão apresentados conceitos sobre segurança da informação, engenharia social e uma análise do *phishing*. Na Seção 3 terá a metodologia descrevendo os métodos utilizados para o desenvolvimento do trabalho. Na seção 4 os resultados, onde fornecerá compreensões sobre o impacto e as técnicas de *phishing*. E por fim, na Seção 5 será apresentado a conclusão e trabalhos futuros.

2 REFERENCIAL TEÓRICO

Neste tópico serão expostos alguns conceitos importantes relacionados a Segurança da Informação, Engenharia Social e temas relacionados a *phishing*.

2.1 Segurança da Informação

Uma vez que as empresas e organizações dependem cada vez mais de sistemas de informação para armazenar e gerenciar informações importantes e confidenciais, a segurança da informação é um assunto cada vez mais abordado nos dias atuais.

Segurança da informação pode ser entendido como quem garante a integridade e a proteção das informações de uma organização. Não se baseando apenas na proteção dos dados de um computador, mas também de um sistema, do ambiente externo à infraestrutura da empresa (CASTRO; PIMENTEL, 2010).

Pode ser entendido 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 e de uso de quem utiliza da informação, pelo ambiente ou infraestrutura que a cerca, pessoas com intenções duvidosas com a finalidade de obter, furtar, destruir tal informação (SÊMOLA, 2006).

Segurança da informação é um termo que se refere a medidas que são tomadas para proteger os sistemas de informação contra a negação de serviço a utilizadores aprovados, a intrusão, e a modificação não-autorizada dos dados ou da informação armazenada, em processo de transação, ou transacionada. Este fator inclui a segurança dos recursos humanos, material, documentação, das áreas e instalações, das comunicações e computacional, bem como as medidas tomadas para evitar, detectar, conter e documentar ataques que possam virtualmente afetar a evolução dos negócios (ABNT, 2005).

A segurança é a base sobre a qual podemos dar às organizações a possibilidade e a liberdade de depender das tecnologias para expandir os seus negócios. E para isso a segurança da informação possui três princípios norteadores, como mostra a Figura 1.

Dentre os pilares a confidencialidade é garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso. A integridade é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento. A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre

Figura 1 – Pilares norteadores da Segurança da Informação

Fonte: ABNT (2005)

que necessário (NBR, 2005).

Um dos grandes desafios é justamente conseguir manter essa estrutura da passagem destas informações de forma confiável e íntegra sem que haja a enorme dificuldade ou até mesmo a impossibilidade de captar de forma viável tais informações (PEIXOTO, 2006).

Para garantir a segurança da informação, é necessário que esses pilares trabalhem juntos de forma integrada na proteção dos dados da empresa. Além desses princípios citados acima existem outros princípios aplicados à segurança da informação, sendo eles: o não repúdio, autenticidade e a privacidade (STONEBURNER, 2001).

2.2 Engenharia Social

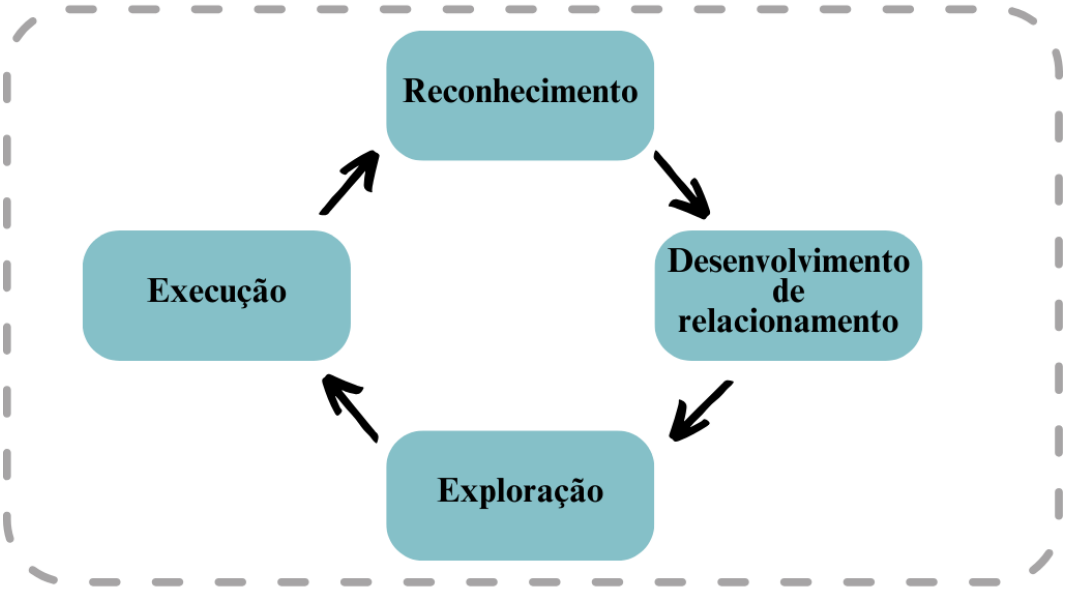
As pessoas são muito importantes para manter as informações seguras. Elas estão diretamente envolvidas nos processos de proteção das informações, tornando cada pessoa importante para manter as informações seguras (FONSECA, 2017).

A engenharia social envolve o uso de truques e psicologia para obter informações privadas. O engenheiro age como outra pessoa para obter informações conversando com familiares e amigos da vítima. A engenharia social engana as pessoas usando sua lógica cotidiana (HINTZBERGEN *et al.*, 2018).

O engenheiro social pode ser definido como uma pessoa que utiliza um conjunto de técnicas para a manipulação da confiança de outras pessoas para ter acesso às informações privadas. É possível também, 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, socialmente, financeiramente ou psicologicamente (MITNICK; SIMON, 2004).

Na Figura 2 mostra as fases de vida de um ataque de engenharia social, considerando a fase do Reconhecimento como a mais importante, pois nessa fase lida com a aquisição da informação de diversas fontes, informações que serão usadas pelo atacante durante o ataque (RUSSELL *et al.*, 2009).

Figura 2 – Fases do ataque de engenharia social



Fonte: adaptado de Heikkinen (2006)

Na fase de Desenvolvimento de Relacionamento se busca uma relação entre o atacante e a vítima para construir confiança (HADNAGY; MAXWELL, 2012). O atacante tem como objetivo ser "apreciado" pela vítima, para ser considerado confiável e não levantar suspeitas sobre o seu ato (MANN, 2008).

Já na fase de Exploração o alvo já está engajado, o invasor explora sua confiança, curiosidade ou emoções para atingir seus objetivos. Esta etapa pode envolver convencer o alvo a revelar informações confidenciais, como credenciais de login, ou a realizar ações que beneficiem o invasor, como baixar *malware* ou transferências bancárias (FERNANDES, 2023).

Na fase de Execução o atacante concretiza seu objetivo, ele utiliza as informações ou

ações obtidas nas etapas anteriores para atingir seus objetivos maliciosos (FERNANDES, 2023).

Os ataques de engenharia social giram em torno do uso da persuasão e da confiança por parte do invasor. Quando você experimenta esses hábitos, é mais provável que você faça coisas que não deseja. Os ataques geralmente induzem os seguintes comportamentos (KASPERSKY, 2018):

a) emoções fortes: a manipulação emocional pode dar aos atacantes uma vantagem nas interações. Você pode tender a correr riscos e cometer erros de maneira impulsiva. As seguintes emoções são frequentemente usadas para persuadir: medo, empolgação, curiosidade, raiva, culpa e tristeza;
b) urgência: oportunidades ou solicitações urgentes são outra ferramenta confiável no arsenal do invasor. O risco de cair em uma armadilha sob o pretexto de um problema sério que requer atenção imediata, ou se expor porque existe um prêmio ou recompensa que pode desaparecer se não agir rapidamente. Qualquer uma das abordagens desativa as habilidades de pensamento crítico;
c) confiança: a confiança é inestimável e essencial para um ataque de engenharia social. Como o invasor está mentindo, a confiança desempenha um papel importante. Eles fizeram pesquisas suficientes para criar uma história fácil de acreditar e com pouca probabilidade de levantar suspeitas.

Há algumas exceções a essas características a depender do caso, os invasores usam métodos mais simples de engenharia social para conseguir acessar a rede ou o computador, tudo isso vai de acordo com o método que o ataque vai usar.

O engenheiro social para alcançar seu objetivo se aproxima do seu alvo, conquistando sua confiança e atacando suas vulnerabilidades. Alguns fatores sociais são explorados pelo engenheiro, como: vaidade, curiosidade, persuasão e autoconfiança. Para alcançar seus objetivos os engenheiros sociais usam algumas técnicas, como (FONSECA, 2017):

a) análise do lixo: os 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 é uma das fontes mais ricas de informações para os engenheiros sociais;
b) *phishing*: 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, objetivando 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 IRC é um protocolo de comunicação pela internet utilizado, basicamente, 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: usa chamadas em cadeia, quando o objetivo é conseguir informações mais profundas de uma companhia ou pessoa. Realizando uma primeira ligação para conseguir dados pessoais ou empresariais, se passando por empresas ou patrocinadores. Na segunda chamada usa as informações da primeira para conseguir ainda mais informações com outra pessoa. E não são chamadas consecutivas para não se estabelecer conexão entre elas;

f) *trojan horse*: 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.

As técnicas usadas por engenheiros sociais nem sempre precisam ser complexas. Técnicas simples, mas eficazes são usadas também. Entre elas tem-se a técnica denominada *Phishing*, que tendo o termo surgido em 1996 ainda causa efeito (FERREIRA; ARAUJO, 2008).

Vale ressaltar que para a utilização de suas técnicas, o engenheiro social usa como sua principal vantagem à psicologia, explorando os pontos fracos de cada indivíduo e, em diversas ocasiões, explorando os medos de suas vítimas como meio de obter sucesso, no entanto, também utiliza a simpatia a fim de se mostrar uma pessoa agradável (PEIXOTO, 2006).

Essas técnicas usadas pelos engenheiros sociais podem ser divididas em duas categorias quanto ao modo do qual eles atuam, sendo elas: física ou psicológica. Na categoria física se encaixa: a análise do lixo; a presença física da pessoa com a técnica de olhar sobre os ombros para ter acesso a informações importantes sobre a pessoa; escuta telefônica, ou de conversas; ou buscar informações na mesa onde trabalha (DAWEL, 2005).

Na categoria psicologia as questões identificadas estão voltadas ao comportamento humano, qualidades do ser humano como honestidade, educação, prestatividade, honestidade e caráter das pessoas (LYRA, 2008). Quando junta essas características e as intenções maléficas

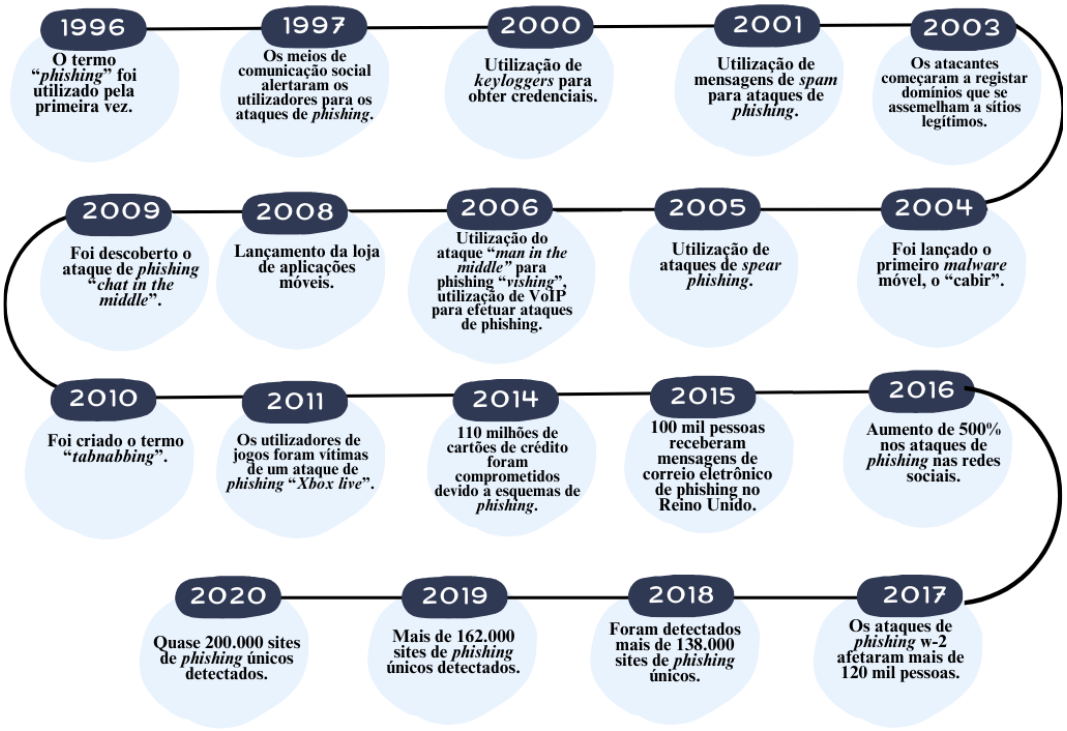
do engenheiro social, cresce a oportunidade de um ataque bem-sucedido.

2.3 *Phishing*

O termo *"phishing"*, originário da junção das palavras inglesas *"fishing"* (pesca) e *"phreaks"* (termo que designava os primeiros *hackers* (PHISHING.ORG, 2012). Traduzido livremente como “pescaria” ou “golpe de pescaria”, consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um *link* falso, acesse uma página falsa ou executar algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios. É uma técnica de engenharia social (PINHEIRO, 2020).

O termo foi primeiramente empregado em 1996 num fórum de notícias da provedora americana *American Online (AOL)* para designar ataques que estavam ocorrendo dentro de sua rede (PHISHING.ORG, 2012), como mostra a Figura 3.

Figura 3 – Evolução do *phishing*

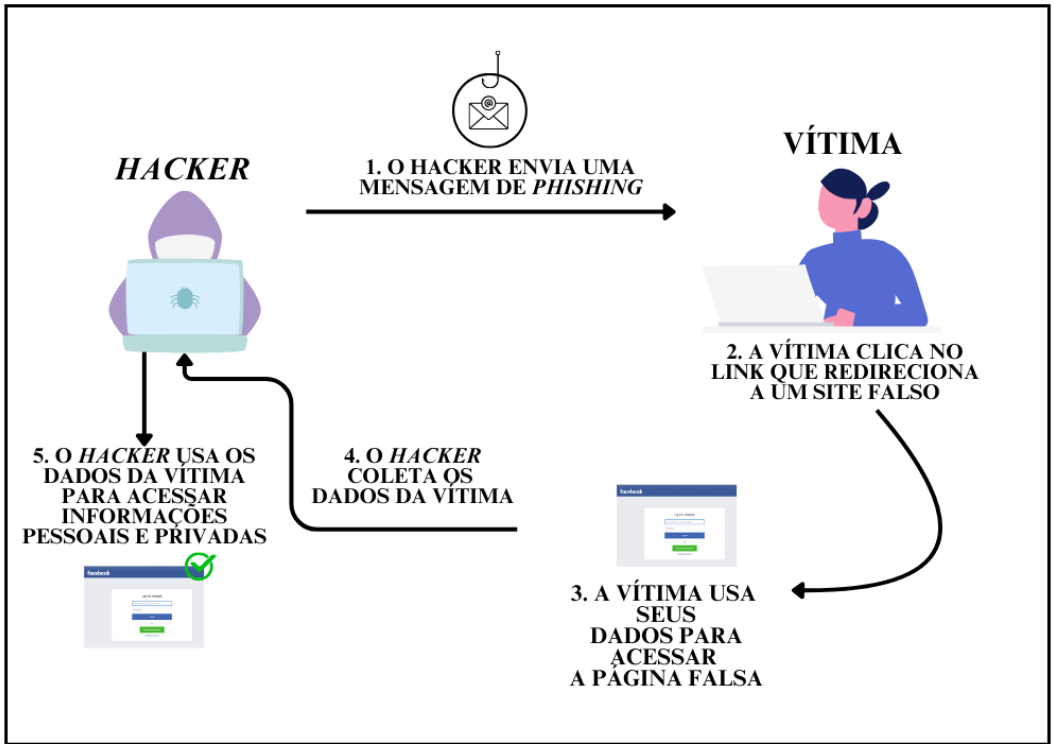


Fonte: adaptado de Ollmann (2007)

Desde então o *phishing* vem crescendo e com o avanço da tecnologia possibilitou que o *phishing* fosse se aperfeiçoando tornando-o mais eficaz devido ao aumento de recursos computacionais, o alcance de um ataque ficou cada vez maior.

O *phishing* funciona da seguinte forma: uma pessoa mal-intencionada envia uma mensagem eletrônica (pode ser um e-mail, um recado em uma página de relacionamentos etc.) a outrem e, utilizando-se de pretextos falsos, tenta enganar a pessoa receptora da mensagem e induzi-la a fornecer informações como número do cartão de crédito, senhas, dados de contas bancárias, ou, ainda, instiga a baixar e executar arquivos que permitam a futura subtração ou roubo de informações ou o acesso não autorizado ao sistema da vítima (CRESPO, 2011), como mostrado na Figura 4.

Figura 4 – Como funciona um ataque de *phishing*



Fonte: adaptado de Crespo (2011)

Um ataque de *phishing* típico é composto por três partes principais: isca, anzol e captura (JAKOBSSON; MYERS, 2006):

a) isca: Pode ser uma mensagem de correio eletrônico parecendo ser de organização legítima, um banco, um fornecedor de serviços de Internet, e que contém uma ligação para o gancho. O gancho é muitas vezes escondido através da ofuscação da URL (*Uniform Resource Locator*);

b) anzol: é um site falso que imita o site da instituição legítima à qual a vítima pode divulgar informações confidenciais;

c) captura: é que o atacante utiliza as informações recolhidas.

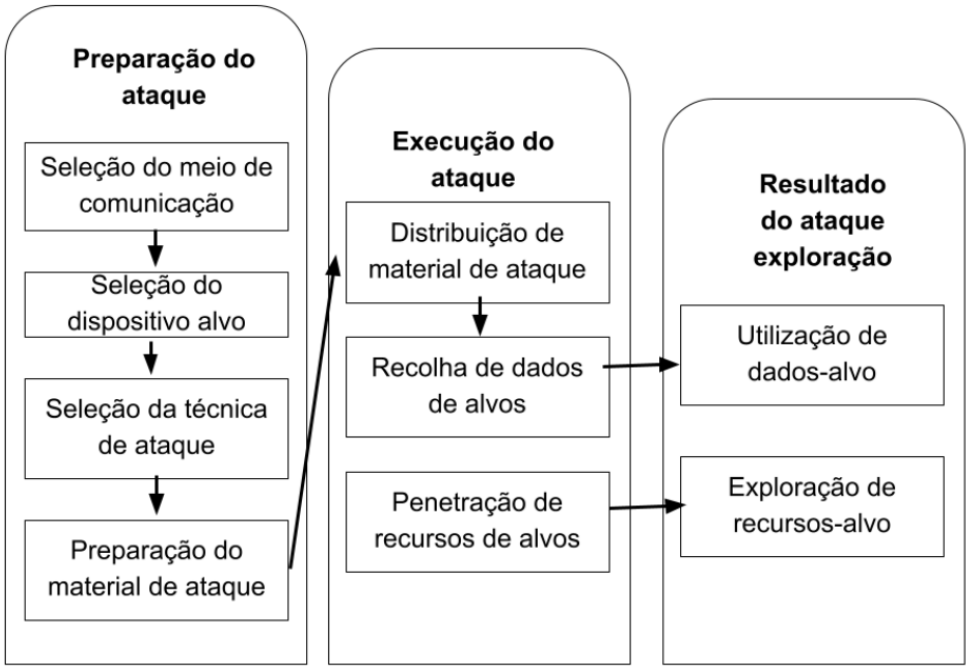
Os atacantes se utilizam dessas três partes para realizar um ataque de *phishing*, a

depender do tipo de ataque os componentes podem mudar, mas esses três componentes estarão presentes. O ataque de *phishing* geralmente usa vários truques para parecer mais real. Alguns desses truques são (JAKOBSSON; MYERS, 2006):

a) usar marcas, logotipos e imagens de empresas conhecidas para fazer a vítima acreditar que a mensagem veio delas. Muitas pessoas nem percebem o quão fácil é copiar essas coisas;
b) em alguns casos, o e-mail de *phishing* diz até para a pessoa não clicar nos *links*. Isso faz com que a mensagem pareça mais confiável, mas mesmo assim, muitas pessoas acabam clicando nos *links*;
c) falsificar o remetente do e-mail para parecer que veio de alguém confiável. A maioria das pessoas não sabe o quão fácil é falsificar um endereço de e-mail;
d) esconder e codificar *links* para disfarçar a página falsa.

Para que tenha sucesso no ataque, os criminosos têm passos para alcançar seus objetivos, cada passo feito é realizado de acordo com a abordagem que ele vai executar. Com os truques mencionados no parágrafo anterior, os atacantes passam por uma fase de preparação, escolha do meio de comunicação e a técnica usada. Esse planejamento é importante para a execução e pode ser observado na Figura 5.

Figura 5 – Fases do processo de um ataque de *phishing*



Fonte: Adaptado de (ALEROUD; ZHOU, 2017)

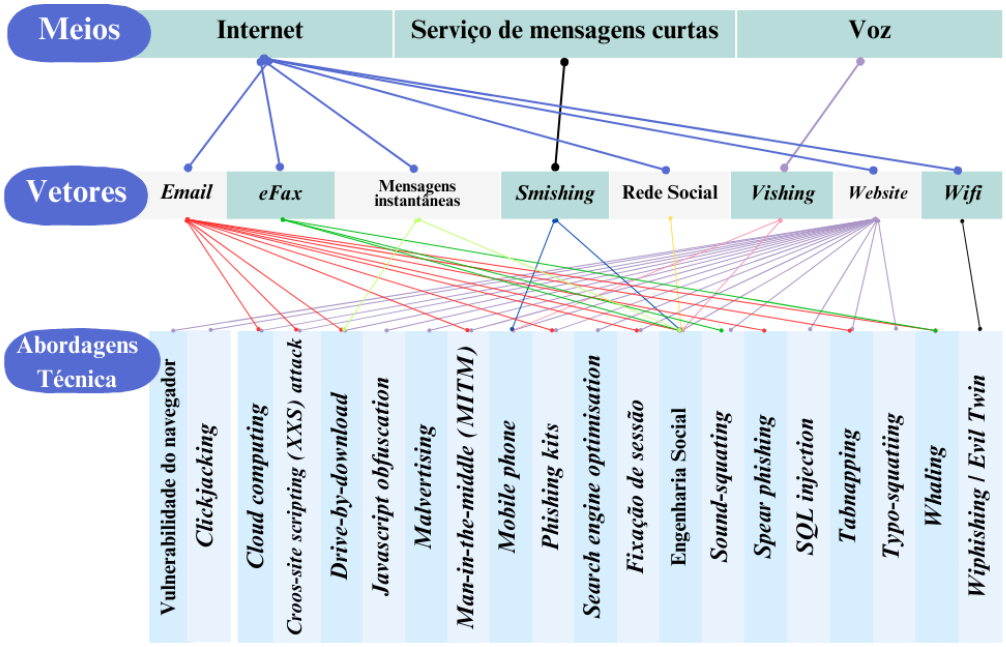
Como mostra na Figura 5 as fases de um ataque de *phishing* tem passos a serem

seguidos. Na fase de preparação do ataque tem que selecionar o meio de comunicação, o dispositivo alvo, a técnica que será utilizada para assim preparar o material para o ataque. Sendo selecionado o material vai para fase de execução de ataque onde será distribuído o material contaminado na coleção de dados do alvo ou em recursos. Desta forma o alvo vindo a usar o dado ou explorar o recurso pode acabar fornecendo dados sensíveis ou relevantes para o atacante.

2.3.1 Técnicas de phishing

As técnicas de *phishing* consistem em três componentes: vetores de *phishing*, vetores de propagação de ataque e métodos técnicos utilizados durante o ataque (CHIEW *et al.*, 2018). Como mostra a Figura 6.

Figura 6 – Meios, vetores e abordagem técnica de um ataque de *phishing*



Fonte: adaptado de (CHIEW *et al.*, 2018)

Para elaboração do ataque tem meios, vetores e a técnica que será usada na elaboração do ataque de *phishing*. No meio os atacantes podem abordar as suas vítimas através destes três meios: internet, voz e serviço de mensagens curtas. A conveniência e facilidade dos meios facilitam que os atacantes interajam com as suas vítimas numa tentativa de roubar informações pessoais (CHIEW *et al.*, 2018).

Existem vários vetores associados aos meios, a maioria dos vetores estão associados à Internet. Deste modo, a Internet é a escolha popular de meio para os atacantes (CHIEW *et al.*, 2018). Entre eles tem: e-mail; *eFax*: mensagens instantâneas, *smishing*, rede social, *vishing*,

website e Wi-fi.

O *vishing* ou *phishing* de voz, usa *software* de síntese de voz para deixar mensagens de voz notificando a vítima sobre atividades suspeitas em uma conta bancária ou de crédito. A chamada solicita que a vítima responda para verificar sua identidade, comprometendo assim as credenciais de sua conta. No caso do *smishing* é orientado a dispositivos móveis que usam mensagens de texto para convencer as vítimas a divulgar credenciais de contas ou instalar *malware*. *eFax* é uma versão digitalizada de um fax padrão (IBSEC, 2024).

Entre as abordagens técnicas vários vetores podem ser utilizados como vetores para implementação de um ataque de *phishing*, como mostrado na Figura 6. A seguir serão abordados os tipos de técnicas (CHIEW *et al.*, 2018):

a) vulnerabilidade de navegador: explorar a vulnerabilidade de um *browser* para lançar um ataque de *phishing* a um usuário, podendo usar usando extensões ou similares;
b) *clickjacking* (roubo de cliques): conhecido também como user interface UI *redressing attack*, é uma manipulação de UI de uma página *web*, possibilitando uma ação externa ao utilizar a página;
c) *cloud computing* (computação em nuvem): é o acesso sob demanda a recursos de computação: servidores físicos ou virtuais, armazenamento de dados, recursos de rede, ferramentas de desenvolvimento de aplicações, *software*, ferramentas analíticas impulsionadas por IA e outros, pela internet, com pagamento de acordo com o uso(IBM, 2024);
d) *cross-site scripting* (XSS) *attack* (ataque de *scripting* entre sítios (XSS): explora a vulnerabilidade de um *website* onde aceitam que o atacante injete um código malicioso dentro de algum campo de dados e o código permite que acesse informações pessoais das vítimas;
e) *drive-by-download* (Descarregamento automático): injetar um *malware* ou código malicioso em uma máquina apenas visitando um *websites*, podendo ser recebendo um email ou vendo um Linguagem de Marcação de Hipertexto (HTML);
f) *javascript obfuscation* (Ofuscação de *javascript*): usa o *JavaScript* para mascarar a barra de endereços, barras de status, barra de ferramentas ou área de menu, conseguindo assim falsificar os endereços;
g) *malvertising* (publicidade enganosa): usa um serviço de hospedagem online de

anúncios como meio de distribuir *malware*, que ao clicar no anúncio um *malware* infecta a máquina da vítima e explora suas vulnerabilidades com o objetivo de roubar informações;

h) *man-in-the-middle* (MITM - homem no meio): o atacante se coloca no meio de comunicação entre a vítima e uma aplicação *web*, ele é capaz de controlar as informações submetidas da vítima à aplicação *web* possibilitando a captura de credenciais de autenticação;
i) *mobile phone* (telefone celular): distribuição de aplicativos maliciosos para aparelhos de telefones móveis, que busca controlar a transferência de dados entre as aplicações do dispositivo, possibilitando a captura de informações pessoais;
j) *phishing kits*: ferramentas que possibilitam criar *websites*, e-mails e *scripts* para obter dados inseridos pelo usuário sem a necessidade de programação;
k) *search engine optimisation* (Otimização de motores de busca): otimizar a entrega de *websites* de *phishing* para potenciais vítimas usando técnicas de otimização para ferramentas de busca;
l) *session fixation* (Fixação da sessão): roubar identificadores de sessões gerados quando um usuário faz login em um site com esse tipo de falha de segurança, permitindo que o atacante use a seção do usuário para efetuar atividades maliciosas;
m) engenharia Social: técnicas de engenharia social para obter informações, ou vantagens sobre a vítima;
n) *sound-squatting*: registar domínio de site com nomes similares aos de site legítimos, levando a vítima a se confundir e ser levado a uma versão de *phishing* do *website* que deseja acessar;
o) *spear phishing*: ataque direcionado a um indivíduo, um grupo ou organização, que se cria um e-mail com conteúdo relevante e que a vítima conhece o remetente, evitando assim suspeitas da vítima e possibilitando efetuar solicitações de detalhes de login ou mesmo algum *malware*;
p) *Linguagem de consulta estruturada (SQL) injection* (injeção de SQL): roubo de abas de navegador. O atacante envia um e-mail que é aberto no navegador da vítima, o site tem um código que monitora a atividade do navegador, carrega a tela de login conhecida pela vítima, ela vai achar que a sessão foi fechada sendo

indispensável entrar novamente;

q) *typo-squating* (Erro de digitação): o atacante registra nomes de domínio com possíveis erros de digitação que o usuário possa fazer e com isso propiciando o acesso acidental ao site malicioso e baixando um *malware* no dispositivo da vítima;

r) *whaling*: um tipo de *spear phishing* com alvo pessoas de alto nível executivo e com altos privilégios de acesso na organização, que através de um *malware* o atacante tem acesso às informações de toda a organização;

s) *wiphishing/evil twin*: o atacante usa redes sem fio se colocando entre o usuário e a verdadeira rede sem fio, possibilitando assim que ele seja capaz de espionar os dados enviados e recebidos pelo usuário.

Essas técnicas exploram vulnerabilidades nos navegadores, sistemas operacionais, e dispositivos móveis, ou utilizam a engenharia social para enganar os usuários. Além disso, o uso de kits de *phishing* e métodos como SQL *injection* e *malvertising* são algumas das táticas que tornam os ataques mais sofisticados.

Nos últimos anos, o uso das redes sociais tornou-se parte integrante do dia a dia, proporcionando conexões rápidas e interações mais fáceis. No entanto, esta popularidade também abriu novas portas para os cibercriminosos, que exploram estas plataformas como terreno fértil para ataques de *phishing*. Os métodos de *phishing* evoluíram, adaptando-se ao comportamento do usuário e às características únicas de cada rede social. Os ataques atuais não estão mais limitados a e-mails fraudulentos; os golpistas agora usam mensagens diretas, comentários e *links* em perfis aparentemente legítimos para enganar os usuários e coletar informações confidenciais.

Neste sentido o *phishing* de mídia social se refere a um ataque executado por meio de plataformas como *Instagram*, *LinkedIn*, *Facebook* ou *Twitter*. O objetivo do ataque é roubar dados pessoais ou obter controle de sua conta de mídia social. As informações coletadas pelos atacantes incluem credenciais de login de contas de mídia social, informações de cartão de crédito e informações pessoais sobre você que podem ser usadas para lançar outros golpes e ataques. O ataque de *phishing* no *Instagram* funciona da seguinte forma:

> Começa quando um criminoso cria uma página de *login* falsa no *Instagram*. Para enganá-lo, essas páginas falsas são criadas para se parecerem o máximo possível com o site real. Quando você fornece um ID de usuário e senha do *Instagram* para a página falsa, o invasor captura suas credenciais. Geralmente será redirecionado para a página de login real do *Instagram* para autenticação, mas o estrago já foi feito. Com suas credenciais do *Instagram*, o invasor tem acesso total à sua conta (MICRO, 2023).

Outra rede social que os atacantes usam é o *Linkedin* e funciona da seguinte forma:

> Os criminosos enviam e-mails, mensagens do *LinkedIn* e *links* para você para convencê-lo a divulgar informações confidenciais, dados de cartão de crédito, informações pessoais e credenciais de *login*. O agente da ameaça pode invadir sua conta do *LinkedIn* para se passar por você e enviar mensagens de *phishing* para suas conexões para coletar dados pessoais. O invasor também pode enviar e-mails que parecem vir diretamente do *LinkedIn*. Isso é possível devido ao fato de que o site oficial do *LinkedIn* possui vários domínios de e-mail legítimos, incluindo*linkedin@e.linkedin.com e linkedin@el.linkedin.com*. Isso torna difícil acompanhar os domínios autênticos contra os falsos que podem ser usados por um invasor. (MICRO, 2023)

Um ataque de *phishing* típico do *Facebook* é realizado por meio de uma mensagem ou *link* que solicita que forneça ou confirme informações pessoais. Entregue por meio de uma postagem do *Facebook* ou da plataforma do *Facebook Messenger*, muitas vezes é difícil separar a mensagem legítima de um amigo em potencial de uma tentativa de *phishing*. As informações obtidas através de uma tentativa de *phishing* no *Facebook* fornecem aos atacantes os dados necessários para acessar sua conta do *Facebook*. Você pode receber uma mensagem informando que há um problema com sua conta do *Facebook* e que você precisa fazer *login* para corrigir o problema. Essas mensagens têm um *link* conveniente para seguir que leva a um site semelhante ao *Facebook*. Assim que chegar a este site impostor, você será solicitado a fazer o *login*. A partir daí, o criminoso pode coletar suas credenciais. Preste muita atenção ao URL para ter certeza de que está sendo redirecionado para *www.facebook.com*. Qualquer outra coisa provavelmente será uma farsa. (MICRO, 2023).

Além de usar as redes sociais para aplicar os ataque de *phishing* os criminosos continuam a se modernizar e melhorar suas técnicas, um exemplo disso é o *deepfake phishing*. O *deepfake phishing* funciona da seguinte forma: inicialmente, os atacantes disseminam os conteúdos falsos por e-mail, SMS, redes sociais, aplicativos de mensagens. Eles frequentemente imitam o remetente legítimo, com os dados do banco da vítima ou empresa, para parecer autêntico. A fim de convencer seus alvos a realizarem as ações solicitadas, os cibercriminosos usam táticas psicológicas e de engenharia social. Os vídeos *deepfake* são projetados para manipular as emoções e o comportamento das vítimas. Entre os gatilhos utilizados, os mais comuns são (ISH, 2023):

a) autoridade: usam *deepfakes* de pessoas em posições de autoridade, como CEOs, policiais ou governantes, para ganhar a obediência da vítima;
b) escassez: dizem que a pessoa precisa agir rapidamente para evitar a perda de fundos, o fechamento da conta ou outras consequências negativas. Isso aumenta

o senso de urgência;

c) ameaça: ameaçam seus alvos com multas, encargos ou outras punições se não fornecer informações ou pagamentos. Isso desencadeia o medo e a ansiedade;
d) confiança: os *deepfakes* que imitam marcas ou pessoas familiares à vítima, como seu banco ou políticos, geram confiança no golpe. Ela acredita que o vídeo é legítimo;
e) reciprocidade: pedem um pequeno favor, como fornecer parte das informações solicitadas, o que pode levar a vítima a revelar mais por reciprocidade.

Se as táticas psicológicas funcionarem, as informações solicitadas serão fornecidas, como senhas, dados financeiros e outros detalhes confidenciais (ISH, 2023).

2.4 Estratégias de persuasão utilizadas em ataques de *phishing*

As ações dos ciberataques são guiadas por uma variedade de fatores, permitindo que eles desenvolvam estratégias eficazes para atingir os seus objetivos. Estes indivíduos ou grupos não só utilizam ferramentas tecnológicas avançadas, mas também exploram características comportamentais que lhes permitem realizar atividades ilegais de forma eficaz. Para atingir os objetivos que almejam, os atacantes compartilham algumas características em comum, incluindo:

a) determinação: os atacantes estão constantemente criando novas maneiras de atacar e comprometer a infraestrutura de segurança de uma organização. Eles procuram ativamente por novas vulnerabilidades que possam ser exploradas para realizar atividades maliciosas. A sua atitude firme é uma das principais razões pelas quais as empresas ainda são vítimas de ataques cibernéticos, apesar de possuírem tecnologia de segurança de última geração (MANAGEENGINE, 2022);
b) criatividade: os atacantes trabalham arduamente para pesquisar e atingir usuários e organizações específicas. Eles encontram novas maneiras de contornar os sistemas de segurança e planejam todo o ataque para evitar a detecção. Para realizar esse tipo de golpe, eles precisam ser criativos e sempre apresentar novas técnicas de evasão de defesa, como a capacidade de desabilitar ferramentas de segurança ou impedir que usuários legítimos acessem dados no caso de um ataque de *ransomware* (MANAGEENGINE, 2022);
c) curiosidade: faz com que os atacantes se interessem em se infiltrar em redes e

sistemas;

d) paciência: *hackear* é um processo completo, não apenas atos isolados. Os *hackers* dedicam tempo para observar, pesquisar e compreender cuidadosamente seus alvos e, uma vez que tenham informações suficientes para atacar as vulnerabilidades e especificações técnicas, entre outros detalhes, tentam atacar o sistema. Um bom exemplo dessa paciência é quando os atacantes permanecer indetectados em uma rede pelo maior tempo possível e esperam pacientemente para coletar dados em um ataque *man-in-the-middle* (MANAGEENGINE, 2022);
e) capacidade de correr riscos: quando violam as infraestruturas de segurança corporativa, assumindo um risco imenso. Eles estão cientes de que a consequência de serem presos são grandes (MANAGEENGINE, 2022).

Entendendo mais sobre os fatores psicológicos o psicólogo americano *Burrhus Frederic Skinner* (B.F. *Skinner*) foi amplamente reconhecido como um dos principais proponentes do *behaviorismo*, uma abordagem na psicologia que se concentra no estudo do comportamento observável e na influência do ambiente sobre esse comportamento (WIKIPEDIA, 2024). Ele argumentava que o comportamento humano é principalmente influenciado pelo ambiente e pelas consequências das ações individuais.

No contexto do condicionamento operante, as ações são afetadas pelas consequências que se seguem. Um engenheiro social pode empregar o condicionamento operante como uma estratégia psicológica para manipular e influenciar as pessoas de forma mais eficaz durante seus ataques. Existem quatro tipos principais de consequências nesse processo: reforço positivo, reforço negativo, punição positiva e punição negativa (DIO, 2024).

Reforço positivo ocorre quando um comportamento é seguido por uma consequência que é percebida como agradável ou recompensadora, aumentando assim a probabilidade de que esse comportamento se repita no futuro. Por exemplo, um engenheiro social pode incentivar a vítima a agir de uma determinada forma por meio de elogios ou promessas de ajuda (DIO, 2024).

O reforço negativo um comportamento resulta na remoção de um estímulo desagradável, o que também aumenta a chance de repetição do comportamento. Um engenheiro social pode utilizar ameaças ou pressão para motivar a vítima a agir. Após a cooperação da vítima, a remoção da pressão ou da ameaça pode ser vista como uma forma de reforço negativo (DIO, 2024).

Já punição positiva ocorre quando uma consequência desagradável é aplicada após

um comportamento, com o objetivo de diminuir a probabilidade de que o comportamento se repita. Um engenheiro social pode recorrer a consequências negativas, como chantagem emocional ou ameaças, para desestimular a vítima a agir de determinada maneira. O atacante pode prometer interromper a punição se a vítima cooperar (DIO, 2024).

E por fim, punição negativa envolve a remoção de um estímulo agradável após um comportamento, visando também reduzir a probabilidade de que o comportamento ocorra novamente. Nesse cenário, o engenheiro social pode ameaçar retirar algo valioso da vítima, como informações pessoais ou sua reputação online, caso ela não cumpra as instruções. A vítima pode evitar a punição negativa ao seguir as orientações do atacante (DIO, 2024).

A APWG (2024) identifica alguns preconceitos cognitivos e táticas utilizadas pelos atacantes de *phishing* que exploram esses vieses para enganar suas vítimas. Embora não seja listado diretamente os preconceitos cognitivos, suas publicações e relatórios frequentemente abordam como os atacantes utilizam estratégias psicológicas para aumentar a eficácia de seus ataques. Alguns das técnicas são: efeito de ancoragem, excesso de confiança, tática de urgência, apelo à autoridade, efeito de escassez, dissonância cognitiva e familiaridade.

O efeito de ancoragem os atacantes podem utilizar informações iniciais para influenciar a percepção das vítimas. Como por exemplo, um e-mail pode começar com uma informação aparentemente confiável ou alarmante, criando um estado de alerta que leva a vítima a agir rapidamente sem questionar. Usando logotipos oficiais ou endereços de e-mail que se assemelham aos legítimos para ancorar a confiança da vítima (APWG, 2024a).

Muitas pessoas acreditam que estão bem informadas sobre segurança e que não cairão em fraudes. Essa confiança excessiva pode levar à complacência. Diante disso, os atacantes exploram essa confiança ao criar mensagens que parecem normais e, portanto, não despertam desconfiança. Os atacantes frequentemente usam prazos curtos ou ameaças para criar um senso de urgência. Isso pode fazer com que as vítimas ajam rapidamente, sem pensar nas consequências. Frases como “Ação imediata necessária” ou “Sua conta será bloqueada” são comuns em e-mails de *phishing* (APWG, 2024a).

Os atacantes se passam por autoridades ou instituições respeitáveis para ganhar a confiança das vítimas. As vítimas tendem a obedecer a comandos dados por figuras de autoridade. Usando de táticas de criar e-mails que imitam comunicações de bancos, governos ou empresas conhecidas, instigando um senso de obrigação. O efeito de escassez, a ideia de que algo é limitado pode levar as pessoas a agir impulsivamente. Os atacantes exploram essa percepção

para induzir ações rápidas. Mensagens que afirmam que uma oferta ou uma ação é válida por um tempo limitado podem aumentar a pressão sobre a vítima (APWG, 2024a).

Dissonância cognitiva as vítimas experimentam conflito entre suas crenças e ações, podem buscar justificativas para suas decisões. Isso pode levar a decisões impulsivas, como clicar em um *link* malicioso. Mensagens que parecem oferecer uma solução fácil para um problema podem explorar essa dissonância. As pessoas tendem a confiar em informações que parecem familiares. Os atacantes usam isso para criar e-mails e sites que se assemelham a marcas conhecidas. Utilizando de elementos visuais, como logotipos e *design* de marca, que são familiares à vítima para aumentar a credibilidade (APWG, 2024a).

Esses preconceitos cognitivos e táticas psicológicas utilizadas por atacantes de *phishing* demonstram mais uma vez a importância da conscientização contínua e educação em segurança cibernética. Ao compreender como esses vieses são explorados, indivíduos e organizações podem se proteger melhor contra os ataques de *phishing* e melhorar sua capacidade de identificação de ameaças.

3 METODOLOGIA

A metodologia deste trabalho é composta por uma pesquisa bibliográfica e um questionário online. O Questionário que se encontra no Apêndice A foi realizado no período de 31 de julho a 30 de agosto de 2024, contando com 222 alunos com matriculas ativas, como público alvo os alunos dos cursos de Análise e Desenvolvimento de Sistemas (ADS), Ciências de Dados (CD) e Segurança da Informação (SI) do Campus Jardins de Anita da UFC. Esta abordagem proporciona uma melhor compreensão de como os aspectos psicológicos e comportamentais estão envolvidos no *phishing*, utilizando tanto métodos qualitativos quanto quantitativos.

Na grade curricular de SI, disciplinas como segurança de redes, criptografia, gestão de incidentes e auditoria de sistemas fornecem uma base para o entendimento de ataques cibernéticos, inclusive *phishing*. Em ADS, o foco está na construção e desenvolvimento de *softwares* e sistemas seguros, com disciplinas que envolvem programação, engenharia de *software* e desenvolvimento seguro de sistemas. Em Ciência de Dados, disciplinas voltadas para análise de dados, *machine learning* e *Big Data* são comuns. O foco do curso está em extrair informações valiosas de grandes volumes de dados. O entendimento sobre *phishing* se torna importante a medida que o conhecimento sobre *phishing* é importante para os estudantes de SI, pois buscam detectar, mitigar e prevenir ataques cibernéticos. O *phishing* é uma das técnicas mais usadas para comprometer redes e sistemas, explorando fraquezas na segurança humana. Estudantes de SI precisam entender tanto os aspectos técnicos quanto os psicológicos dos ataques para elaborar medidas de defesa e conscientização, tornando-se aptos a criar soluções que minimizem riscos e protejam organizações contra violações de dados.

A compreensão de *phishing* permite que os estudantes de ADS projetem sistemas mais resilientes a esse tipo de ameaça. Eles desenvolvem interfaces e funcionalidades que dificultem a ação de atacantes que tentam induzir usuários ao erro. Além disso, ao conhecer o *phishing*, eles podem implementar mecanismos de autenticação robustos e sistemas de detecção de fraudes, garantindo que o *software* desenvolvido esteja protegido contra esse tipo de ataque.

O *phishing* impacta os estudantes de Ciência de Dados ao lidar com a análise de comportamentos e padrões associados a ataques cibernéticos. Conhecer o *phishing* permite que eles identifiquem anomalias em dados que podem indicar ataques ou fraudes, desenvolvendo modelos preditivos para detectar tentativas de *phishing* em tempo real. Para todos os cursos, a conscientização sobre *phishing* é crucial. Isso inclui não apenas a proteção de sistemas, mas também que se possa entender seus conhecimentos sobre o assunto e como pode ser melhorado

de acordo com suas habilidades, a fim de desenvolver estratégias preventivas e corretivas que são cruciais para garantir a segurança da informação em um mundo digital.

Desta forma, o conhecimento sobre *phishing* é importante para os alunos dos cursos de SI, ADS e CD, pois não apenas treina esses futuros profissionais para proteger sistemas, dados e usuários, mas também os prepara para enfrentar um dos maiores desafios na segurança cibernética. Estar consciente desta ameaça é um passo fundamental para garantir que as soluções tecnológicas sejam eficazes, seguras e resilientes num ambiente digital cada vez mais frágil.

A revisão bibliográfica contém conceitos sobre segurança da informação, engenharia social, *phishing* e comportamento do usuário. Essa revisão busca identificar as principais teorias, estudos e práticas relevantes que fundamentam a pesquisa, permitindo uma base teórica para a análise dos dados coletados.

Na pesquisa de Matos (2017) ele analisa as características do ataque de *phishing*, os métodos psicológicos e tecnológicos utilizados pelos atacantes, e apresenta medidas de proteção que os internautas podem adotar. Além disso, o autor avalia a eficácia de ferramentas anti-*phishing* disponíveis no mercado, contribuindo para a conscientização e segurança dos usuários.

No trabalho de Chiew (2018) é realizada uma discussão sobre as abordagens de execução de ataques de *phishing*, o objetivo é apresentar uma revisão que melhore a compreensão das características utilizadas. Enquanto o Vishwanath; Sinha (2018) oferecem uma visão abrangente sobre a literatura existente e sugerem direções para futuras investigações. Essas contribuições são essenciais para compreender a dinâmica do *phishing* e desenvolver estratégias mais eficazes de prevenção e conscientização.

A dissertação de Gomes (2019) investiga o *phishing* via e-mail e propõe métodos de prevenção. Inicialmente, foram realizadas entrevistas com profissionais de Segurança da Informação para aprofundar o tema. Em seguida, um questionário online avaliou o conhecimento dos participantes sobre *phishing* e as medidas que adotam antes e após ataques.

O artigo de Pinto (2023) explora as vulnerabilidades humanas como o elo mais fraco na segurança da informação, destacando a importância de focar não apenas em soluções tecnológicas, mas também no comportamento dos usuários. A engenharia social utiliza psicologia e técnicas de manipulação para obter acesso a dados sensíveis por meio da exploração de fatores humanos, como a confiança excessiva e a falta de conscientização sobre ameaças. O artigo revisa as principais técnicas de ataque, como *phishing*, e sugere medidas preventivas, como o

treinamento e a conscientização dos colaboradores.

O questionário utilizado encontra-se no Apêndice A, com 20 perguntas diversas sobre dados demográficos, conhecimento, experiência, comportamento e atitude sobre o *phishing*, além da psicologia, percepção, educação e conscientização sobre o tema. Ele foi dividido em seis seções, conforme detalhado a seguir:

a) **seção 0 - Concordância em Participar da Pesquisa**: Termo de Consentimento Livre e Esclarecido (TCLE): Os participantes devem concordar em participar da pesquisa;
b) **seção 1: Dados Demográficos**: Coleta de informações básicas como idade, gênero, curso e semestre;
c) **seção 2 - Conhecimento e Experiência com *Phishing***: Avaliação do conhecimento prévio e experiências dos participantes com ataques de *phishing*;
d) **seção 3 - Comportamento e Atitude**: Investigação sobre como os participantes reagem a possíveis ataques de *phishing* e como avaliam a autenticidade de e-mails e sites;
e) **seção 4 - Psicologia e Percepção**: Análise da confiança dos participantes em identificar *phishing*, fatores que consideram importantes para a vulnerabilidade e percepção de sua capacidade de evitar ataques;
f) **seção 5 - Educação e Conscientização**: Avaliação da opinião dos participantes sobre a importância da educação em *phishing* e os métodos mais eficazes de conscientização.

Com a combinação de métodos qualitativos e quantitativos é explicada a importância de uma investigação do fenômeno do *phishing*. Ao passo que os primeiros fornecem uma perspectiva dos padrões de comportamento e conhecimento, a abordagem qualitativa revela os motivos destes padrões, levando a recomendações de prevenção mais fundamentadas e eficazes do *phishing*. O questionário utilizado encontra-se no Apêndice A.

4 RESULTADOS

Durante um período de um mês, o questionário foi aplicado com o objetivo de investigar as opiniões e o nível de conhecimento dos alunos em relação aos ataques de *phishing*. O público-alvo consistiu de estudantes dos cursos de Segurança da Informação, Análise e Desenvolvimento de Sistemas e Ciência de Dados da Universidade Federal do Ceará (UFC) do Campus de Itapajé. A aplicação do questionário culminou em um conjunto de 50 (cinquenta) amostras válidas, as quais representam os elementos de análise deste trabalho.

A pesquisa realizada sobre o conhecimento de *phishing* possui alguns aspectos legais que merecem consideração, especialmente no que diz respeito à coleta, ao armazenamento e ao uso de dados dos participantes. Primeiramente,foi garantido que a pesquisa estivesse em conformidade com as legislações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil. Essa regulamentação exige que os pesquisadores obtenham o consentimento informado dos participantes antes de coletar quaisquer dados pessoais, assegurando que eles estejam cientes dos objetivos da pesquisa, da natureza dos dados coletados e de como essas informações serão utilizadas, o que foi realizado antes de iniciar as perguntas.

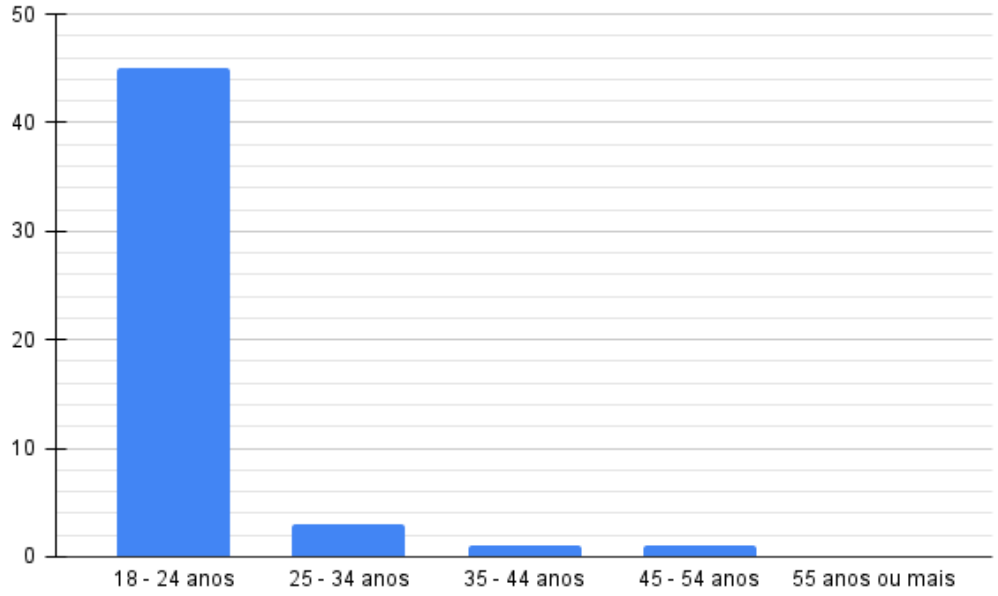
Além disso, é preciso garantir a confidencialidade e a segurança dos dados dos participantes durante e após a realização da pesquisa. Isso significa que medidas adequadas foram utilizadas para proteger as informações coletadas contra acessos não autorizados e vazamentos. A anonimização dos dados é uma prática recomendada, pois minimiza o risco de identificação dos participantes e ajuda a proteger sua privacidade.

Na primeira seção, composta por quatro questões, foi possível identificar o perfil dos estudantes. O gráfico da Figura 7 demonstra a classificação dos estudantes por faixa etária.

A faixa etária com maior representatividade foi de 18 a 24 anos, com 90%, seguida por 6% de 25 a 34 anos e 2% para a faixa etária de 35 a 44 anos e 45 a 54 anos. Portanto, ressalta-se que, a maioria dos estudantes que responderam ao questionário são jovens e adultos entre 18 a 24 anos de idade. O gráfico da Figura 8 demonstra a separação dos estudantes por gênero.

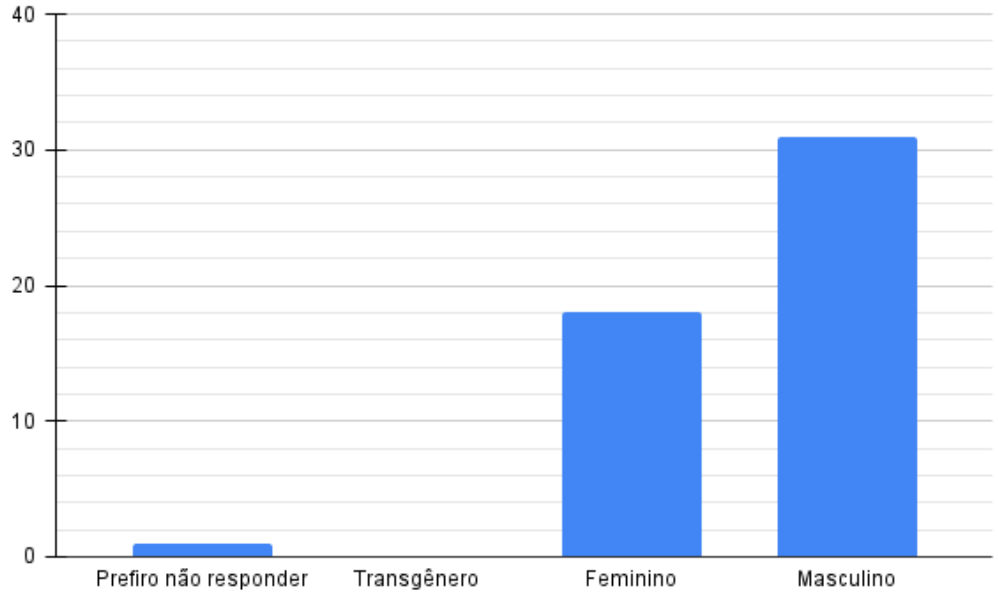
Dos pesquisados, 62% são do sexo masculino, 36% do sexo feminino e 2% não quis responder, demonstrando a relevante presença masculina na participação da pesquisa. Esses dados mostram uma predominância masculina entre os participantes, o que pode indicar uma maior representação desse grupo no contexto acadêmico dos cursos analisados. O gráfico da Figura 9 refere ao curso que estão matriculados.

Figura 7 – Distribuição da idade dos participantes



Fonte: Elaborada pela autora

Figura 8 – Distribuição por gênero dos participantes

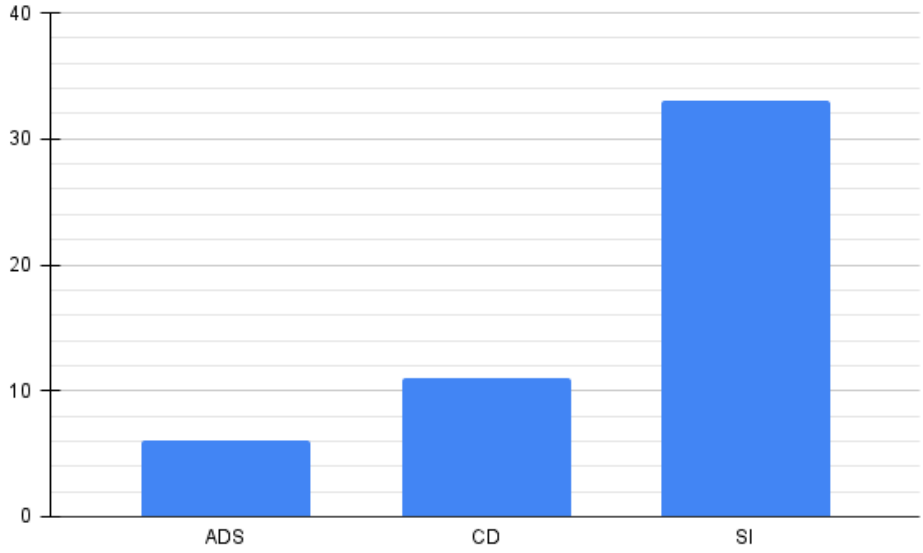


Fonte: Elaborada pela autora

De acordo com a Figura 9, é notória a participação dos alunos do curso de Segurança da Informação com participação de 66%, seguido pelos estudantes do curso de Análise e Desenvolvimento de Sistemas com 22% de participação, com 12% os alunos do curso de Ciência de Dados. O gráfico da Figura 10 apresenta o semestre que cada aluno está cursando.

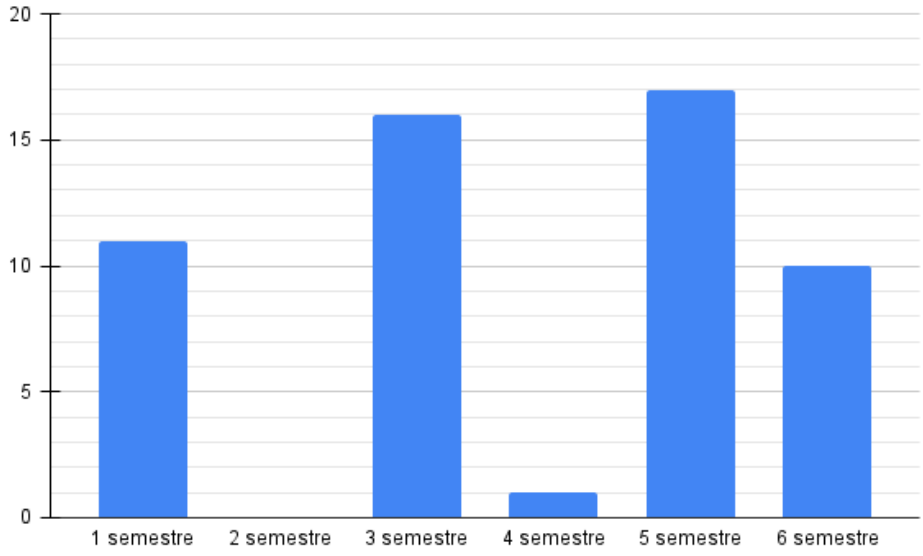
A maior parte dos alunos que responderam o questionário são do quinto semestre com 17 estudantes, seguido de 16 estudantes do terceiro semestre, 11 estudantes do primeiro

Figura 9 – Distribuição dos participantes por curso



Fonte: Elaborada pela autora

Figura 10 – Distribuição dos participantes por semestre



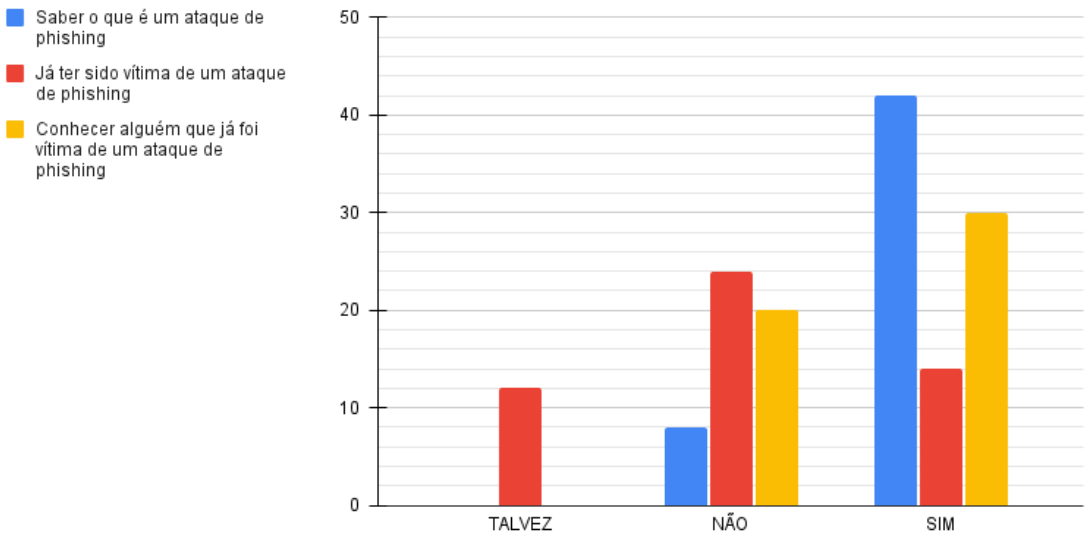
Fonte: Elaborada pela autora

semestre, 10 estudantes do sexto semestre e 1 estudante do quarto semestre.

A segunda seção é composta por quatro questões e refere-se a conhecimentos e experiência com *phishing*. O gráfico da Figura 11 é relacionado ao conhecimento sobre *phishing* que o estudante possui.

Por meio do Figura 11 é possível observar que grande parte dos pesquisados sabem o que é um *phishing* com 84% (42) o que é um ponto positivo para segurança do usuário quanto a esse tipo de ataque. Apenas 16% (8) não sabem o que é um *phishing*, ponto que a ser levado

Figura 11 – Conhecimento sobre *phishing*



Fonte: Elaborada pela autora

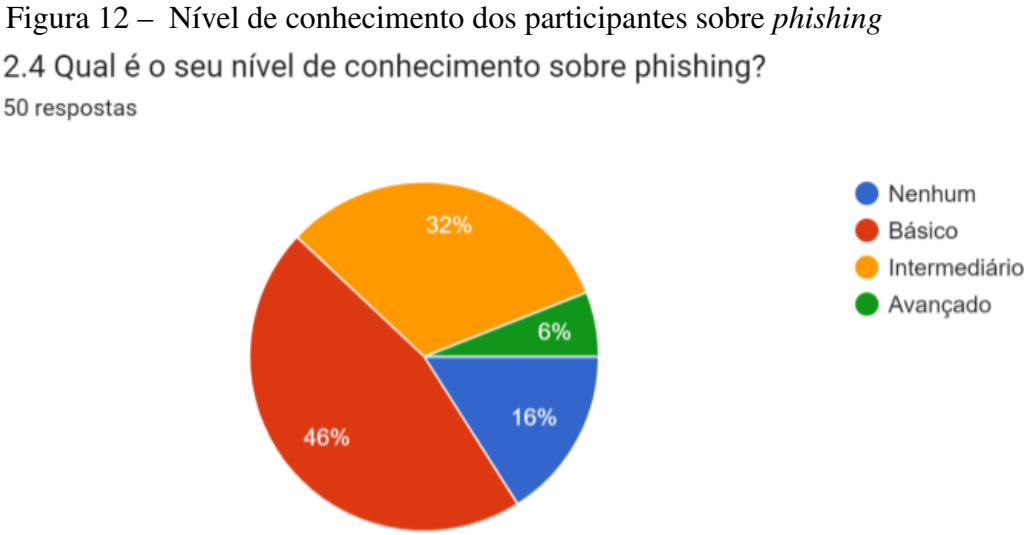
em consideração e surge como oportunidade de ação de conscientização. O gráfico da Figura 11 mostra ainda se o estudante foi vítima de um ataque de *phishing*.

É evidente através da Figura 11 que 48%, 24 dos participantes, não tinham sido vítimas de um ataque de *phishing*, seguido de 28% (14) que relataram terem sofrido algum tipo de ataque, e com 24% (12) afirmando que não tinham certeza de terem sido vítimas, sugerindo que uma parte relevante de usuários pode não ter conhecimento suficiente para identificar ou reconhecer um ataque de *phishing*. Isto destaca a importância de melhorar as capacidades de conscientização e detecção de tais ataques. O gráfico da Figura 11 contempla o aspecto sobre conhecer alguém que foi vítima de um ataque de *phishing*.

Em relação a conhecer alguém que já sofreu um ataque de *phishing*, 60% (30) afirmam que conhecem e 40% (20) afirmam que não conhecem. Mostrando que os ataques de *phishing* são comuns e uma grande proporção de pessoas tem indiretamente conhecimento deles, mesmo que nem todos sejam vítimas diretas. Os dados também destacam que o *phishing* é uma ameaça comum que não afeta apenas indivíduos específicos. O questionamento da Figura 11 tem a ver com nível de conhecimento de *phishing*.

Referente a Figura 12 temos que 46%, 23 relatam que possuem conhecimentos básicos sobre o assunto, indicando uma compreensão superficial dos conceitos e práticas de segurança. No entanto, essa parcela ainda apresenta lacunas que podem ser exploradas por ataques mais complexos ou menos óbvios, indicando a necessidade de treinamento contínuo. Entre os participantes, 32% (16) afirmam que tem conhecimento intermediário, o que sugere

Figura 12 – Nível de conhecimento dos participantes sobre *phishing*



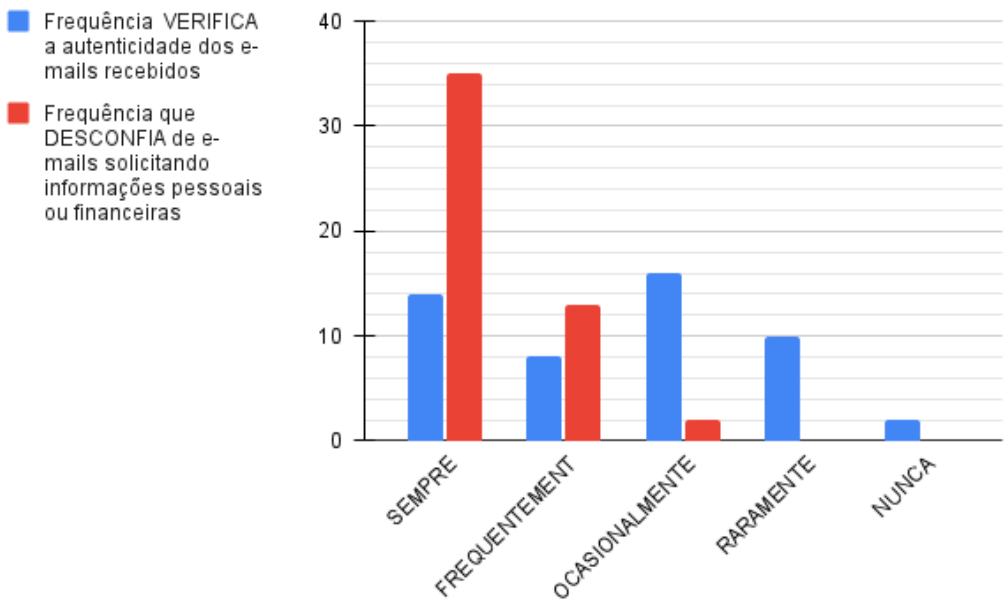
Fonte: Elaborado pela autora

uma capacidade moderada de identificar e evitar ataques de *phishing*, mas possivelmente ainda com algumas lacunas. Esses indivíduos podem ser alvos fáceis para ataques, pois não possuem ferramentas cognitivas ou técnicas para identificar sinais de alerta em e-mails ou mensagens fraudulentas. Esse dado é especialmente relevante, pois demonstra que uma parte significativa do público ainda está desprotegida frente a uma das ameaças de *phishing*. Uma parcela de 16% (8) afirmam que não tem conhecimento nenhum, o que os coloca em uma posição altamente vulnerável a esse tipo de ataque. Apenas 6% (3) responderam que possuem conhecimento avançado, mostrando que poucos possuem uma compreensão aprofundada e estão totalmente preparados para lidar com essas ameaças. Essa porcentagem sugere uma deficiência na formação e conscientização em segurança cibernética, o que ressalta a importância de programas educacionais mais intensivos e práticos que possam elevar o nível de conhecimento entre todos os usuários.

A terceira sessão é composta por três questões e se refere ao comportamento e atitudes com relação ao *phishing*. A Figura 13 mostra a frequência em que o estudante verifica a autenticidade dos e-mails recebidos.

Como demonstra no gráfico da Figura 13, 16 estudantes ocasionalmente verificam seus e-mails, o que pode sugerir uma prática irregular e, potencialmente, maior exposição a e-mails maliciosos. Entre os participantes, 14 sempre verificam, um grupo que provavelmente tem uma atitude mais proativa e, possivelmente, mais alerta a potenciais ataques. Um grupo de 10 estudantes raramente verificam, o que indica um comportamento que pode aumentar o risco de deixar passar mensagens fraudulentas sem que sejam notadas a tempo. Com uma rotina mais consistente, 8 frequentemente, tendo uma rotina mais consistente, embora ainda

Figura 13 – Prática de verificação e desconfiança sobre e-mails recebidos



Fonte: Elaborada pela autora

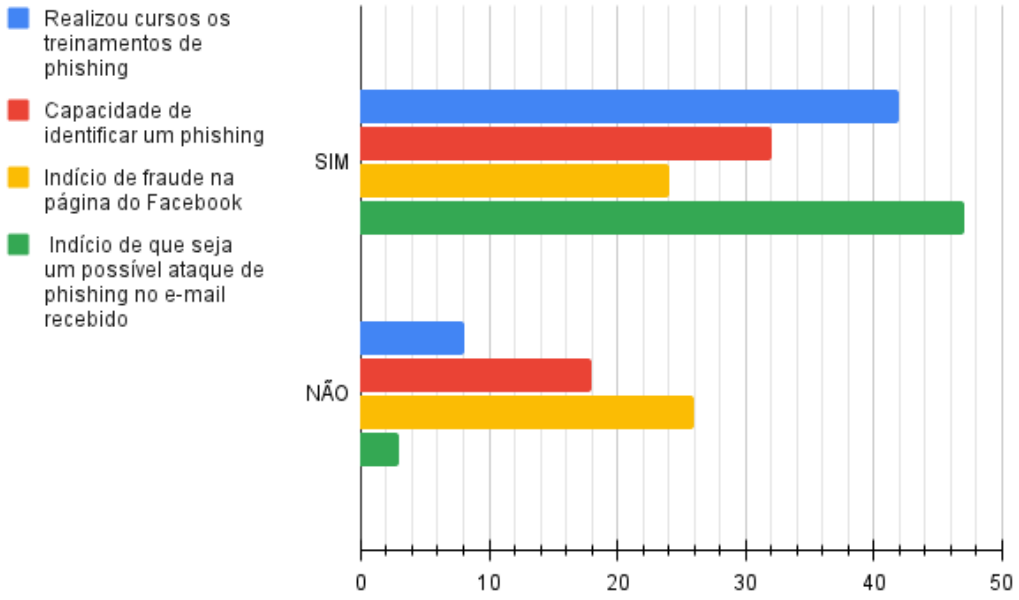
haja espaço para melhora. Somente 2 estudantes nunca verificam, o que pode indicar completa desconexão ou despreocupação com essa forma de comunicação, aumentando significativamente sua vulnerabilidade a ataques, já que e-mails de *phishing* podem passar despercebidos por longos períodos. A Figura 13 mostra o comportamento quanto a frequência que desconfia de e-mails solicitando informações pessoais ou financeira.

Por meio da Figura 13, é visível que 35 dos estudantes sempre desconfiam de e-mail solicitando informações pessoais ou financeiras, 13 frequentemente e 2 ocasionalmente desconfiam, sugerindo uma abordagem menos consistente ou uma menor percepção do risco associado a e-mails solicitando dados pessoais. Esses dados retratam uma atitude geral positiva em relação à segurança, onde a maioria dos estudantes adotando uma abordagem proativa para proteger suas informações contra possíveis ataques de *phishing*. A Figura 13 busca saber se o participante da pesquisa já tinha realizado curso ou treinamento sobre *phishing*.

De acordo com os dados da Figura 14, 42 dos participantes relataram que nunca fizeram curso ou treinamento sobre *phishing* enquanto 8 participantes relatam que já participaram. Essa falta de treinamento pode deixar os usuários menos preparados para identificar e lidar com tentativas de *phishing* de uma maneira eficiente. Esses resultados reforçam a necessidade de aumentar a oferta e a adesão a programas de treinamento e educação sobre segurança em relação ao *phishing*, para melhorar a proteção e a capacidade de resposta dos usuários a essas ameaças.

A quarta sessão é composta por sete questões e corresponde a psicologia e percepção.

Figura 14 – Relação de conhecimentos e habilidades de identificar um ataque *phishing*



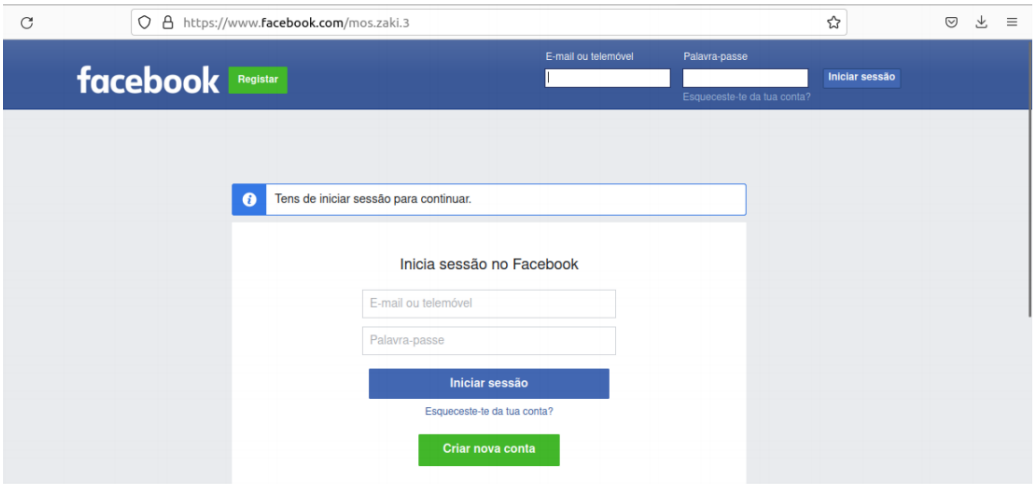
Fonte: Elaborada pela autora

A Figura 14 mostra a capacidade do participante identificar um *phishing*. Conforme disposto no gráfico da Figura 14 indicam que 32 acreditam que podem identificar um e-mail de *phishing* facilmente, e 18 afirmam que não conseguem identificar facilmente. Esse grupo pode estar mais vulnerável a ataques de *phishing* e pode se beneficiar de mais treinamento e recursos para melhorar sua capacidade de identificação e prevenção.

No gráfico da Figura 14 verifica as habilidades dos participantes de verificar uma página do *Facebook*. Quanto à possibilidade de verificar a página criada, conforme a Figura 15, 26 relataram que a página não tinha nenhuma modificação, que seria uma página real do *Facebook*. Outros 24 relataram que a página criada tinha modificações, indica que essa parte conseguiu perceber diferenças que podem ter sinalizado que a página era falsa. Levando em conta que a Figura 15 da pergunta 4.2 do Apêndice A, tem modificações que podem ser percebidas como variações na URL, sendo um dos sinais típicos de ataques de *phishing*.

A Figura 15 mostra alguns sinais típicos começando pelo URL incomum com "https:/www.facebook.com/mos.zaki.3", que não condiz com o formato típico de login do Facebook, geralmente “https:/www.facebook.com/login". A mensagem "Tens de iniciar sessão para continuar"uma tática para forçar o usuário a inserir suas credenciais na página. A capacidade dos participantes de identificar essas diferenças é importante para evitar cair em golpes, e a percepção de alterações na URL demonstra uma habilidade mais apurada para detectar fraudes.

Figura 15 – Pergunta 4.2 do questionário



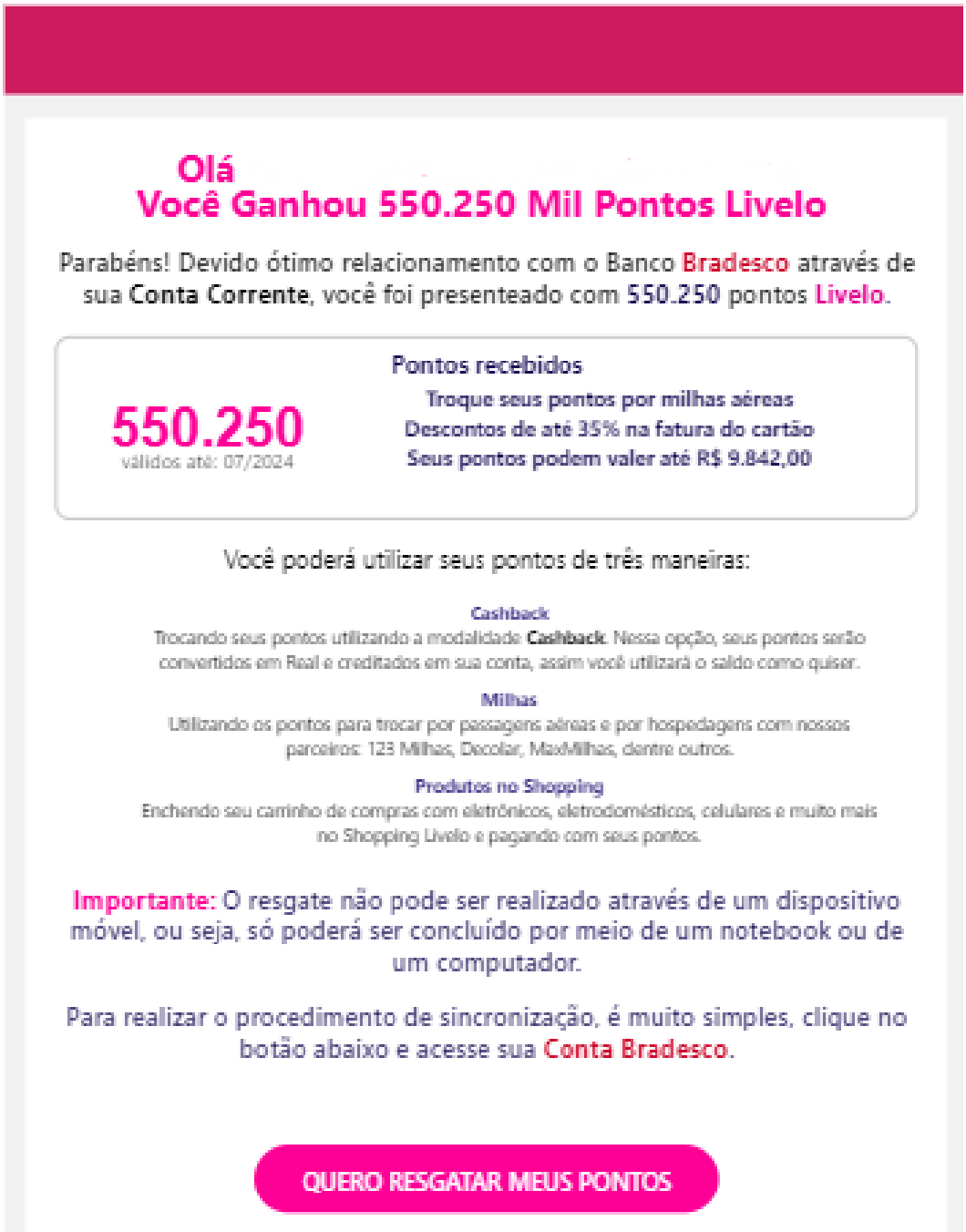
Fonte: Elaborada pelo autora

Já na Figura 14 é avaliado a capacidade de perceber um e-mail recebido seja um possível ataque de *phishing*, nela contém alguns indícios de ser uma tentativa de ataque de *phishing*, como: O número de pontos (550.250 pontos) é extremamente elevado; a mensagem menciona que os pontos expiram em "07/2024"e inclui um botão grande e destacado com o texto "QUERO RESGATAR MEUS PONTOS"; o aviso "O resgate não pode ser realizado através de um dispositivo móvel"sugere que o usuário deve usar um computador para realizar o procedimento. Esses indícios demonstram que a mensagem pode estar tentando induzir o usuário a clicar em *links* ou fornecer informações pessoais de forma enganosa, o que é típico em ataques de *phishing*.

Quanto à identificação do usuário em relação ao e-mail recebido, Figura 16, 47 acreditam que têm indícios de um ataque de *phishing*, como mostra o gráfico da Figura 14, e os outros 3 acreditam que não seja um possível ataque de *phishing*. Esse resultado mostra que a grande maioria tem um bom nível de conscientização sobre os sinais comuns de fraude cibernética. Mas sem esquecer que a minoria indica uma falta de percepção ou de conhecimento sobre as técnicas usadas em ataques desse tipo. A Figura 17 envolve a postura adotada por parte do participante ao receber um e-mail com uma suposta entrega.

Ao receber um e-mail com a Figura 18 referente a pergunta 4.4 do Apêndice A, como mostra a Figura 17, onde os estudantes revelaram que 21 apenas ignora, 11 verificam a fonte, 6 bloqueia o remetente, 5 apagam, outros 5 relata o e-mail, 1 afirmou não estar esperando nenhuma encomenda, ignora. Se estiver esperando verifica no aplicativo ou plataforma da compra se o código de rastreio é o mesmo, e caso seja, em todo é melhor verificar a situação de entrega do

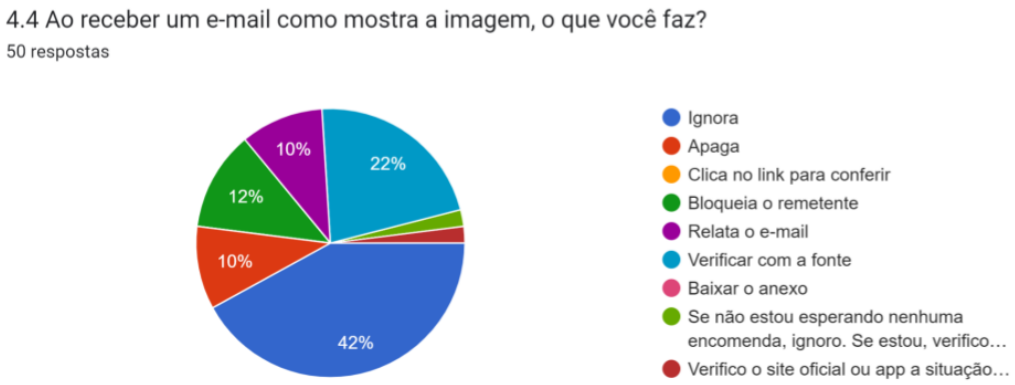
Figura 16 – Pergunta 4.3 do questionário



Fonte: Elaborada pela autora

pacote diretamente no site do distribuidor responsável. Uma pessoa faz a verificação no site ou aplicativo a situação da compra, para verificar o status do pedido. Neste tópico nenhum participante fez a opção de *download* do anexo, o que indica um bom nível de cautela em relação aos riscos associados à anexos desconhecidos. Importante destacar que nenhum dos participantes optou por fazer o *download* do anexo, o que indica um bom nível de cautela em relação aos riscos associados a anexos desconhecidos, frequentemente utilizados em ataques de *phishing* para distribuir *malware*. Esses dados mostram que, embora a maioria dos estudantes

Figura 17 – Ação tomada após receber um e-mail duvidoso



Fonte: Elaborada pela autora

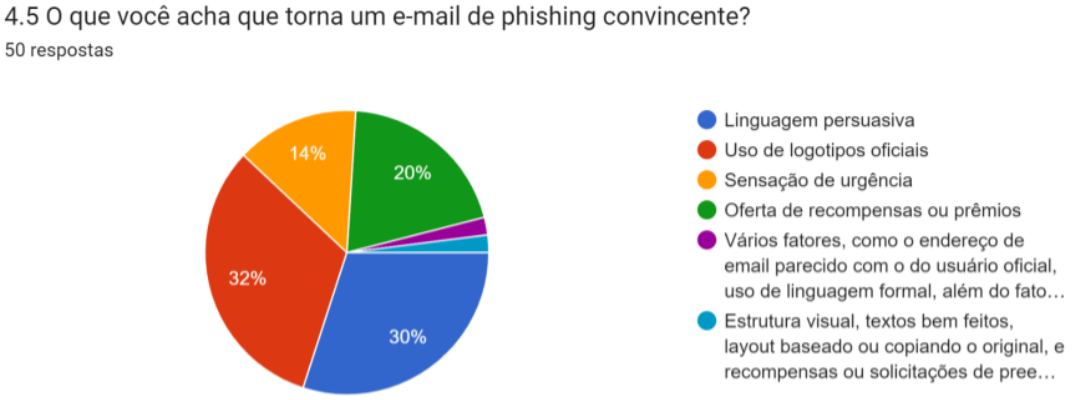
Figura 18 – Pergunta 4.4 do questionário

Fonte: Elaborada pela autora

adote práticas seguras, como verificar a fonte ou bloquear o remetente, há espaço para melhorar o comportamento diante de e-mails suspeitos, promovendo maior conscientização sobre a importância de sempre confirmar a legitimidade de qualquer comunicação antes de tomar qualquer ação. A Figura 19 se refere ao que torna um e-mail de *phishing* convincente.

Conforme disposto na Figura 19, é possível interpretar que dos participantes 16 acham que o uso de logotipos oficiais favorecem o convencimento de que o *phishing* seja legítimo. Outros 15 acham que linguagem persuasiva é o que torna o *phishing* convincente, 10 acreditam que seja a oferta de recompensas ou prêmios. Uma turma de 7 acreditam que seja a sensação de urgência, apenas 1 cita que vários fatores, como endereço de e-mail parecido com o do usuário oficial, uso de linguagem formal, além do fato do conteúdo do e-mail não seja tão extravagante. E outra pessoa respondeu que a estrutura visual, textos bem feitos, *layout* baseado ou copiado o original, e recompensas ou solicitações de preenchimento de dados para resolver

Figura 19 – Fatores que tornam um e-mail de *phishing* convincente para os participantes



Fonte: Elaborada pela autora

algo, tudo que imita com certa fidelidade a algum serviço de certa forma. Esses dados indicam que a combinação de elementos visuais e textuais familiares, aliados à manipulação emocional, são as principais técnicas utilizadas para tornar os ataques de *phishing* mais eficazes. A Figura 20 refere-se a confiança na capacidade de evitar ser enganado por *phishing*.

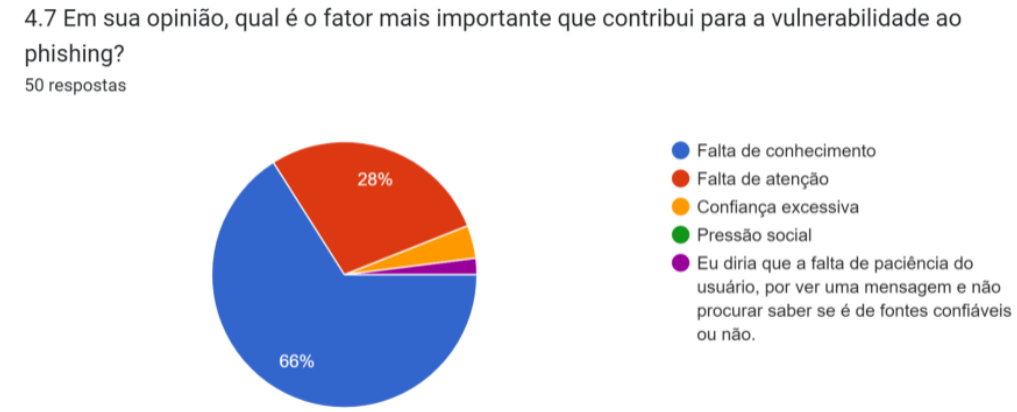
Figura 20 – Capacidade dos participantes de evitar um ataque de *phishing*

Fonte: Elaborada pela autora

Na Figura 20 tem a percepção dos estudantes sobre sua capacidade de evitar ser enganado por *phishing*, onde 25 se acham confiantes, o que sugere que metade dos estudantes acredita ter um nível razoável de habilidade para identificar e evitar essas ameaças. Outros 14 participantes se declaram neutros, o que pode indicar incerteza ou uma percepção de que podem ser vulneráveis a depender da situação. Um grupo de 6 participantes que se acham muito confiantes, essa parcela acredita estar altamente preparada para enfrentar tentativas de *phishing*.

Por outro lado, 4 pessoas relatam estar pouco confiantes, e um participante afirma não estar nada confiante, o que revela uma vulnerabilidade significativa em uma fração dos estudantes. Essas informações revelam uma variação significativa na autopercepção dos estudantes, com uma parte expressiva precisando de maior conscientização e treinamento para melhorar sua segurança contra *phishing*. O gráfico da Figura 21 demonstra a opinião dos estudantes sobre qual fator é mais importante para a vulnerabilidade ao *phishing*.

Figura 21 – Fatores de vulnerabilidade ao *phishing* entre os participantes



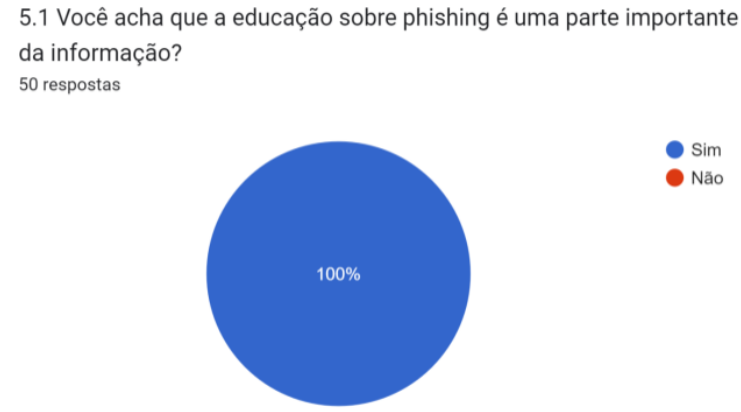
Fonte: Elaborado pela autora

Ao analisar os fatores que mais contribui para a vulnerabilidade, como mostra o gráfico da Imagem 21, 33 acreditam que seja a falta de conhecimento, 14 acreditam que seja a falta de atenção, 2 acreditam que seja por confiança excessiva e 1 acredita que seja a falta de paciência do usuário, por ver uma mensagem e não procurar saber se é de fontes confiáveis ou não. Esses dados ajudam a orientar estratégias de mitigação eficazes, como treinamentos personalizados que abordam tanto o aspecto técnico quanto os fatores comportamentais. Ao entender quais elementos tornam as pessoas mais suscetíveis a ataques, é possível desenvolver intervenções que reduzam essas vulnerabilidades, melhorando a resiliência contra *phishing*.

A quinta seção, que é composta por quatro questões, abrange a educação e a conscientização sobre *phishing*. A Figura 22 busca a opinião dos participantes sobre a educação sobre *phishing* ser uma parte importante da formação em segurança da informação.

O gráfico da Figura 22 mostra que 100%, ou seja, os 50 participantes acham que educação sobre *phishing* é uma parte importante da formação em segurança da informação, esse fato demonstra o consenso absoluto sobre o assunto. A resposta unânime reforça a necessidade de incorporar a pesquisa e a conscientização sobre *phishing* nos currículos educacionais, já que a formação teórica e prática é importante para os futuros profissionais lidarem com esse tipo de

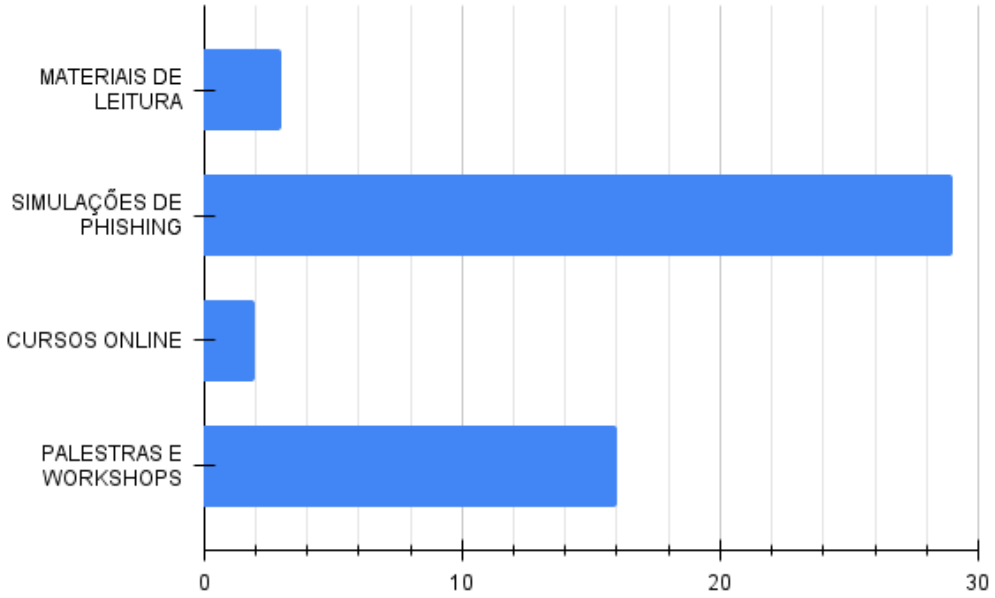
Figura 22 – Impacto do *phishing* na segurança da informação dos participantes



Fonte: Elaborada pela autora

ameaça. No gráfico da Figura 23 demonstra quais os métodos de educação sobre *phishing* são considerados mais eficazes.

Figura 23 – Métodos de educação sobre *phishing* mais eficazes para os participantes



Fonte: Elaborada pela autora

Os números da Figura 23 mostram que 29 participantes consideram as simulações de *phishing* mais eficazes, mostrando a importância do aprendizado prático e da experiência direta para entender as táticas de *phishing*. Seguido de 16 com palestras e *workshops*, onde fornece uma base teórica e prática ao mesmo tempo, onde poderia ser utilizado especialista na área para valorizar mais ainda o assunto. Depois tem 3 pessoas que acreditam que materiais de leitura podem ajudar na educação sobre *phishing*, o que pode indicar que algumas pessoas preferem se aprofundar no assunto por meio de textos especializados e outras duas pessoas

cursos online. Esses dados podem refletir a necessidade de formas mais dinâmicas e envolventes de aprendizado. Por fim, tem o gráfico da Figura 24 que mostra se as simulações de *phishing* ajudam a melhorar a conscientização.

Figura 24 – Simulações de *phishing* para conscientização

Fonte: Elaborada pela autora

De acordo com o resultado obtido na Figura 24, sendo 98%, 49 pessoas acreditam ajudar a melhorar a conscientização, é notório a importância deste método como uma forma de conscientização. Sabendo que a abordagem prática das simulações, ao reproduzir condições reais, auxilia na fixação do conhecimento e na melhoria do comportamento preventivo. Deste modo, as simulações se destacam como uma metodologia altamente valorizada para reforçar a educação e aumentar a capacidade dos estudantes de reconhecer tentativas de *phishing*. Uma pessoa que não acredita que as simulações sejam importantes.

Nesta seção foi realizado uma pergunta aberta que visava saber sobre sugestão ou comentário sobre como melhorar a prevenção contra *phishing*. Obtiveram-se sugestões do que poderia ser realizado e implementado. Dentre as sugestões podemos destacar:

> Para melhorar a prevenção contra *phishing*, é essencial combinar educação, medidas técnicas, políticas robustas, ferramentas adequadas e colaboração. Realize treinamentos regulares e simulações de *phishing* para conscientizar os funcionários. Utilize filtros de *spam*, autenticação multi fator e mantenha os sistemas atualizados. Estabeleça políticas claras de segurança, conduza auditorias regulares e implemente soluções específicas de segurança cibernética. Monitore atividades suspeitas, compartilhe informações sobre ameaças com outras organizações e incentive a verificação cuidadosa de URL e a desconfiança de solicitações inesperadas de informações pessoais ou financeiras [1].

A sugestão acima mostra alguns vieses que podem ser implementados para melhorar a conscientização contra *phishing*. Realizar treinamentos regulares e simulações é importante,

[1] Informação fornecida pelo participante por meio da aplicação do questionário.

pois isso ajuda a reconhecerem sinais de ataques e como reagir adequadamente. As simulações de *phishing* são uma estratégia para aumentar a conscientização e preparar os estudantes para reconhecer e reagir adequadamente a ataques cibernéticos.

Uma abordagem é realizar campanhas de e-mails simulados, onde e-mails falsos que imitam ataques de *phishing* são enviados aos participantes, projetados para parecer legítimos e contendo *links* suspeitos ou solicitações de informações sensíveis. Com objetivo de avaliar a capacidade dos participantes de identificar esses e-mails fraudulentos e fornecer *feedback* sobre suas respostas, destacando a taxa de cliques e o número de informações solicitadas. Além disso, treinamentos práticos em segurança podem ser oferecidos, envolvendo cenários de *phishing* em tempo real, permitindo que os participantes pratiquem a identificação de e-mails e *sites* fraudulentos em um ambiente seguro.

Outra estratégia envolve simulações de resposta a incidentes, em que um ataque de *phishing* bem-sucedido é simulado e os participantes devem seguir os procedimentos de resposta da empresa, testando sua prontidão e a eficácia dos planos de segurança. A gamificação (uso de técnicas e dinâmicas de jogos para enriquecer outros contextos diversos) das simulações, através de jogos ou competições, torna o aprendizado mais envolvente, incentivando a participação e a retenção do conhecimento. Após as simulações, é fundamental realizar sessões de *feedback*, onde os funcionários podem discutir suas experiências, aprender com os erros dos outros e compreender a importância de relatar suspeitas de *phishing* rapidamente. Por fim, a avaliação contínua através de simulações regulares ajuda a manter a segurança cibernética como uma prioridade na cultura organizacional, assegurando que os colaboradores estejam sempre atualizados sobre as táticas mais recentes utilizadas pelos atacantes.

A conscientização contínua é uma das melhores defesas contra *phishing*, pois os atacantes frequentemente atualizam suas táticas. Além de utilização de filtros de *spam* e autenticação multifator que são ações recomendadas que ajuda a reduzir o risco de ataques bem-sucedidos, os filtros de *spam* ajudam a bloquear e-mails maliciosos antes que cheguem à caixa de entrada, enquanto a autenticação multifator adiciona uma camada extra de segurança além da senha.

Essas ações são importantes porque garantem uma proteção eficaz contra *phishing* e ataques cibernéticos. Políticas claras e auditorias regulares ajudam a manter práticas de segurança e identificar vulnerabilidades. Ferramentas de segurança, como antivírus e sistemas de prevenção de intrusão, oferecem proteção ativa contra ameaças. Outra sugestão dada foi que:

> O público mais atacado com golpes desse tipo tendem a ser a geração mais velha,

> não só idosos, mas com idade entre 30-60 anos, logo, seria interessante a criação de *workshops* e simulações focando nesse público alvo. Não que a geração mais nova não tenda a cair nesses golpes, mas tendo em vista que até mesmo esses ataques tendem a terem como alvo esse público, com a conscientização dos mais velhos, o índice cairia bastante[2].

A iniciativa de *workshops* oferecem uma oportunidade para o público mais velho aprender sobre *phishing* de maneira prática e interativa. Com essa atividades eles podem ver exemplos reais de ataques e entender como identificá-los e evitá-los. Experiências práticas ajuda a reforçar a teoria. Isso reforça a ideia de que “Aplicar propostas tanto teóricas como palestras, mas também ações práticas para melhor compreensão"com a implementação de que “Ensinar os usuários a reconhecer sinais de *phishing*, como erros gramaticais, URLs suspeitas e solicitações de informações pessoais. Incentivar o uso de senhas fortes e únicas e, se possível, gerenciadores de senhas para manter as credenciais seguras". Essa abordagem complementa a ideia de que é essencial aplicar propostas tanto teóricas, como palestras, quanto ações práticas para uma melhor compreensão. Como representado a seguir:

> Palestras públicas e práticas demonstrativas poderiam ser um diferencial, pois a educação virtual e a prevenção contra as engenharias de *phishing* são assuntos que não são muito abordados em instituições de ensino ou em outros meios populares, e que os "alvos"acabam tendo que aprender por si mesmos, seja como vítimas ou pesquisando a fundo sobre o tema [3].

Demonstrações e demonstrações públicas são cruciais para fornecer educação acessível e eficaz sobre *phishing*, um tópico frequentemente negligenciado em instituições educacionais e mídia popular. Essas atividades educam diretamente o público, reforçam a teoria e facilitam a aplicação do conhecimento, aumentando a conscientização, preparando os participantes para a conscientização sobre *phishing* e fortalecendo a segurança online.

---

2 Informação fornecida pelo participante por meio da aplicação do questionário.
3 Informação fornecida pelo participante por meio da aplicação do questionário.

5 CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho buscou analisar os aspectos psicológicos envolvidos em ataques de *phishing*, com o objetivo de compreender o comportamento dos usuários diante dessas ameaças. Para isso, foi conduzida uma revisão bibliográfica sobre *phishing* e sua relação com a engenharia social, além da aplicação de um questionário com estudantes da área de tecnologia da informação do campus da UFC Jardim de Anita.

O questionário abordou temas como o nível de conhecimento dos estudantes sobre *phishing*, suas experiências, e as medidas preventivas adotadas. A análise dos resultados revelou importantes percepções sobre as vulnerabilidades dos usuários e a percepção de risco associada aos ataques de *phishing*.

Entre os principais achados, destacam-se que 94% dos participantes identificaram indícios de *phishing* em e-mails suspeitos, enquanto 84% nunca participaram de cursos ou treinamentos sobre o tema. Além disso, 64% acreditam que conseguem identificar e-mails de *phishing* facilmente, mas ainda existe uma parcela significativa que demonstra insegurança. O estudo também evidenciou que 70% dos participantes sempre desconfiam de e-mails que solicitam informações pessoais ou financeiras. No entanto, também foi identificado que 84% dos participantes nunca receberam treinamento específico sobre *phishing*, o que pode explicar as lacunas observadas na capacidade de identificação e resposta a essas ameaças.

Além disso, os dados sugerem que a confiança dos usuários em sua capacidade de evitar ataques de *phishing* varia significativamente, com 50% dos estudantes se considerando apenas "*confiante*", enquanto 28% se mostram neutros, e 12% se consideram muito confiantes. Essas variações indicam a necessidade de programas de educação e treinamento mais eficazes e acessíveis.

Diante desses resultados, propõem-se alguns trabalhos futuros que podem ser desenvolvidos para ampliar o conhecimento e a eficácia das estratégias contra *phishing*.

Um ponto interessante que surgiu dos dados coletados é a possibilidade de estratificar os casos de *phishing* em que os participantes foram vítimas. Ao categorizar os tipos de *phishing* que levaram ao erro (*phishing* por e-mail, SMS ou redes sociais), seria possível identificar padrões específicos de vulnerabilidade entre diferentes grupos de usuários. Com o objetivo de analisar quais tipos de *phishing* são mais eficazes em determinados perfis de usuários, permitindo o desenvolvimento de medidas de proteção mais direcionadas.

Em continuidade a esta pesquisa, um trabalho futuro pode focar na criação de perfis

de risco dos participantes, associando o momento e a situação em que caíram em um golpe de *phishing*. A proposta é buscar entender as circunstâncias (período do semestre, carga de trabalho, nível de estresse) em que os indivíduos foram mais suscetíveis ao ataque. Com isso poderia ser possível identificar fatores comportamentais que aumentam a vulnerabilidade ao *phishing* e sugerir medidas específicas para reduzir esses riscos em situações de maior exposição.

Uma investigação futura poderia buscar indícios de *phishing* em *sites* de reclamação ou comunidades *online*. Alguns usuários recorrem a esses espaços para relatar experiências com fraudes, o que pode oferecer um banco de dados relevante para identificar tendências e novos métodos de ataque. Podendo verificar a frequência e os tipos de *phishing* mais relatados nessas plataformas, comparando com os casos identificados no estudo. Isso ajudaria a alinhar as ações preventivas com as práticas de *phishing* mais recentes no mundo real.

Uma possível extensão deste trabalho seria a expansão da amostra para incluir não apenas estudantes do campus, mas também os Técnico-Administrativos em Educação (TAEs) e docentes. Esses grupos têm perfis e rotinas de uso de tecnologia diferentes, o que pode trazer novos compreensões sobre o comportamento frente ao *phishing*. Obtendo uma visão mais abrangente sobre o comportamento dos profissionais da área educacional diante de ataques de *phishing*, possibilitando um treinamento específico para cada grupo.

A implementação de simulações de *phishing* em ambientes educacionais e profissionais para avaliar o impacto dessas atividades na conscientização dos usuários, é outra vertente para um trabalho futuro. Isso pode ajudar a melhorar a capacidade dos usuários de identificar e evitar essa ameaça. Outro possível trabalho seria a criação de um programa de educação contínua, com foco em públicos mais vulneráveis, como os que possuem menos familiaridade com a tecnologia, especialmente as faixas etárias de 30 a 60 anos.

Para aprofundar ainda mais o tema, seria relevante realizar um estudo para observar como a percepção dos usuários sobre *phishing* evolui após a exposição contínua a treinamentos e simulações. Dessa forma, seria possível medir a efetividade de diferentes abordagens educacionais ao longo do tempo e desenvolver práticas mais direcionadas e eficazes.

Com base nas descobertas e sugestões apresentadas, espera-se que este trabalho contribua para o avanço nas estratégias de combate ao *phishing*, proporcionando maior proteção aos usuários e ajudando a criar uma cultura de sólida de segurança digital.

REFERÊNCIAS

ABNT. **NBR ISO/IEC 17799:2000 - Tecnologia da Informação - Código de Prática para a Gestão da Segurança da Informação**. Rio de Janeiro, 2005.

ADVISOR, C. **Microsoft, Google e Apple são as marcas mais usadas em phishing**. 2023. Disponível em: https://www.cisoadvisor.com.br/microsoft-google-e-apple-sao-as-marcas-mais-usadas-em-phishing/. Acesso em: 15 set 2024.

ALEROUD, A.; ZHOU, L. Phishing environments, techniques, and countermeasures: A survey. **Computers & Security**, v. 68, p. 160–196, 2017. ISSN 0167-4048.

APWG. **Phishing Activity Trends Report**. 2024. Disponível em: https://apwg.org/trendsreports/. Acesso em: 15 set. 2024.

APWG. **Phishing Activity Trends Report - Q2 2024**. 2024. Disponível em: https://apwg.org/trendsreports/. Acesso em: 27 set. 2024.

CASTRO, R. d. C.; PIMENTEL, S. V. L. Segurança em cloud computing: Governança e gerenciamento de riscos de segurança.l. p. 18, 2010.

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**, v. 106, p. 1–20, 2018. ISSN 0957-4174.

CRESPO, M. X. da S. **Crimes digitais**. São Paulo, SP: Editora Saraiva, 2011. 25 p. ISBN 9788502136663.

DAWEL, G. **A segurança da informação nas empresas**: Ampliando horizontes além da tecnologia. Rio de Janeiro: Editora Ciência Moderna Ltda, 2005.

DIO. **Engenharia Social**: como criminosos usam a psicologia para manipular suas vítimas. 2024. Disponível em: https://www.dio.me/articles/engenharia-social-como-criminosos-usam-a-psicologia-para-manipular-suas-vitimas. Acesso em: 14 ago. 2024.

FERNANDES, D. Q. V. M. **Engenharia Social**: usuários na linha de frente dos ataques. 2023. Disponível em: https://www.linkedin.com/pulse/engenharia-social-usu%C3%A1rios-na-linha-de-frente-dos-ataques-dqvmf/. Acesso em: 14 ago. 2024.

FERREIRA, F.; ARAUJO, M. **Política de segurança da informação**: Guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

FONSECA, M. Engenharia social: conscientizando o elo mais fraco da segurança da informação. 2017. **Trabalho de conclusão de curso (Pós-Graduação em Especialização em Inteligência em Segurança Pública) - Universidade do Sul de Santa Catarina, Brasília**, 2017.

HADNAGY, C.; MAXWELL, E. **Social Engineering Capture the Flag Results 2012**. 2012. Defcon USA.

HEIKKINEN, S. **Social engineering in the world of emerging communication technologies**. 2006. Proceedings of Wireless World Research Forum, 1.10.

HINTZBERGEN, J.; SMULDERS, A.; HINTZBERGEN, K.; BAARS, H. **Fundamentos de Segurança da Informação**: com base na iso 27001 e na iso 27002. Rio de Janeiro: Brasport, 2018.

HONG, J. The state of phishing attacks. **Communications of the ACM**, ACM, v. 55, n. 1, p. 74–81, 2012.

IBM. **O que é computação em nuvem?** 2024. Disponível em: https://www.ibm.com/br-pt/topics/cloud-computing. Acesso em: 27 set. 2024.

IBSEC. **Ataques de phishing**: o que são e como funcionam? 2024. Disponível em: https://ibsec.com.br/ataques-de-phishing-o-que-sao-e-como-funcionam/. Acesso em: 3 jun. 2024.

ISH. **Deepfake Phishing**: O que é, como funciona e como se proteger. 2023. Disponível em: https://ish.com.br/blog/deepfake-phishing-o-que-e-como-funciona-como-se-proteger/. Acesso em: 30 set. 2024.

JAKOBSSON, M.; MYERS, S. **Phishing and Countermeasures**: Understanding the increasing problem of electronic identity theft. Hoboken, NJ, EUA: Wiley, 2006.

KASPERSKY. **O que é engenharia social? Definição e exemplos**. 2018. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 15 ago. 2024.

KASPERSKY. **Brasil é o quinto país mais atacado por phishing no mundo no segundo trimestre de 2022**. 2022. Disponível em: https://www.kaspersky.com.br/blog/brasil-ataques-phishing-2022/20943/. Acesso em: 15 jul. 2024.

KASPERSKY. **Nova epidemia de phishing cresce mais de 5 vezes no Brasil com retomada das atividades econômicas e apoio da IA**. [S.l.]: Kaspersky, 2024. Disponível em: https://www.kaspersky.com.br. Acesso em: 14 ago. 2024.

LYRA, M. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

MANAGEENGINE. **Conheça seu inimigo**: um mergulho profundo na mente do hacker. 2022. Disponível em: https://blogs.manageengine.com/portugues/2022/05/20/conheca-seu-inimigo-um-mergulho-profundo-na-mente-do-hacker.html. Acesso em: 5 abr. 2024.

MANN, I. W. **Hacking the Human**. Aldershot (GB): Gower, 2008.

MICRO, T. **What is Social Media Phishing?** 2023. Disponível em: https://www.trendmicro.com/pt_br/whatis/phishing/socialmediaphishing.html. Acesso em: 30 set. 2024.

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

NBR. **NBR ISO/IEC 17799: Código de Prática para a Gestão da Segurança da Informação**. [S.l.], 2005. Disponível em: https://tororodeideias.wordpress.com/wp-content/uploads/2012/03/nbr-iso-iec-17799.pdf. Acesso em: 7 abr. 2024.

OLLMANN, G. **The Phishing Guide–Understanding & Preventing Phishing Attacks**. 2007. Disponível em: https://www.pt.scribd.com/document/219802442/The-Phishing-Guide-Understanding-Preventing-Phishing-Attacks-IBM-Internet-Security-Systems. Acesso em: 3 jun. 2024.

PEIXOTO, M. C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006. 39 p.

PHISHING.ORG. **History of phishing**. 2012. Disponível em: http://www.phishing.org/history-of-phishing. Acesso em: 24 abr. 2024.

PINHEIRO, P. P. **Segurança Digital - Proteção de Dados nas Empresas**. 1ª. ed. São Paulo, SP: Grupo GEN, 2020.

RODRIGUES, G. A. P. **Análise Abrangente de Vazamentos de Dados**: Riscos, conformidade e estratégias de prevenção. 2023. Disponível em: https://unb.br. Acesso em: 5 abr. 2024.

RUSSELL, R.; MULLEN, T.; LONG, J. **Stealing the Network**: The complete series collector's edition. Burlington, MA: Elsevier Inc, 2009.

SANTOS, L.; MOREIRA, J. **Desafios Pessoais nos Incidentes de Segurança e Vazamentos de Dados em Redes Wi-Fi Públicas Sob o Escopo da LGPD**. 2023. Disponível em: https://iftm.edu.br. Acesso em: 5 abr. 2024.

SÊMOLA, M. **Curso de Educação Continuada - Gestão de Segurança Informação**. [S.l.: s.n.], 2006. v. 1993.

STONEBURNER, G. **Underlying Technical Models for Information Technology Security**. [S.l.]: National Institute of Standards & Technology, 2001. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-33.pdf. Acesso em: 14 ago. 2024.

WIKIPEDIA. **B. F. Skinner**. 2024. Disponível em: https://pt.wikipedia.org/wiki/B._F._Skinner. Acesso em: 6 jun. 2024.

APÊNDICE A – QUESTIONÁRIO: COMPREENDENDO A PSICOLOGIA DO *PHISHING*

Caro(a) participante,

Este questionário faz parte de uma pesquisa para o Trabalho de Conclusão de Curso (TCC) intitulado "Compreendendo a Psicologia do *Phishing*: uma abordagem prática centrada no usuário", conduzido por Larisse Cruz Lucas, 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 os aspectos psicológicos envolvidos em ataques de *phishing*, compreender o comportamento dos usuários diante dessas ameaças e desenvolver 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 phishing.

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

++

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

O participante desta pesquisa acessará um questionário contendo questões demográficas, questões técnicas de múltipla escolha e questões abertas. O questionário visa caracterizar a familiaridade e extensão dos conhecimentos de cibersegurança dos alunos de cursos superiores em ciência da computação e tecnologia da informação, a amostra está de interesse pela proximidade com o tema.

O participante da pesquisa terá um questionário contendo questões sobre dados demográficos, conhecimento e experiência com *phishing*, comportamento e atitude, percepção e psicologia, educação e conscientização, opiniões adicionais de um projeto de pesquisa intitulado “Compreendendo a Psicologia do *Phishing*: uma abordagem prática centrada no usuário”, conduzido por Larisse Cruz Lucas sob a orientação do Prof. Dr. João Henrique Gonçalves Medeiros Corrêa no Campus de Itapajé. O objetivo é analisar os aspectos psicológicos envolvidos em ataques de *phishing* para 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 *phishing*. 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 larissecruz@alu.ufc.br. Ao assinar este termo, você concorda em participar do estudo.

Seção 0: Concordo em participar da pesquisa

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

Seção 1: Dados Demográficos

1.1 Idade:

- 18-24 anos
- 25-34 anos
- 35-44 anos
- 45-54 anos
- 55 anos ou mais

1.2 Gênero:

- feminina,
- masculina,
- transgênero
- Prefiro não responder
- Outros

1.3 Curso:

- Análise e Desenvolvimento de Sistemas - ADS
- Ciências de Dados - CD
- Segurança da Informação - SI

1.4 Semestre do curso:

- 2 semestre
- 3 semestre
- 4 semestre
- 5 semestre
- 6 semestre

Seção 2: Conhecimento e experiência com *Phishing*

2.1 Você sabe que é um ataque de *phishing*?

- Sim
- Não

2.2 Você já foi vítima de um ataque de *phishing*?

- Sim
- Não
- Não tenho certeza

2.3 Você conhece alguém que foi vítima de um ataque de *phishing*?

- Sim
- Não

2.4 Qual é o seu nível de conhecimento sobre *phishing*?

- Nenhum
- Básico
- Intermediário
- Avançado

Seção 3: Comportamento e atitude

3.1 Com que frequência você VERIFICA a autenticidade dos e-*mails* recebidos?

- Sempre
- Frequentemente
- Ocasionalmente
- Raramente
- Nunca

3.2 Com que frequência você DESCONFIA de *e-mails* solicitando informações pessoais ou financeiras?

- Sempre
- Frequentemente
- Ocasionalmente
- Raramente
- Nunca

3.3 Você já realizou cursos ou treinamentos específicos sobre *phishing*?

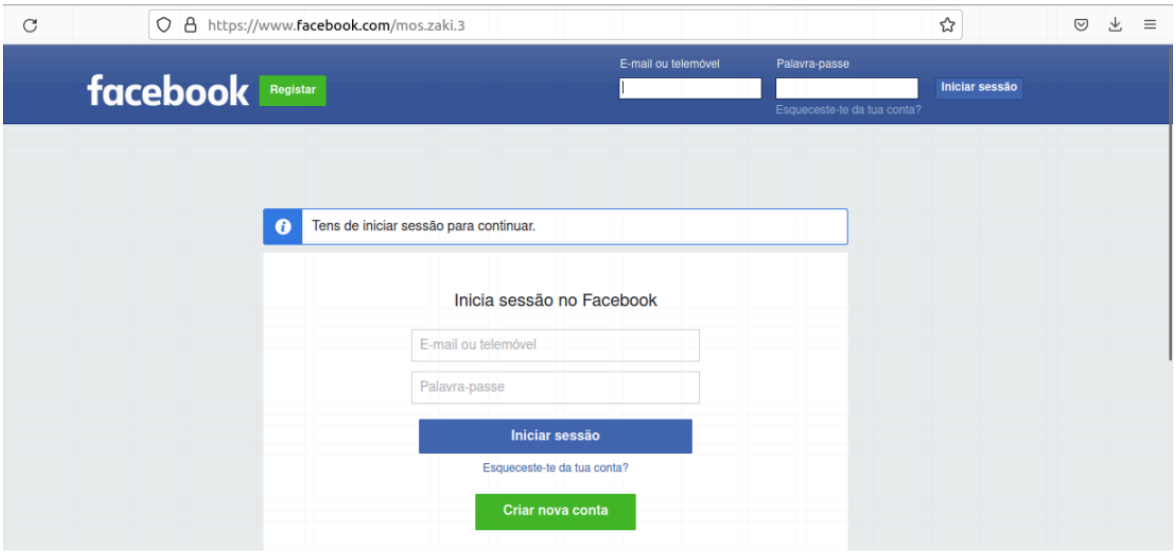
- Sim
- Não

Seção 4: Psicologia e Percepção

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

- Sim
- Não

4.2 O Facebook é uma das redes sociais mais conhecidas e acessadas do mundo. Observando atentamente e considerando esta imagem e os recursos visuais a disposição, existe algum indício de que este site seja falso ou que apresente um risco na transmissão de dados?



- Sim
- Não

4.3 Avaliando o e-mail recebido abaixo, tem algum indício de que seja um possível ataque de phishing?

- Sim
- Não

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

- Ignora

- Apaga
- Clica no link para conferir
- Bloqueia o remetente
- Relata o e-mail
- Verifica com a fonte
- Baixa o anexo
- Outros: _____

4.5 O que você acha que torna um *e-mail* de *phishing* convincente?

- Linguagem persuasiva
- Uso de logotipos oficiais
- Sensação de urgência
- Oferta de recompensas ou prêmios
- Outro: _____

4.6 Você se sente confiante em sua capacidade de evitar ser enganado por *phishing*?

- Muito confiante
- Confiante
- Neutro
- Pouco confiante
- Nada confiante

4.7 Em sua opinião, qual é o fator mais importante que contribui para a vulnerabilidade ao p*hishing*?

- Falta de conhecimento
- Falta de atenção
- Confiança excessiva
- Pressão social
- Outro: _____

Seção 5: Educação e Conscientização

5.1 Você acha que a educação sobre *phishing* é uma parte importante da formação em segurança da informação?

- Sim
- Não

5.2 Quais métodos de educação sobre *phishing* você considera mais eficazes?

- Palestras e *workshops*
- Cursos online
- Simulações de *phishing*

- Materiais de leitura
- Outro: _____

5.3 Você acredita que as simulações de phishing ajudam a melhorar a conscientização?

- Sim
- Não

5.4 Você tem alguma sugestão ou comentário sobre como melhorar a prevenção contra phishing?

Instruções Finais

Obrigado por participar deste questionário. Suas respostas serão utilizadas para compreender melhor os aspectos psicológicos do *phishing* e desenvolver estratégias eficazes de prevenção e conscientização.