INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PEDRO II
TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

DIEGO PEREIRA GONÇALVES

PHISHING NO INSTAGRAM, VULNERABILIDADES E PRÁTICAS DE SEGURANÇA DOS USUÁRIOS: UM ESTUDO DE CASO

PEDRO II, PIAUÍ
2025

DIEGO PEREIRA GONÇALVES

PHISHING NO INSTAGRAM, VULNERABILIDADES E PRÁTICAS DE SEGURANÇA DOS USUÁRIOS: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Pedro II.

Orientador: Profº. Esp. Danniel Rocha do Nascimento.
Coorientador: Profº. Mᵉ. Marcos Soares de Oliveira.

PEDRO II, PIAUÍ
2025

PHISHING NO INSTAGRAM, VULNERABILIDADES E PRÁTICAS DE SEGURANÇA DOS USUÁRIOS: UM ESTUDO DE CASO

Diego Pereira Gonçalves[1]
Profº. Esp. Danniel Rocha do Nascimento[2]
Profº. Mᵉ. Marcos Soares de Oliveira[3]

RESUMO

O aumento do uso de redes sociais, como o Instagram, trouxe novas vulnerabilidades, tornando os usuários alvos frequentes de ataques de engenharia social e phishing. Essas técnicas exploram falhas humanas e a falta de conhecimento em segurança digital, resultando no roubo de informações e invasões de contas. Um dos ataques mais comuns de phishing na plataforma é a falsificação, em que criminosos criam perfis e mensagens falsas para coletar dados confidenciais. Com base no referencial teórico estudado e na análise de dados coletados de 108 participantes por meio de um questionário estruturado, este estudo analisou o nível de conhecimento dos usuários sobre phishing e suas práticas de segurança digital, além de investigar a influência da formação em Tecnologia da Informação na adoção de medidas preventivas. Os resultados indicam que, embora a maioria dos respondentes conheça ou já tenha ouvido falar do termo phishing, poucos possuem conhecimento intermediário ou avançado sobre o tema, evidenciando uma lacuna na compreensão desse ataque. O estudo também demonstrou que, embora usuários com formação em TI tenham conhecimento sobre medidas básicas de segurança digital, essa proteção não é absoluta, pois ainda há comportamentos de risco,como a baixa adesão à autenticação em dois fatores e a falta de verificação recorrente de URLs. Esta pesquisa contribui para os estudos sobre segurança digital no Instagram, ao identificar vulnerabilidades dos usuários e sugerir medidas básicas de proteção,que costumam ser negligenciadas, como a autenticação em dois fatores e verificação de URLs, enfatizando a importância de campanhas educativas para reduzir os riscos.
Palavras-chave: phishing; engenharia social; cibersegurança; instagram; segurança da informação.

ABSTRACT

The increasing use of social networks, such as Instagram, has introduced new vulnerabilities, making users frequent targets of social engineering and phishing attacks. These techniques exploit human flaws and a lack of digital security awareness, leading to information theft and account breaches. One of the most common phishing attacks on the platform is impersonation, where cybercriminals create fake profiles and messages to collect confidential data. Based on the theoretical framework studied and data collected from 108 participants through a structured questionnaire, this study analyzed users' knowledge of phishing and their digital security practices, as well as the influence of Information Technology education on the adoption of preventive measures. The results indicate that while most respondents are familiar with the term phishing, few have an intermediate or advanced understanding of the topic, revealing a gap in the comprehension of this type of attack.The study also demonstrated that, although users with IT education have knowledge of basic digital security measures, this protection is not absolute, as risky behaviors persist, such as low adherence to two-factor authentication and the lack of regular URL verification.

[1] Graduação em Análise e Desenvolvimento de Sistemas. IFPI. E-mail: caped.20211p2ads0320@aluno.ifpi.edu.br
[2] Especialização em Pós-graduação lato sensu. ESAB. E-mail: danniel.rocha@ifpi.edu.br
[3] Mestrado em Computação Aplicada. USP- FFCLRP. E-mail: marcos.soares@ifpi.edu.br

This research contributes to studies on digital security on Instagram by identifying user vulnerabilities and suggesting basic protection measures that are often overlooked, such as enabling two-factor authentication and verifying URLs. Furthermore, it emphasizes the importance of educational campaigns to mitigate risks.
Keywords: phishing; social engineering; cybersecurity; Instagram; information security.

Data de aprovação: 25/03/2025

1 INTRODUÇÃO

As redes sociais têm se tornado um dos principais meios de comunicação e interação no mundo contemporâneo. Entre elas, o Instagram, lançado em 2010, se tornou uma das redes sociais mais usadas do mundo, com mais de um bilhão de contas e 500 milhões de usuários ativos diariamente (Bodnar, 2022) . Segundo o relatório Data Report 2024 Brasil, que mediu o uso de plataformas digitais por usuários, de 16 a 64 anos, que usam cada plataforma mensalmente, o Instagram é a segunda rede social mais usada no Brasil e é considerada a rede social preferida de 35,9% dos usuários (We are Social; Meltwater, 2024). Essa popularidade, no entanto, também torna a plataforma um alvo atrativo para cibercriminosos que utilizam técnicas sofisticadas, incluindo engenharia social, para realizar crimes cibernéticos, como o phishing.

O crime cibernético é amplamente reconhecido como um dos crimes graves da era moderna, sendo um problema significativo tanto para os países quanto para os indivíduos, especialmente devido ao rápido avanço da tecnologia e da informação (Al-duwairi et al., 2022). Dentre os diversos tipos de ataques, destaca-se o phishing, uma estratégia de engenharia social que se refere a um conjunto de ataques cibernéticos em que técnicas de disfarce e engano são empregadas por um invasor para obter acesso às informações confidenciais da vítima na Internet (Varshney et al., 2024). A engenharia social refere-se às táticas e estratégias empregadas por invasores para manipular indivíduos, induzindo-os a revelar informações sigilosas ou a executar ações que normalmente não fariam (Grbic; Dujlovic, 2023).

O Instagram tem se destacado como uma das plataformas preferidas por golpistas para realizar ataques de phishing, que anteriormente eram enviados por e-mail, mas agora abrangem diversos meios de comunicações eletrônicas, como SMS, chamadas telefônicas e redes sociais (Avast, 2022). Os aplicativos de mídia social facilitam o envio rápido e prático de dados e informações, o que torna o cuidado com a segurança desses conteúdos transmitidos uma questão de grande importância (Surjandy et al., 2023). A segurança da informação, segundo Fontes (2017) , envolve um conjunto de medidas e políticas que têm como objetivo proteger a integridade, a confidencialidade e a disponibilidade das informações. No ambiente das mídias sociais, como o Instagram, onde as interações são constantes e abertas, falhas na adoção de práticas robustas de segurança podem expor os usuários a riscos severos, como golpes de phishing.

De acordo com o relatório do Group (2024), publicado no primeiro trimestre de 2024, as

redes sociais foram o setor mais atacado e representaram 37,4% de todos os ataques de phishing. Esses números reforçam a necessidade de investigar como os usuários do Instagram percebem, lidam e se protegem contra essas ameaças. Com interações informais e rápidas, os usuários tornam-se alvos mais suscetíveis a golpes digitais, tornando-se alvos simples para fraudadores. Entre os ataques mais comuns no Instagram, destacam-se a criação de perfis falsos, o envio de mensagens enganosas, a disseminação de links fraudulentos e o uso da confiança como estratégia de manipulação (Almudahi et al., 2022).

Diante desse cenário, este estudo busca analisar o nível de conhecimento dos usuários sobre phishing, suas práticas de segurança digital na plataforma e como essas práticas podem influenciar sua vulnerabilidade. Além disso, a pesquisa investiga alguns aspectos, tais como formação acadêmica, intensidade do uso da plataforma e conhecimento prévio, impactam a adoção de medidas preventivas, como a autenticação em dois fatores e a verificação de URLs. Espera-se que os resultados contribuam para o desenvolvimento de medidas educativas capazes de reduzir os riscos associados a essas ameaças.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

O objetivo deste estudo é avaliar o nível de conhecimento dos usuários do Instagram sobre phishing na plataforma, bem como suas práticas de segurança digital. O estudo também buscará identificar como o conhecimento em informática, seja com curso superior ou técnico, influencia a capacidade dos usuários de identificar e tomar mais medidas de segurança na plataforma. A partir dessa análise, serão extraídas implicações para a segurança digital dos usuários da rede social. Através de um questionário, serão analisados o conhecimento dos usuários e suas práticas de segurança, com foco em identificar possíveis vulnerabilidades na plataforma.

1.1.2 Objetivos Específicos

1. Identificar os principais tipos de ataques de phishing no Instagram e as práticas mais comuns utilizadas pelos golpistas.
2. Avaliar o nível de conhecimento dos usuários sobre phishing e segurança no Instagram por meio da aplicação de um formulário.
3. Analisar as implicações para a segurança dos usuários.
4. Analisar se uma formação técnica ou superior em TI tem influência direta nas praticas de

segurança digital.

1.1.3 Justificativa

Os dados apresentados pela Group (2024), que mostram que as redes sociais são o principal alvo de ataques de phishing , sublinham a urgência de investigar esse fenômeno em plataformas como o Instagram, onde o mesmo atualmente é a 2ª plataforma de rede social mais usada do Brasil, perdendo apenas para o YouTube (We are Social; Meltwater, 2024). Este estudo se justifica pelo alto número de casos de fraude, estelionato e outros crimes que têm sido facilitados pela utilização das mídias digitais, o que aponta para a necessidade de ampliar o conhecimento e a conscientização sobre segurança digital e desenvolver recomendações práticas, baseadas em dados, para usuários do Instagram. Espera-se que os resultados obtidos possam contribuir para o aprimoramento das estratégias de proteção digital e servirem como base para futuras iniciativas de educação e combate aos crimes cibernéticos.

Este projeto está organizado da seguinte forma, A Seção 2 apresenta os conceitos fundamentais relacionados a segurança da informação, engenharia social, phishing e às ameaças nas redes sociais, com ênfase na plataforma Instagram. A Seção 3 descreve a metodologia utilizada para a condução do estudo de caso, incluindo o detalhamento do questionário que será aplicado. A Seção 4 discute os resultados obtidos, analisando as respostas e cruzando dados. Por fim, a Seção 5 apresenta as conclusões obtidas a partir da análise.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão apresentados os trabalhos relacionados e os principais termos e tecnologias empregados para alcançar os objetivos propostos neste trabalho.

2.1 TRABALHOS RELACIONADOS

O estudo de Frauenstein e Flowerday (2020), sobre a suscetibilidade ao phishing em redes sociais fornece uma base teórica relevante, destacando como características de personalidade e modos de processamento de informação influenciam a vulnerabilidade dos usuários a ataques de phishing. O artigo enfatiza que os phishers utilizam técnicas de engenharia social para manipular usuários, explorando suas vulnerabilidades comportamentais. Esse estudo evidencia a relação entre aspectos comportamentais e a suscetibilidade ao phishing, especialmente em plataformas como o Instagram, em que os usuários podem confiar excessivamente nas interações sociais.

Kaya e Sanders (2021), ao investigarem o vício em redes sociais e as preocupações

com segurança, destacam que o comportamento dos usuários em plataformas como Facebook e Instagram pode aumentar sua vulnerabilidade a ataques, incluindo phishing. O desconhecimento sobre configurações de privacidade e o compartilhamento excessivo de dados pessoais são fatores críticos que facilitam atividadess maliciosas. O estudo concluiu que há uma lacuna significativa entre o conhecimento sobre privacidade digital e o comportamento dos usuários, mesmo conscientes dos riscos, muitos não ajustam suas configurações de segurança. Esses aspectos são particularmente relevantes para o Instagram, por sua alta adoção entre o público brasileiro, e fornecem uma base importante para a análise da conscientização dos usuários, objetivo deste estudo.

O artigo de Nasution et al. (2024) explora estratégias de defesa em profundidade contra ataques de phishing no Instagram, destacando como técnicas de engenharia social são usadas para roubar informações pessoais. O estudo detalha métodos de ataque, como phishing por SMS e sites falsos, e apresenta uma abordagem integrada de segurança que combina fatores humanos, organizacionais e tecnológicos. Esse trabalho é relevante para esta pesquisa, pois oferece uma visão abrangente das técnicas de phishing no Instagram, contribuindo diretamente para o objetivo de avaliar a conscientização dos usuários e propor estratégias educativas eficazes para reduzir os riscos.

Embora diversos estudos tenham explorado ataques de phishing, nosso trabalho se diferencia ao focar especificamente no Instagram e na influência da formação acadêmica na adoção de medidas preventivas. Os estudos anteriores geralmente analisam aspectos psicológicos ou abordam phishing em um contexto mais amplo. Abaixo, apresentamos uma comparação entre as principais pesquisas e este estudo.

Tabela 1 – Comparação entre trabalhos relacionados e este estudo

Autor	Diferença para estre Trabalho
Frauenstein e Flowerday (2020)	Nosso estudo foca exclusivamente no Instagram.
Kaya e Sanders (2021)	Investigamos usuários brasileiros do centro norte piauiense,identificando também uma lacuna significativa entre o conhecimento sobre privacidade digital e o comportamento dos usuários.
Nasution et al. (2024)	Incluímos análise de algumas dessas defesas por formação em TI.

Fonte: Elaborado pelo autor.

2.2 INSTAGRAM

Plataformas de mídia social são sistemas digitais online que permitem que os usuários

criem, compartilhem e interajam com conteúdo (Syamsuar; Darren, 2023). A plataforma de mídia social é utilizada para diversos fins,tanto usuários quanto clientes recorrem às redes sociais para buscar informações e formar opiniões sobre uma gama de temas, como produtos, educação, saúde, política, transporte, seguros, bancos e serviços públicos, entre outros (Rahman; Reza, 2022).

Segundo Garcia (2017), "o Instagram é um aplicativo de rede social que permite o compartilhamento de fotos e vídeos com os contatos da rede social de cada usuário". Essa rede social se destaca como uma plataforma visual ideal, permitindo não apenas a conexão social entre as pessoas, mas também funcionando como um dos sistemas de mídia social mais eficazes para finalidades comerciais (Teotia et al., 2023), sua capacidade de disseminar informações rapidamente permite que elas atinjam milhões de usuários em questão de segundos, alcançando lugares antes inimagináveis (Sousa et al., 2021).

2.3 SEGURANÇA DA INFORMAÇÃO

A segurança da informação, conforme abordado por Schneier (2000), é essencial para proteger dados sensíveis contra ameaças como a engenharia social e o phishing. O padrão internacional, ISO/IEC 27001, define segurança da informação como um conjunto de práticas e processos que visam proteger a confidencialidade, integridade e disponibilidade das informações (Malatji, 2023).

Segundo Fontes (2017):

- Confidencialidade: refere-se à proteção das informações contra acesso não autorizado. Isso significa que apenas pessoas, sistemas ou processos devidamente autorizados podem acessar determinadas informações.
- A disponibilidade: diz respeito à garantia de que as informações e recursos estão acessíveis e utilizáveis quando necessário.
- A integridade: trata-se da garantia de que as informações são precisas e completas, e que não foram alteradas de forma não autorizada.

O nível de conscientização sobre segurança da informação pode ser medido por três dimensões, a saber, conhecimento, atitude e comportamento (Kruger; Kearney, 2006).

> "O conhecimento reflete o que os usuários sabem sobre ameaças e proteção à segurança da informação. Enquanto isso, a atitude descreve como os usuários se sentem sobre o tópico relacionado à ameaça e proteção à segurança. O comportamento descreve o que eles fazem para proteger suas informações da ameaça (Sari; Prasetio, 2017)."

Apesar dos avanços tecnológicos serem fundamentais para proteger sistemas e dados, o fator humano continua sendo o elemento decisivo para o sucesso ou falha das estratégias de segurança da informação, destacando sua relevância e complexidade (Kanagusku; Gaseta, 2023). As ameaças à segurança não se limitam às vulnerabilidades tecnológicas, elas também exploram fraquezas humanas, como é o caso da engenharia social e o phishing.

2.4 ENGENHARIA SOCIAL

Cibercriminosos tendem a atacar usuários, que representam um ponto de acesso vulnerável (Albladi; Weir, 2018). Mitnick e Simon (2002) descrevem a engenharia social como um conjunto de técnicas de manipulação que exploram a confiança humana para comprometer a segurança da informação. Ou seja esses ataques buscam a falha humana ao invés da falha tecnológica. Uma ação de engenharia social pode ocorrer em um ambiente pessoal, visando coletar informações pessoais, ou em um contexto profissional, com o objetivo de obter dados sobre uma organização (Brasil, 2023).

Os atacantes utilizam as redes sociais para reunir informações sobre suas vítimas, como suas qualificações profissionais, interesses pessoais, conexões sociais e a frequência em eventos específicos, criando ataques mais eficazes e personalizados (Tavares, 2017).Essas informações são posteriormente usadas para enganar as vítimas, induzindo-as a revelar dados sensíveis ou a executar ações perigosas. As estratégias de engenharia social estão se tornando cada vez mais comuns nas mídias sociais, explorando vulnerabilidades no comportamento humano para comprometer a segurança das empresas (Wilcox; Bhattacharya, 2016).

2.5 PHISHING

Phishing é uma forma de roubo de identidade eletrônica na qual uma combinação de engenharia social e técnicas de falsificação é empregada para enganar um usuário e fazê-lo revelar informações confidenciais de valor econômico (Aburrous et al., 2010). Ainda que a tecnologia seja fundamental, a literatura especializada em segurança da informação destaca que a vulnerabilidade humana é um dos principais alvos dos ataques de phishing, tornando insuficiente a adoção exclusiva de medidas técnicas de mitigação (Frauenstein; Flowerday, 2020). Os phishers geralmente empregam estratégias variadas para alcançar seus objetivos, mas, em situações comuns, eles se passam por entidades confiáveis, como empresas respeitadas, pessoas conhecidas ou até órgãos públicos, utilizando e-mails como iscas para direcionar os usuários a páginas fraudulentas (Moreno-Fernández et al., 2017).

Embora o phishing possa ocorrer em diversos contextos, nos meios digitais, as redes

sociais têm se mostrado um terreno particularmente fértil para esse tipo de ataque. De acordo com o relatório da Kaspersky (2023), o uso da IA para automatizar mensagens de phishing no Brasil permitiu uma escalada significativa nos golpes, especialmente focados no roubo de dados financeiros. As técnicas de phishing direcionadas se desenvolveram, resultando na criação de novos termos, como spear phishing, whaling, "smishing"(phishing via SMS), in-session phishing, spy phishing, "vishing"(phishing por chamadas de voz) e vários outros (Gonzales; Nance; Nazario, 2011). Conforme Chrysanthou,Pantis e Patsakis (2024), "as táticas dos criminosos cibernéticos seguiram os avanços tecnológicos, levando a uma escalada significativa na sofisticação das campanhas de phishing".

2.6 PHISHING NAS REDES SOCIAIS

Usuários de mídia social estão se tornando vítimas cibernéticas de muitas ações antiéticas e ilegais, resultando em danos mentais ou físicos graves (Al-Duwairi et al., 2022). Os ataques de phishing têm se tornado cada vez mais sofisticados, especialmente em plataformas de redes sociais, onde os usuários, muitas vezes, ficam vulneráveis devido ao aumento do uso de distratores em smartphones e aplicativos sociais (Alharbi et al., 2022). Educar os usuários sobre os riscos associados a phishing é fundamental para mitigar os impactos negativos dessa tecnologia nas plataformas sociais (Dolhansky et al., 2020). Sem essa educação, os usuários podem ser ainda mais facilmente enganados por conteúdos manipulados que parecem autênticos. Atualmente, diversos invasores utilizam sites de mídia social para lançar ataques de phishing, onde é bastante fácil para um intruso abusar da confiança e se passar por outra pessoa (Alharbi et al., 2022). Os atacantes utilizam estratégias como a criação de perfis falsos para imitar pessoas ou organizações confiáveis e enganar as vítimas. Esses perfis enviam mensagens diretas com links maliciosos que parecem legítimos, direcionando as vítimas a sites fraudulentos ou projetados para roubar informações pessoais (Almudahi et al., 2022). Os ataques de phishing em ambientes de redes sociais (SNEs) empregam várias táticas para enganar os usuários e extrair informações confidenciais. Algumas delas são apresentadas a seguir.

2.6.1 Spear Phishing

O spear phishing, diferentemente do phishing tradicional,é um ataque altamente direcionado e específico ao contexto, direcionado a grupos específicos de indivíduos ou organizações (Allodi et al., 2020). Os atacantes visam pessoas ou empresas específicas, utilizando informações que estão publicamente acessíveis, em sites e aplicativos, como o Instagram, em seguida, ajustam sua mensagem de acordo com as características, o cargo e o contato da vítima, a fim

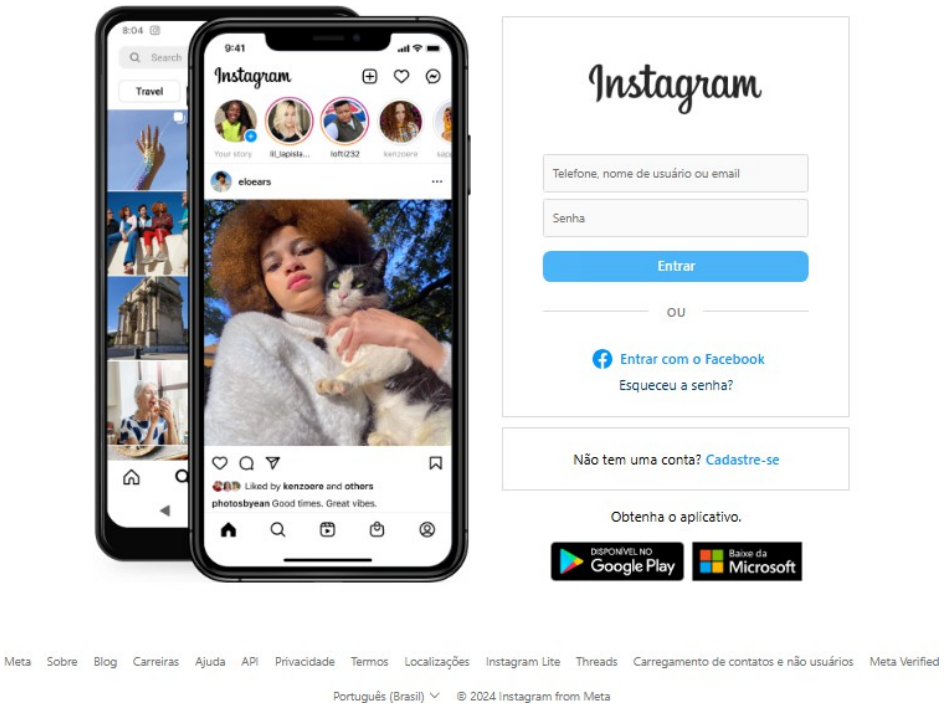
de potencializar o ataque (Nasution et al., 2024). Esse nível de personalização torna o ataque mais eficaz e difícil de detectar, já que a comunicação parecerá legítima. O spear phishing tem como objetivo acessar dados confidenciais, como nomes de usuário, senhas e outras informações pessoais, levando o consumidor, por exemplo, ao clicar em um link malicioso, a acessar um site fraudulento que pode infectar seu computador (Baig; Ahmed; Memon, 2021).

2.6.2 Falsificação

Os phishers geralmente empregam técnicas de falsificação, como criar e-mails ou mensagens falsas que parecem vir de fontes confiáveis. Isso pode incluir imitar a marca e a linguagem de empresas conhecidas para induzir os usuários a fornecerem suas credenciais (Ali et al., 2020). O phishing se torna ainda mais poderoso quando o golpista se faz passar por uma celebridade. Nesse caso, o perfil falso seria acompanhado por uma rede de amigos fictícios vinculados àquela conta falsa (Frauenstein; Flowerday, 2016). Essa estratégia busca convencer a vítima de que a conta é autêntica, já que um perfil com poucos amigos pode despertar suspeitas. Em sites de phishing, são comuns ataques online em andamento. Nesse tipo de ataque, os invasores criam páginas de sites copiando sites genuínos e enviam URLs suspeitas para as vítimas visadas, por meio de mensagens em redes sociais online (Basit et al., 2021).

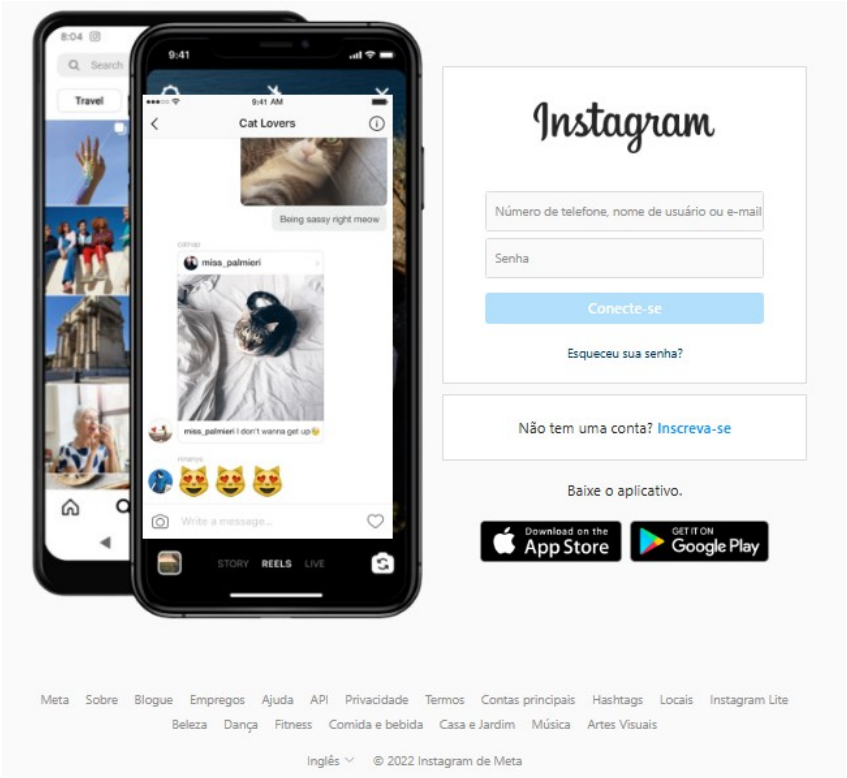
As imagens abaixo mostram duas interfaces de login do Instagram: a Figura 2, projetada para enganar os usuários e roubar suas credenciais. A Figura 1 é a verdadeira. Embora pareçam semelhantes, é importante prestar atenção aos detalhes, como o design e a URL, para evitar cair em fraudes. Na segunda imagem podemos ver o arroba da plataforma desatualizado (2022 Instagram de Meta), além da tela contendo um Iphone antigo com um design maior.

Figura 1 – Login Verdadeiro do Instagram



Fonte: extraido do site do Instagram: https://www.instagram.com/ (2024)

Figura 2 – Login Falso do Instagram



Fonte: extraido do site do Zphisher: https://github.com/htr-tech/zphisher/tree/master/(2024)

3 METODOLOGIA

Esta seção apresenta os materiais e métodos empregados para realização deste projeto de pesquisa. A pesquisa proposta será de natureza quantitativa, utilizando-se de um questionário estruturado para coleta de dados. O método quantitativo foi escolhido, pois permite a coleta de dados em larga escala e possibilita a identificação de padrões estatísticos no comportamento dos participantes (Apuke, 2017).

3.1 OBJETIVO DO ESTUDO

O objetivo desta pesquisa é analisar o nível de conhecimento sobre phishing e as práticas de segurança digital adotadas pelos usuários do Instagram. Além disso, investiga como a formação em Tecnologia da Informação (nível técnico ou superior) influencia na adoção de medidas preventivas contra ataques.

3.2 DEFINIÇÃO DA AMOSTRA

A amostragem é o processo de selecionar uma parte de uma população ou universo para realizar uma pesquisa (Etikan; Musa; Alkassim, 2015). Neste estudo foi utilizado uma amostra não probabilística por conveniência, na qual os participantes serão selecionados de acordo com a disponibilidade e acesso ao questionário. Essa abordagem foi escolhida por ser de fácil aplicação e acessível, permitindo a obtenção de um número significativo de respostas dentro de um curto período para a pesquisa. Esse tipo de amostragem não busca representar a população de forma ampla, mas sim possibilitar uma coleta mais prática e eficiente.

De acordo com Arruda Filho e Farias (2015), a amostra por conveniência consiste em entrevistar pessoas que vão aparecendo de forma espontânea, sem a necessidade de selecionar um grupo específico para a pesquisa, ou seja, são indivíduos que o pesquisador tem maior facilidade de acesso.

3.3 COLETA DE DADOS

A coleta de dados foi realizada por meio de um questionário online, elaborado com perguntas de múltipla escolha e caixas de seleção, facilitando a participação dos usuários. A coleta de dados é o processo sistemático de obtenção de informações relevantes para um objetivo de pesquisa (Kabir, 2016), sendo o questionário uma ferramenta amplamente utilizada em estudos quantitativos. Antes da aplicação definitiva, o questionário foi testado com um grupo piloto de nove pessoas. Como sugerido por Hilton (2015), a realização de um teste piloto antes

da aplicação de um questionário é fundamental para avaliar a clareza, coerência e confiabilidade das perguntas.

Nesse sentido, o questionário foi divulgado em diferentes plataformas digitais como o WhatsApp e o Instagram, aberto para o público em geral responder entre os dias 11 e 18 de dezembro de 2024.A pesquisa obteve 108 respostas. O questionário foi formulado em quatro blocos principais:

1. Perfil do respondente: inclui questões sobre idade, formação em TI e experiência com o Instagram.

2. Conhecimento e experiência com phishing: avaliação do nível de familiaridade dos usuários com o conceito de phishing e se já foram alvos de tentativas de ataque.

3. Situações reais de phishing no instagram: análise das mensagens suspeitas recebidas pelos participantes.

4. Práticas de segurança: identificação das ações que os usuários tomam para proteger suas contas e como lidam com mensagens suspeitas.

Algumas perguntas foram adaptadas de estudos anteriores, como o trabalho de Kaya e Sanders (2021), que analisou comportamentos de privacidade e segurança em redes sociais. Essas adaptações foram feitas para melhor atender ao escopo da pesquisa e focar no uso específico do Instagram, considerando situações práticas relacionadas a mensagens suspeitas e práticas de segurança digital.

3.4 ANÁLISE DE DADOS

Os dados obtidos foram analisados por meio de uma análise estatística descritiva,utilizando percentuais com o objetivo de quantificar os resultados e identificar padrões relevantes. A pesquisa quantitativa visa quantificar o problema ao gerar dados numéricos que podem ser transformados em estatísticas utilizáveis (Apuke, 2017).

Para isso,foi utilizado o Google Sheets para gerar gráficos estatísticos para facilitar a vizualização dos resultados. Além disso, foi realizado o cruzamento de variáveis para identificar possíveis padrões e relações estatísticas, como a análise se usuários com formação em Tecnologia da Informação demonstram maior conhecimento sobre phishing e se adotam mais medidas de segurança digital em comparação com aqueles sem essa formação

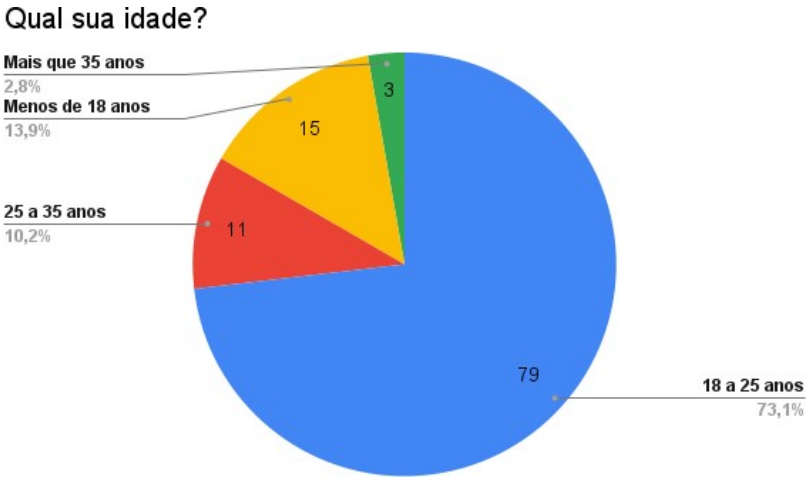
3.5 ÉTICA DA PESQUISA

A pesquisa seguiu as diretrizes éticas estabelecidas pela Resolução nº 466/2012 do Conselho Nacional de Saúde (2012), respeitando a dignidade e autonomia dos envolvidos, assegurando que a pesquisa foi planejada e executada de maneira a evitar danos e proteger os dados sensíveis. Nesse contexto, antes de responderem ao questionário, todos os participantes foram informados sobre o objetivo da pesquisa e tiveram a opção de consentir ou não com a participação. Todas as respostas foram tratadas de forma confidencial, garantindo assim a conformidade com os princípios éticos que regem a pesquisa.

4 RESULTADOS E DISCUSSÕES

Esta seção apresenta os dados coletados a partir das 108 respostas ao questionário estruturado, que utilizou a plataforma Google Forms e foi apresentado ao público usuário do Instagram por meio de aplicativos como o Whatsapp. O formulário foi organizado em torno de quatro categorias principais: Perfil dos Respondentes, Conhecimento sobre Phishing, Práticas de Segurança Digital e Percepção de Segurança no Instagram. Bem como a discussão sobre os achados em relação ao referencial teórico. Os resultados foram analisados por meio de estatísticas descritivas e são complementados por gráficos e tabelas para facilitar a interpretação. Além disso, são discutidos cruzamentos de variáveis relevantes, buscando compreender melhor os fatores que podem influenciar na vulnerabilidade dos usuários a ataques de phishing.

Figura 3 – Faixa Etária

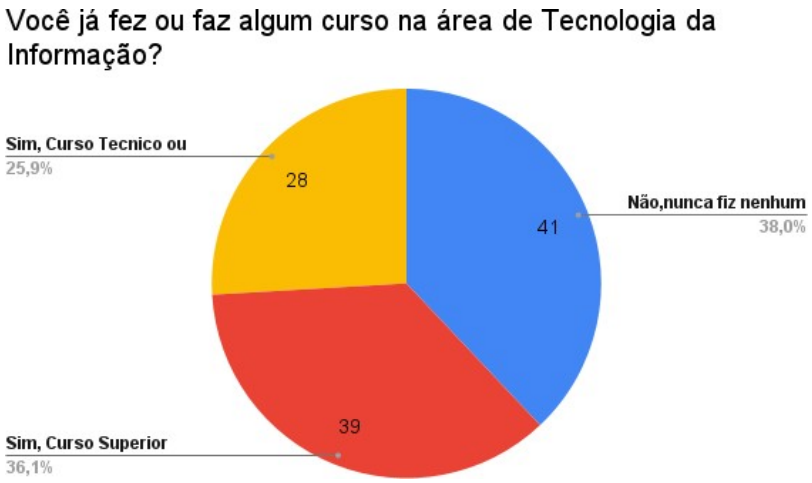


Fonte: Elaborado pelo autor.

A maioria dos participantes (73,1%) tem entre 18 e 25 anos, enquanto apenas 2,8% possuem mais de 35 anos, indicando um público predominantemente jovem. Em relação à formação acadêmica, 63,9% dos respondentes estão cursando ou já concluíram cursos relacionados à Tecnologia da Informação (TI), enquanto 36,1% não possuem formação na área. Além disso,

62% dos participantes acessam o Instagram várias vezes ao dia, 27,8% acessam algumas vezes por dia e 9,3% acessam raramente, evidenciando um uso intensivo da plataforma, o que pode impactar na exposição a tentativas de phishing.

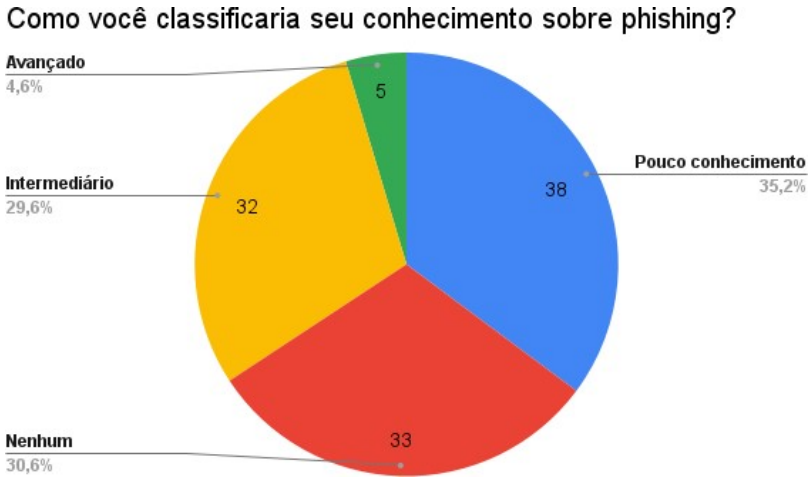
Figura 4 – Formação em TI



Fonte: Elaborado pelo autor.

Os resultados deste estudo revelam lacunas significativas no conhecimento e nas práticas de segurança digital dos usuários do Instagram, além de destacar vulnerabilidades que os tornam suscetíveis a ataques de phishing.

Figura 5 – Conhecimento sobre Phishing

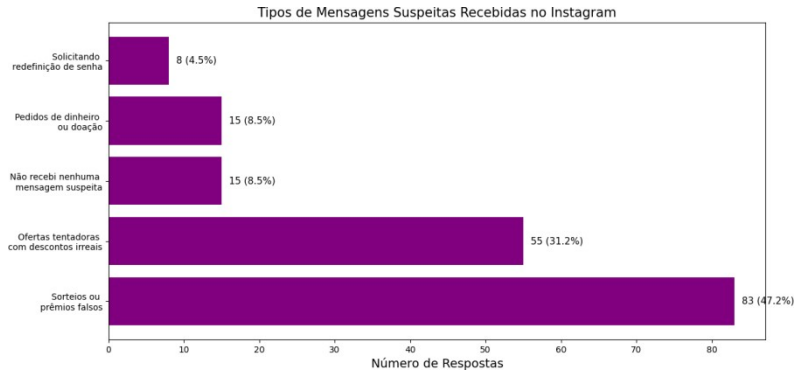


Fonte: Elaborado pelo autor.

Embora 63% dos respondentes afirmaram conhecer o termo "phishing", apenas 34,2% se consideram com conhecimento intermediário ou avançado sobre o tema. Isso indica que, apesar da familiaridade com o conceito, o entendimento aprofundado sobre ataques de phishing

ainda é limitado.

Figura 6 – Tipos de Mensagens suspeitas recebidas no Instagram

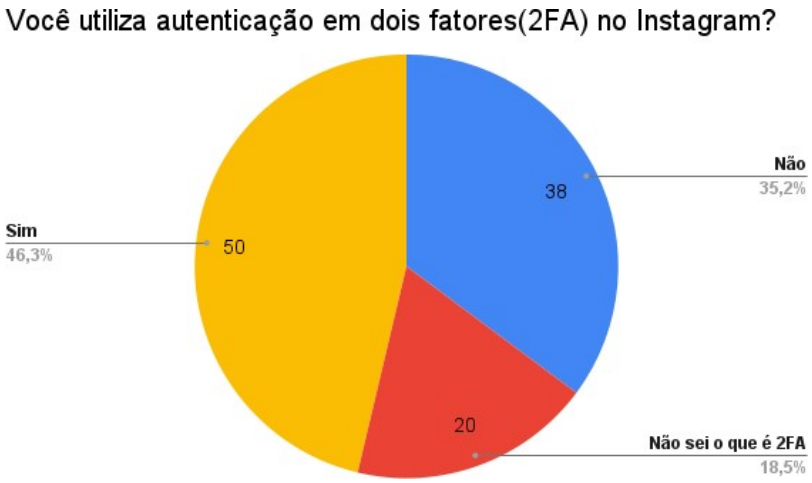


Fonte: Elaborado pelo autor.

A pesquisa revelou que 86,1% dos participantes já receberam mensagens suspeitas no Instagram, sendo os sorteios ou prêmios falsos os tipos mais comuns (76,9%). Esses dados refletem táticas de phishing baseadas em recompensas ou promessas atraentes, explorando o desejo humano de ganhos fáceis, um ponto destacado por AlMudahi et al. (2022) como uma das principais estratégias de cibercriminosos. Por outro lado, apesar de mensagens solicitando redefinição de senha ou doações em dinheiro serem menos frequentes no grupo de respondentes, ainda representam ameaças graves, pois podem resultar em roubo de credenciais ou fraudes financeiras, com a possibilidade adicional de recorrência ou do cometimento de mais de um crime com os mesmos dados capturados. Esse dado reforça a necessidade de maior conscientização sobre engenharia social e manipulação psicológica, elementos-chave explorados em ataques de phishing. Essa lacuna reflete a necessidade de intervenções educacionais para ampliar a compreensão sobre as táticas utilizadas por cibercriminosos, como manipulação psicológica e engenharia social, que exploram a confiança e o desejo de vantagens imediatas.

Apenas 46,3% dos respondentes utilizam autenticação em dois fatores (do inglês, Two-Factor Authentication - 2FA). E, enquanto 35,2% conhecem, mas não utilizam 2FA, 18,5% sequer sabem de sua existência. Essa baixa adesão preocupa, visto que o 2FA é uma proteção adicional para suas contas, diminuindo a probabilidade de sua conta ser invadida (Carneiro; Farina; Florian, 2024). Quando questionados sobre como lidam com mensagens suspeitas, 64,8% dos participantes afirmaram ignorá-las, enquanto 20,4% denunciariam ao Instagram, 12,0% pesquisaria sobre a mensagem e apenas 2,8% clicaria no link para verificar.

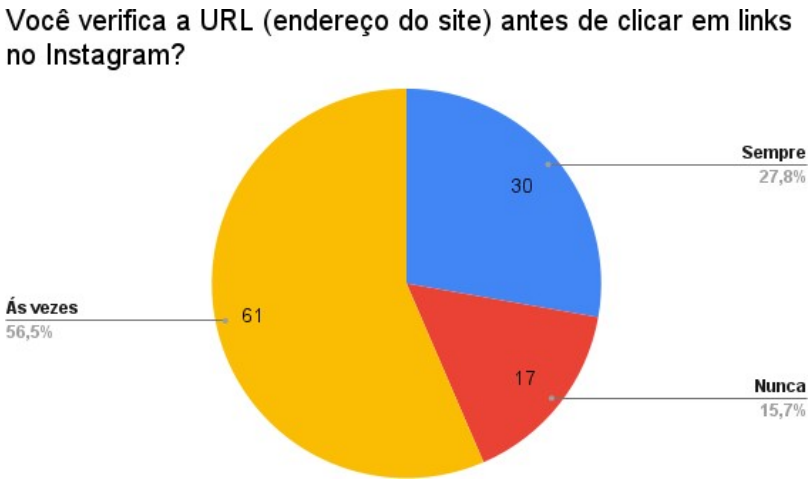
Figura 7 – Uso de 2FA



Fonte: Elaborado pelo autor.

A baixa adesão à autenticação em dois fatores é um ponto preocupante, considerando sua eficácia comprovada na prevenção de ataques cibernéticos. De acordo com Ellahi (2022), a autenticação em dois fatores apresenta uma camada extra de segurança ao exigir, além da senha, um segundo fator de verificação, que pode ser algo que o usuário sabe (como uma senha), algo que possui (como um aplicativo ou token de hardware) ou algo que é (como uma impressão digital). Essa abordagem torna mais difícil para os invasores acessar a conta, mesmo que tenham obtido a senha. O baixo uso dessa funcionalidade pelos participantes sugere que a falta de informação ou a percepção de dificuldade em ativá-la ainda são barreiras significativas.

Figura 8 – Verificação de URL



Fonte: Elaborado pelo autor.

Outro aspecto relevante é o comportamento dos usuários em relação a mensagens suspeitas, visto que apenas 27,8% verificam URLs regularmente antes de clicar. Esses resultados indicam a necessidade de maior conscientização sobre a verificação de links, uma vez que essa é uma das medidas mais simples e eficazes para evitar o comprometimento de contas. Como descrito por Alharbi (2022), uma URL maliciosa pode redirecionar o usuário para um site sob o controle do invasor, que frequentemente contém páginas de login falsas ou aplicativos maliciosos. O autor também destaca que quase 90% dos cliques em URLs maliciosas ocorrem nas primeiras 24 horas após a liberação, evidenciando a rapidez com que os invasores aproveitam essas vulnerabilidades.

Figura 9 – Compartilhamento de Informações

Fonte: Elaborado pelo autor.

Sobre compartilhar informações pessoais na plataforma, 35,2% revelaram compartilhar essas informações sempre ou frequentemente. Embora o percentual de compartilhamento frequente seja relativamente baixo, esses usuários podem estar mais suscetíveis a ataques de phishing direcionados, que exploram informações publicamente disponíveis no Instagram para personalizar mensagens fraudulentas, como discutido por Nasution (Nasution et al., 2024).

A maioria dos participantes (83,3%) se sente moderadamente segura ao usar o Instagram, enquanto 13% se sentem inseguros. Quando questionados sobre a proteção contra phishing oferecida pelo Instagram: 80,6% dos participantes acreditam que a plataforma poderia fazer mais para proteger os usuários contra ataques de phishing, enquanto 12% não sabem avaliar.

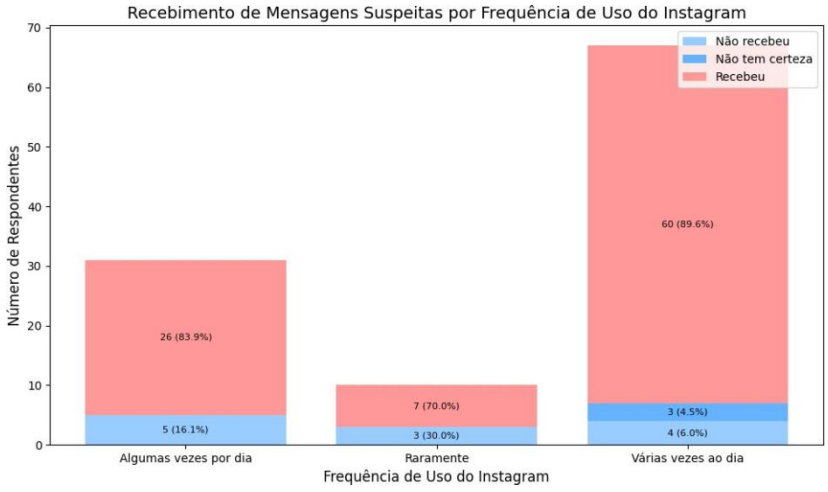
Figura 10 – Proteção do Instagram contra Phishing

Fonte: Elaborado pelo autor.

A insatisfação de grande parte dos usuários sugere tanto uma falta de conhecimento sobre as ferramentas de segurança disponíveis quanto uma falta de informação sobre as iniciativas da plataforma, ambas podendo ser interpretadas como falhas na comunicação educativa sobre segurança da plataforma. Conforme proposto por Chrysanthou, Pantis e Patsakis (2024), as mídias sociais, como o Instagram, deveriam investir em campanhas de conscientização mais eficazes e interativas, como anúncios públicos e vídeos educativos, utilizando exemplos reais de phishing. Tais iniciativas ajudariam a aumentar o conhecimento dos usuários sobre as ferramentas de segurança disponíveis e a reduzir sua vulnerabilidade a ataques.

4.1 CRUZAMENTO DE VARIÁVEIS

Figura 11 – Uso do Insta x mensagens suspeitas recebidas

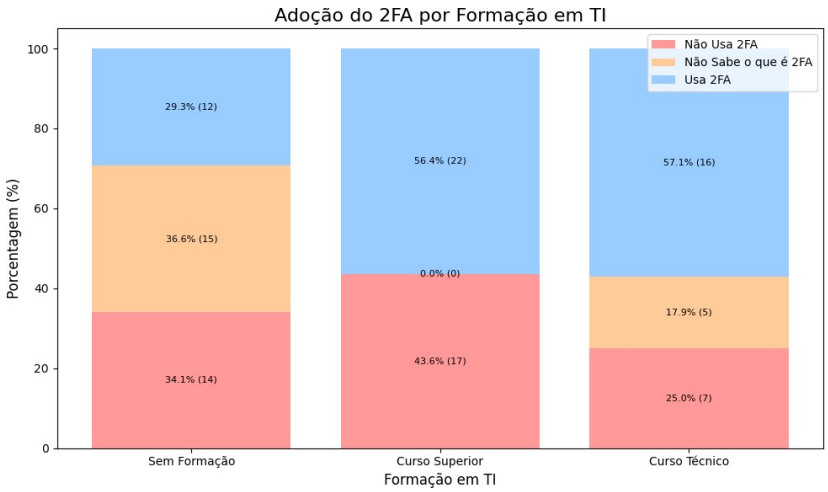


Fonte: Elaborado pelo autor.

Para aprofundar a análise e compreender melhor os fatores que influenciam a suscetibilidade ao phishing, foram realizados cruzamentos entre algumas variáveis. Inicialmente, há a análise da relação entre a frequência de uso do Instagram e o recebimento de mensagens suspeitas. Os resultados indicam que a frequência de uso da plataforma influencia diretamente

no volume de exposição a mensagens suspeitas. Entre os usuários que acessaram o Instagram várias vezes ao dia, 89,6% relataram ter recebido mensagens suspeitas. Esse percentual cai para 83,9% entre aqueles que utilizam algumas vezes por dia e para 70% entre aqueles que acessam raramente. Esses dados sugerem que a exposição prolongada ao Instagram aumenta significativamente as chances de contato com tentativas de phishing, reforçando a necessidade de conscientização e medidas preventivas para todos os usuários, especialmente os mais ativos na plataforma.

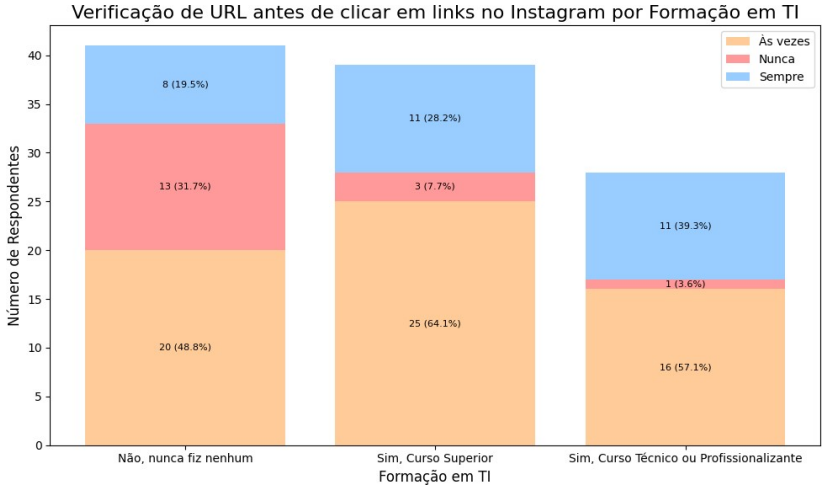
Figura 12 – Uso de 2FA por Formação em TI



Fonte: Elaborado pelo autor.

Usuários com formação em TI demonstraram maior adoção de práticas preventivas, como o uso de autenticação em dois fatores (2FA). Entre os participantes com curso superior ou técnico, mais de 56% utilizam o 2FA, enquanto esse percentual cai para 29,3% entre aqueles sem formação na área. Além disso, o desconhecimento sobre o 2FA é significativamente maior entre os não formados (36,6%), contrastando com 0% entre os formados em nível superior. Apesar desse resultado positivo, observa-se que o percentual de participantes com curso superior que não utilizam o 2FA também é elevado, atingindo 43,6%. Esse dado sugere que, embora o conhecimento sobre o 2FA esteja presente, pode haver falta de interesse ou subestimação da importância de adotar medidas de proteção, mesmo entre usuários tecnicamente capacitados. Dessa forma, os resultados indicam que a educação formal em TI tem um impacto positivo na conscientização sobre segurança digital, mas que o conhecimento por si só não garante a adoção de boas práticas.

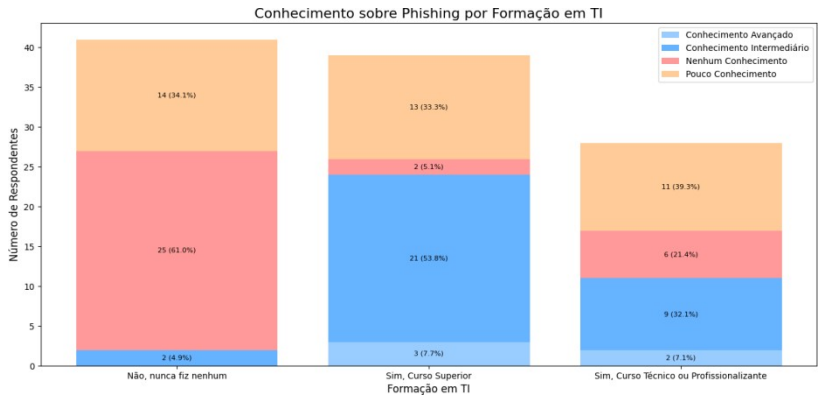
Figura 13 – Verificação de URL por Formação em TI



Fonte: Elaborado pelo autor.

Participantes com formação técnica ou superior demonstraram maior adesão a práticas de segurança, como o uso do 2FA e a verificação de URLs. Entre os respondentes sem formação em TI, 31,7% afirmaram nunca verificar links antes de clicar, o que indica uma maior vulnerabilidade a ataques de phishing. Em contraste, apenas 7,7% dos participantes com curso superior e 3,6% dos que possuem formação técnica relataram o mesmo comportamento de risco. Além disso, 39,3% dos respondentes com formação técnica e 28,2% dos com nível superior afirmaram sempre verificar URLs antes de clicar, evidenciando uma conscientização mais sólida sobre segurança digital. Esses resultados reforçam o impacto positivo da educação formal em TI, além de destacar a importância de campanhas de conscientização voltadas para todos os públicos, com especial atenção aos menos especializados.

Figura 14 – Conhecimento sobre Phishing por Formação em TI



Fonte: Elaborado pelo autor.

A formação acadêmica também influenciou o nível de conhecimento sobre phishing. Entre os participantes sem formação formal em TI, 95,1% relataram ter pouco ou nenhum

conhecimento sobre o tema. Já entre aqueles com curso superior, o percentual de conhecimento intermediário ou avançado foi significativamente maior, atingindo 61,5%. Esse dado reforça a necessidade de iniciativas educativas voltadas para usuários sem conhecimento técnico, uma vez que esse grupo se mostrou mais vulnerável a ataques.

Os resultados deste estudo destacam a necessidade de intervenções educativas e ações práticas para reduzir a vulnerabilidade dos usuários ao phishing no Instagram. As plataformas de mídias sociais precisam apoiar iniciativas educacionais que visem aumentar a conscientização e implementar ações de segurança para proteger dados pessoais (Jyothi; Badiger; Shivakumar, 2023). Além disso, a simplificação e o conhecimento de ferramentas como a autenticação em dois fatores podem aumentar o seu uso.

Em suma, os achados deste estudo evidenciam uma carência significativa quanto ao conhecimento teórico e às práticas de segurança digital entre os usuários do Instagram. O impacto da formação em TI sobre o comportamento preventivo e o conhecimento sobre phishing ressalta a importância da educação como ferramenta para reduzir vulnerabilidades. Mas mesmo entre os grupos com formação acadêmica na área de TI, que têm maior propensão a comportamentos que aumentam a segurança, foi possível notar que a confiança nas plataformas e, possivelmente, as dificuldades de uso das tecnologias de segurança impactam negativamente em sua adoção. Campanhas de conscientização direcionadas, associadas à simplificação de ferramentas de segurança, parecem desempenhar papel relevante na proteção dos usuários contra ataques de phishing na plataforma e no fortalecimento da segurança digital.

4.2 LIMITAÇÕES

Este estudo apresenta algumas limitações que devem ser consideradas,as quais também abrem possibilidades para pesquisas futuras. Uma das principais limitações é o tamanho da amostra (108 participantes) e a utilização de uma amostragem não probabilística por conveniência. Esse método, apesar de viável para estudos exploratórios, não permite a generalização dos resultados para toda a população de usuários do Instagram, pois os dados foram coletados apenas de indivíduos acessíveis ao pesquisador. Em especial, cidadãos, estudantes e professores com alguma relação com o Instituto Federal de Ciências e Tecnologia do Piauí, campus de Pedro II. Outro fator a ser considerado é que os dados foram coletados por meio de autorrelato,
ou seja, os participantes avaliaram o quanto acham que sabem sobre phishing. Esse método pode fazer com que alguns respondentes exagerem na sua capacidade de identificar ataques, levando alguns respondentes a superestimarem ou subestimarem sua capacidade de identificar ataques. Também vale destacar que os dados refletem um momento específico, e as estratégias utilizadas por cibercriminosos evoluem rapidamente. Assim, futuras pesquisas podem realizar um estudo

da evolução desses ataques em plataformas de redes sociais durante os anos.

5 CONCLUSÕES E TRABALHOS FUTUROS

Este estudo analisou as vulnerabilidades de um grupo de usuários do Instagram a ataques de phishing, investigando o nível de conhecimento em segurança digital e a influência da formação em Tecnologia da Informação (TI) na adoção de práticas protetivas. Para isso, utilizou-se um método quantitativo por meio de um questionário estruturado aplicado a 108 participantes, por meio do Google Forms e distribuído por aplicativos de mensagem, permitindo a identificação de padrões de comportamento e lacunas na conscientização sobre segurança digital.

Os principais resultados indicam que, embora uma parcela significativa dos participantes tenha ouvido falar sobre phishing, a compreensão aprofundada sobre o tema ainda é limitada. Conclui-se, a partir dos dados coletados, que a formação em TI tem influencia direta e positiva na adoção de medidas de proteção, como a autenticação em dois fatores e a verificação de URLs. No entanto, observou-se que, mesmo entre esses usuários mais preparados, ainda existem comportamentos de risco, reforçando a necessidade de estratégias mais eficazes e frequentes de conscientização. Além disso, identificou-se que a confiança excessiva dos usuários em sua própria capacidade de detectar golpes pode fazer com que ignorem medidas básicas de proteção, tornando-os mais suscetíveis a ataques no ambiente do Instagram.

Acredita-se que os resultados deste estudo possam complementar o corpo de conhecimento existente e contribuir para a ampliação do conhecimento na área de cibersegurança em redes sociais, especialmente no que se refere à relação entre conhecimento técnico e exposição a riscos de phishing no Instagram. Destaca-se ainda a importância da implementação de campanhas educativas mais eficazes, que não apenas ensinem boas práticas, mas também alertem sobre os riscos de superestimar a capacidade de reconhecer golpes. Além disso, medidas preventivas mais rigorosas, como a criação de alertas educativos diretamente na interface do Instagram, poderiam auxiliar a mitigar essas ameaças.

No entanto, algumas limitações deste estudo devem ser consideradas, o tamanho da amostra, embora relevante, não permite uma generalização ampla dos resultados. Além disso, o foco exclusivo no Instagram restringe a compreensão da vulnerabilidade a ataques de phishing em outras plataformas. Pesquisas futuras podem ampliar essa análise para diferentes redes sociais, faixas etárias e contextos de uso, bem como avaliar a eficácia de diferentes abordagens de conscientização sobre segurança digital.

5.1 TRABALHOS FUTUROS

Estudos futuros poderiam criar um perfil fictício no Instagram, os participantes seriam convidados a adicionar esse perfil ao responder a uma solicitação de amizade. A partir disso, os participantes poderiam comentar sobre como reagiriam a postagens e interações que aparecessem em seu feed, além de mensagens diretas com algo de interesse dos usuários ,originadas do perfil fictício. Contudo, essa abordagem precisaria ser planejada com cuidado, respeitando as diretrizes éticas e boas práticas. Outra possibilidade seria o uso de inteligência artificial para criar mensagens altamente convincentes, juntamente com outros tipos de ataques,como o deepfake, avaliando o nível de vulnerabilidade dos usuários a essas ameaças, podendo expandir a outras plataformas de redes sociais. Essas investigações poderiam contribuir para o desenvolvimento de estratégias mais eficazes de prevenção e conscientização, ajudando a reduzir o impacto dos ataques de phishing em redes sociais.

REFERÊNCIAS

ABURROUS, M. *et al.* Experimental case studies for investigating e-banking phishing techniques and attack strategies. **Cognitive Computation**, v. 2, n. 3, p. 242–253, 2010. Disponível em: https://doi.org/10.1007/s12559-010-9042-7 . Acesso em: 10 fev. 2025.

AL-DUWAIRI, B. *et al.* On the digital forensics of social networking web-based applications. In: **2022 10th International Symposium on Digital Forensics and Security (ISDFS**). Istanbul, Turkey, 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800839. Disponível em: https://ieeexplore.ieee.org/document/9800839. Acesso em: 17 dez. 2024.

ALBLADI, S.; WEIR, G. User characteristics that influence judgment of social engineering attacks in social networks. **Human-centric Computing and Information Sciences**, v. 8, 12 2018. Disponível em: https://www.researchgate.net/publication/323455755_User_characteristics_that_influence_judgment_of_social_engineering_attacks_in_social_networks .Acesso em: 17 dez. 2024.

ALHARBI, A. *et al.* Security in social-media: Awareness of phishing attacks techniques and countermeasures. In: **2022 2nd International Conference on Computing and Information Technology (ICCIT**), Tabuk, Saudi Arabia, 2022, pp. 10-16, doi: 10.1109/ICCIT52419.2022.9711640. Disponível em: https://ieeexplore.ieee.org/document/9711640. Acesso em: 17 dez. 2024.

ALI *et al.* A survey on deceptive phishing attacks in social networking environments In: Raju, K., Govardhan, A., Rani, B., Sridevi, R., Murty, M. (eds**) Proceedings of the Third International Conference on Computational Intelligence and Informatics** . Advances in Intelligent Systems and Computing, vol 1090. Springer, Singapore. Disponível em: https://www.researchgate.net/publication/339993276_A_Survey_on_Deceptive_Phishing_Attacks_in_Social_Networking_Environments. Acesso em: 10 jan. 2025.

ALLODI, L. *et al.* The need for new antiphishing measures against spear-phishing attacks. **IEEE Security Privacy**, v. 18, n. 2, p. 23–34, 2020. Disponível em: https://ieeexplore.ieee.org/document/8852647. Acesso em: 10 jan. 2025.

ALMUDAHI, G. F. *et al.* Social media privacy issues, threats, and risks. In: **2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU)**. Riyadh, Saudi Arabia, 2022, pp. 155-159, doi: 10.1109/WiDS-PSU54548.2022.00043. Disponível em: https://ieeexplore.ieee.org/document/9764859. Acesso em: 17 de fev. 2025.

APUKE, O. Quantitative research methods : A synopsis approach. **Arabian Journal of Business and Management Review (kuwait Chapter).**, v. 6, p. 40–47, 10 2017. Disponível em: https://www.researchgate.net/publication/320346875_Quantitative_Research_Methods_A_Synopsis_Approach. Acesso em: 17 jan. 2025.

ARRUDA FILHO,M. C; FARIAS, E. J. M.. Planejamento da Pesquisa Científica. **2. ed. São Paulo: Atlas, 2015. E-book. ISBN 9788522495351.** Disponível em: https://www.grupogen.com.br/e-book-planejamento-da-pesquisa-cientifica. Acesso em: 17 de nov. 2024.

AVAST. Golpes de phishing no Instagram — Como identificar e evitar golpistas. **2022. Avast Software a.s**. Publicado em 21 de julho de 2022. Disponível em: https://www.avast.com/pt-br/cinstagram-scams. Acesso em: 10 fev. 2025.

BAIG, M. S.; AHMED, F.; MEMON, A. M. Spear-phishing campaigns: Link vulnerability leads to phishing attacks, spear-phishing electronic/uav communication-scam targeted. In: **2021 4th International Conference on Computing Information Sciences (ICCIS)**, Karachi, Pakistan, 2021, pp. 1-6, doi: 10.1109/ICCIS54243.2021.9676394. Disponível em: https://ieeexplore.ieee.org/document/9676394. Acesso em: 17 jan. 2025.

BASIT, A. *et al.* A comprehensive survey of ai-enabled phishing attacks detection techniques. **Telecommunication Systems**, v. 76, p. 139–154, 2021. Disponível em: https://doi.org/10.1007/s11235-020-00733-2. Acesso em: 17 jan. 2025.

BODNAR, D. Golpes de phishing no Instagram — Como identificar e evitar golpistas. 2022. **Avast Software a.s**. Publicado em 21 de julho de 2022. Disponível em: https://www.avast.com/pt-br/c-instagram-scams. Acesso em: 17 dez. 2024.

BRASIL. **Agência Brasileira de Inteligência**. Guia para Proteção de Conhecimentos Sensíveis. Brasília: ABIN, 2023. Disponível em: https://www.gov.br/abin/ptbr/institucional/acoes-eprogramas/PNPC/boaspraticas/cartilha engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis . Acesso em: 17 jan. 2025.

BRASIL. **Ministério da Saúde. Conselho Nacional de Saúde**. Resolução no 466, de 12 de dezembro de 2012. 2012. Trata de diretrizes e normas regulamentadoras de pesquisas envolvendo seres humanos. Brasília, 2012. Disponível em:

https://bvsms.saude.gov.br/bvs/saudelegis/cns/2013/res0466_12_12_2012.html. Acesso em: 17 jan. 2025.

CARNEIRO, E.; FARINA, R.; FLORIAN, F. Eficiênca e efetividade de métodos de autenticação em duas etapas: Uma revisão bibliográfica. **Revista ft**, p. 28–29, 09 2024. Disponível em: https://www.researchgate.net/publication/384469661_EFICIENCIA_E_EFETIVIDADE_DE_METODOS_DE_AUTENTICACAO_EM_DUAS_ETAPAS_UMA_REVISAO_BIBLIOGRAFICA. Acesso em: 17 jan. 2025.

CHRYSANTHOU, A.; PANTIS, Y.; PATSAKIS, C. The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign. **Computers Security**, v. 140, p. 103780, 2024. ISSN 0167-4048. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404824000816. Acesso em: 17 dez. 2024.

DOLHANSKY, B. *et al.* The deepfake detection challenge (dfdc) dataset. **arXiv preprint arXiv:2006.07397**, 2020. Disponível em: https://arxiv.org/abs/2006.07397. Acesso em: 17 dez. 2024.

ELLAHI, O. *et al.* Analyzing 2fa phishing attacks and their prevention techniques. In: **2022 International Conference on Smart Information Systems and Technologies (SIST)**, Nur-Sultan, Kazakhstan, 2022, pp. 1-6, doi: 10.1109/SIST54437.2022.9945766. Disponível em: https://ieeexplore.ieee.org/document/9945766. Acesso em: 17 dez. 2024.

ETIKAN, I.; MUSA, S. A.; ALKASSIM, R. S. Comparison of convenience sampling and purposive sampling. **American Journal of Theoretical and Applied Statistics**, v. 5, n. 1, p. 1–4, 2015. Disponível em: https://doi.org/10.11648/j.ajtas.20160501.11. Acesso em: 17 dez. 2024.

FONTES, E. **SEGURANÇA DA INFORMAÇÃO**. Editora Saraiva, 2017. ISBN 9788502122192. Disponível em: https://books.google.com.br/books?id=FyprDwAAQBAJ. Acesso em: 17 dez. 2024.

FRAUENSTEIN, E. D.; FLOWERDAY, S. Susceptibility to phishing on social network sites: A personality information processing model. **Computers Security**, v. 94, p. 101862, 2020. ISSN 0167-4048. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404820301346. Acesso em: 17 dez. 2024.

FRAUENSTEIN, E. D.; FLOWERDAY, S. V. Social network phishing: Becoming habituated to clicks and ignorant to threats? In: **2016 Information Security for South Africa (ISSA)**, Johannesburg, South Africa, 2016, pp. 98-105, doi: 10.1109/ISSA.2016.7802935. Disponível em: https://ieeexplore.ieee.org/document/7802935. Acesso em: 17 jan. 2025.

GARCIA, I. O. dos S. **Bibliotecas no Instagram: um estudo sobre o uso do aplicativo por unidades de informação**. Monografia, Rio de Janeiro, 2017. 85 f. Trabalho de Conclusão de Curso em Biblioteconomia e Gestão de Unidades de Informação. Disponível em: https://pantheon.ufrj.br/handle/11422/2561. Acesso em: 31 jan. 2025.

GONZALEZ, H.; NANCE, K.; NAZARIO, J. Phishing by form: The abuse of form sites. In: **2011 6th International Conference on Malicious and Unwanted Software**, Fajardo, PR, USA, 2011, pp. 95-101, doi: 10.1109/MALWARE.2011.6112332. Disponível em: https://ieeexplore.ieee.org/document/6112332. Acesso em: 31 jan. 2025.

GRBIC, D. V.; DUJLOVIC, "Social engineering with ChatGPT," **2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH),** East Sarajevo, Bosnia and Herzegovina, 2023, pp. 1-5, doi: 10.1109/INFOTEH57020.2023.10094141. Disponível em: https://ieeexplore.ieee.org/document/10094141. Acesso em: 31 de jan. 2025.

GROUP, A.-P. W. **Phishing Activity Trends Report, 1st Quarter 2024**. 2024. APWG. Publicado em 14 de maio de 2024. Disponível em: https://apwg.org/trendsreports/. Acesso em: 06 ago 2024.

HILTON, C. The importance of pretesting questionnaires: a field research example of cognitive pretesting the exercise referral quality of life scale (er-qls). **International Journal of Social Research Methodology**, p. 1–14, 10 2015. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/13645579.2015.1091640. Acesso em: 31 de jan. 2025.

JYOTHI; BADIGER, V. N.; SHIVAKUMAR, V. Security in social networks and media. In: **2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS)**. Bangalore, India, 2023, pp. 651-654, doi: 10.1109/ICAECIS58353.2023.10170002. Disponível em: https://www.researchgate.net/publication/372205407_Security_in_Social_Networks_and_Media. Acesso em: 10 de fev. 2025.

KABIR, S. M. Methods of data collection. **In Basic Guidelines for Research**: An Introductory Approach for All Disciplines (Chap. 9, pp. 201-275). Bangladesh: Book Zone Publication. Disponível em: https://www.researchgate.net/publication/325846997_METHODS_OF_DATA_COLLECTION. Acesso em: 10 fev. 2025.

KANAGUSKU, A. R. A.; GASETA, E. Fator humano na segurança da informaÇÃo: Desmistificando o elo mais fraco. **FatecSeg - Congresso de Segurança da Informação**, 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/ 114. Acesso em: 17 jan. 2025.

KASPERSKY. O Panorama de Ameaças de 2023 da Kaspersky. 2023. **Kaspersky Lab AO**. Publicado em 28 de novembro de 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/inteligencia-artificial-para-o-bem-ou-mal. Acesso em: 17 jan. 2025.

KAYA, G. A.; SANDERS, B. An analysis on the relation between users' online social networks addiction and users security concerns. 86-92. 10.5220/0010565100002997. Disponível em: https://www.researchgate.net/publication/357777413_An_Analysis_on_the_Relation_between_Users'_Online_Social_Networks_Addiction_and_Users_Security_Concerns. Acesso em: 10 fev. 2025.

KRUGER, H.; KEARNEY, W. A prototype for assessing information security awareness.

Computers Security, v. 25, n. 4, p. 289–296, 2006. ISSN 0167-4048. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404806000563. Acesso em: 11 fev. 2025.

MALATJI, M. Management of enterprise cyber security: A review of iso/iec 27001:2022. In: **2023 International Conference On Cyber Management And Engineering (CyMaEn)**.2023. p. 117–122. Disponível em: https://www.researchgate.net/publication/368911662_Management_of_enterprise_cyber_security_A_review_of_ISOIEC_270012022. Acesso em: 10 fev. 2025.

MITNICK, K.; SIMON, W. L. **The Art of Deception: Controlling the Human Element of Security**. [S.l.]: Wiley, 2002. ISBN 0471237124. Disponível em: https://portal.abuad.edu.ng/lecturer/documents/1585589655The_Art_of_Deception_by_Kelvin_Mitnick.pdf. Acesso em: 10 dez. 2024.

MORENO-FERNÁNDEZ, M. M *et al.* Fishing for phishers. Improving Internet users sensitivity to visual deception cues to prevent electronic fraud, **Computers in Human Behavior**,Volume 69,2017,Pages 421-436,ISSN 0747-5632,Disponível em: https://www.sciencedirect.com/science/article/pii/S074756321630872X. Acesso em: 11 fev. 2025.

NASUTION, M. R. *et al.* Defense in depth strategy from phising attacks in using instagram. In: **2024 International Conference on Data Science and Its Applications (ICoDSA**), Kuta, Bali, Indonesia, 2024, pp. 122-127, doi: 10.1109/ICoDSA62899.2024.10651679. Disponível em: https://ieeexplore.ieee.org/document/10651679. Acesso em: 17 fev. 2025.

RAHMAN, M. S.; REZA, H. A systematic review towards big data analytics in social media. **Big Data Mining and Analytics**, v. 5, n. 3, p. 228–244, 2022. Disponível em: https://www.researchgate.net/publication/361262797_A_Systematic_Review_Towards_Big_Data_Analytics_in_Social_Media. Acesso em: 17 fev. 2025.

SARI, P. K.; PRASETIO, A. Knowledge sharing and electronic word of mouth to promote information security awareness in social network site. In: **2017 International Workshop on Big Data and Information Security (IWBIS)**. Jakarta, Indonesia, 2017, pp. 113-117, doi: 10.1109/IWBIS.2017.8275111. Disponível em: https://ieeexplore.ieee.org/document/8275111. Acesso em: 17 jan. 2025.

SCHNEIER, B. **Secrets and Lies: Digital Security in a Networked World**. [S.l.]: John Wiley & Sons, 2000. ISBN 0471253111. Disponível em: https://accord.edu.so/web/content/32538?download=true&access_token=d5a8988c-4ac7-4eed-872f-c206fd8bd147. Acesso em: 17 dez. 2024.

SOUSA, S. *et al.* O uso do instagram® como ferramenta de divulgação científica. In: **VII CONEDU - Conedu em Casa**. Realize Editora, 2021. Disponível em: https://editorarealize.com.br/artigo/visualizar/79855. Acesso em: 10 dez. 2024.

SURJANDY *et al.* Analysis of social influence, trust, and accuracy on actual use of social media messaging application based on information security model. In: **2023 International Conference on Information Technology Research and Innovation (ICITRI)**. 93-98.

10.1109/ICITRI59340.2023.10249421. Disponível em: https://ieeexplore.ieee.org/document/10249421. Acess em: 17 jan. 2025.

SYAMSUAR, D.; DARREN, C. Integrating trust and risk perception into utaut: Study about consumers' purchase intentions in social media. In:**2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)**. 2023. p. 55–60. Disponível em: https://ieeexplore.ieee.org/document/10349044. Acesso em: 17 jan. 2025.

TAVARES, T. K. da C. O fator humano na segurança de informação nas organizações. 2017. Dissertação (Mestrado em Segurança de Informação e Direito no Ciberespaço) – **Universidade de Lisboa,** Lisboa, 2017. Disponível em: https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973967179/Dissertacao%20o%20Fator%20Humano%20na%20Seguranca.pdf. Acesso em: 10 fev. 2025.

TEOTIA, H. *et al.* Instagram analysis and activity automation: Using python and selenium automation tools. In: **2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)**. Ghaziabad, India, 2023, pp. 522-526. Disponível em: https://ieeexplore.ieee.org/document/10140356. Acesso em: 17 fev. 2025.

VARSHNEY, G. *et al.* Anti-phishing: A comprehensive perspective. **Expert Systems with Applications**, v. 238, p. 122199, 2024. ISSN 0957-4174. Disponível em: https://www.sciencedirect.com/science/article/pii/S095741742302701X. Acesso em: 10 fev. 2025.

WE ARE SOCIAL, MELTWATER, "Digital 2024: Global Overview Report. 2024.", Disponível em: https://datareportal.com/reports/digital-2024-brazil. Acesso em: 17 nov. 2024.

WILCOX, H.; BHATTACHARYA, M. A framework to mitigate social engineering through social media within the enterprise. In: **2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)**. [S.l.: s.n.], 2016. p. 1039–1044. Disponível em: https://ieeexplore.ieee.org/document/7603735/. Acesso em: 17 jan. 2025.