Phishing via Mensagens Instantâneas em Dispositivos Móveis: Uma Revisão Sistemática sobre Estratégias de Ataque e Vulnerabilidades Humanas

Thiago Faria
Instituto de Informática
UFG
Goiânia, Brasil
thiagomourafaria2@gmail.com

Maurício Lima
Instituto de Informática
UFG
Goiânia, Brasil
k20x@outlook.com

Elisângela Silva Dias
Instituto de Informática
UFG
Goiânia, Brasil
elisangelasd@ufg.br

Augusto César Falcão
Instituto de Informática
UFG
Goiânia, Brasil
augustocesar.ffalcao@gmail.com

***Abstract*—This study aims to analyze the characteristics of smishing, a form of phishing attack that uses instant messaging as a channel to deceive mobile device users. The study focuses on an analysis centered on human vulnerabilities, seeking to understand the attack strategies employed by cybercriminals. Based on a systematic literature review using the PRISMA 2020 methodology and conducted with the support of the Parsifal tool, searches were performed in the ACM Digital Library, IEEE Digital Library, Scopus, Springer Link, and SBC OpenLib (SOL) databases. Initially, 10,891 studies were identified, of which 12 were included after the screening process. The study revealed some recurring approaches, such as the use of shortened URLs and emotional manipulation, and discusses the need for further scientific research on the topic in order to propose the integration of technological and educational measures to mitigate the risks posed by these attacks and to suggest directions for future research.**

***Keywords*—Phishing; Smishing; Mobile Devices.**

***Resumo*—Este estudo se propõe a analisar as características do *smishing*, uma modalidade de ataque *phishing* que utiliza mensagens instantâneas como canal para enganar usuários de dispositivos móveis. O estudo foca em uma análise centrada nas vulnerabilidades humanas, buscando compreender as estratégias de ataque empregadas pelos cibercriminosos. A partir de uma revisão sistemática de literatura, que utilizou a metodologia PRISMA 2020 e foi conduzida com o apoio da ferramenta Parsifal, foram realizadas buscas nas bases de dados ACM Digital Library, IEEE Digital Library, Scopus e Springer Link e SBC OpenLib (SOL). Inicialmente, foram identificados 10.891 estudos, sendo 12 incluídos após o processo de triagem. O estudo revelou algumas abordagens recorrentes, como o uso de URLs encurtadas e manipulação emocional, e discute a necessidade de mais pesquisas científicas sobre o tema, a fim de propor a integração de medidas tecnológicas e educacionais para mitigar os riscos relacionados a esses ataques e sugerir caminhos para pesquisas futuras.**

***Palavras-chave*—Phishing; Smishing; Dispositivos Móveis.**

I. Introdução

O *phishing*, crime digital no qual criminosos extraem de suas vítimas informações pessoais e sensíveis, tem se apresentado como um desafio para a cibersegurança, principalmente a partir de 2020, onde teve seu crescimento potencializado durante os anos de isolamento social decorrente da pandemia do COVID-19 e seguiu avançando até o ano de 2024, motivando um estudo acerca das características de tais ataques e das vulnerabilidades às quais os usuários estão expostos [1].

Considerando os *smartphones* como um dos itens fundamentais para a sociedade moderna, surge a oportunidade para os criminosos de lesar usuários por meio deste canal que está quase sempre ao alcance das mãos [2]. Relatórios de ataques de *phishing* demonstram um aumento contínuo no percentual de ataques baseados em números de telefone, em relação ao total de ataques reportados [3], gerando enormes perdas. Em 2020, um relatório do *Federal Bureau of Investigation* (FBI), a principal agência de segurança interna e inteligência do governo dos Estados Unidos, demonstrou que naquele ano, perdas relacionadas a esse tipo de fraude excederam 4,1 bilhões de dólares no país [4].

O *phishing* não é uma novidade, tendo seu primeiro registro relatado em 1996, em um ataque por *e-mail* [5]. Entretanto, os criminosos têm voltado sua atenção para os dispositivos móveis, pois esses armazenam não apenas fotos e conversas pessoais, mas também informações de acesso a instituições financeiras e redes sociais. Criminosos, cientes da relação quase emocional dos humanos com seus dispositivos móveis, adaptam suas estratégias criminosas para explorar esses dispositivos como vetores de ataques de *phishing* [2].

Uma das adaptações do *phishing* a esse cenário é o *smishing*, termo derivado da combinação de *SMS* [6] e *phishing*.

Nesse contexto, plataformas de mensagens instantâneas como *SMS*, *WhatsApp* [7], *Telegram* [7], entre outras, são utilizadas como canais de ataque [2], [8]. Essa abordagem tem acendido um alerta na comunidade acadêmica devido a relatórios que apresentam um aumento expressivo de ataques de *smishing* no ano de 2021 [9], [10]. Tal aumento, associado a um alto índice de sucesso desses ataques [11], justifica o estudo das características do *smishing* e a investigação e compreensão dos fatores que tornam os usuários mais vulneráveis a essa prática. A cartilha desenvolvida pelo CERT [12] possui uma seção dedicada ao *phishing*, entretanto essa seção não trata do *smishing* e das vulnerabilidades relacionadas ao uso de *smartphones* nesse contexto.

O objetivo geral deste trabalho é mapear as características dos ataques de *smishing* em dispositivos móveis, abrangendo estratégias de ataque, vulnerabilidades humanas exploradas por estas e estado da pesquisa, a fim de apoiar novas medidas de proteção.

Entre os objetivos específicos está a identificação e classificação das técnicas e dos canais utilizados, com destaque para as abordagens de engenharia social, prática que explora vulnerabilidades dos usuários para aumentar a taxa de sucesso de ataques, levando em conta fatores comportamentais, contextuais e sociais explorados pelos invasores. Além disso, caracteriza o panorama acadêmico atual, analisando as principais áreas de foco e a distribuição temporal e regional dos trabalhos.

A sequência deste trabalho está organizada da seguinte maneira: A seção 2 apresenta conceitos acerca das subcategorias de ataques de *pishing* e dependência humana do uso de *smartphones*que gera vulnerabilidades exploradas por criminosos. A seção 3, por sua vez, apresenta os trabalhos relacionados, que corroboram à relevância do assunto *smishing* e em quais lacunas o presente estudo possui ênfase. A Seção 4 descreve os procedimentos metodológicos, abordando as questões de pesquisa, as bases de dados consultadas, as ferramentas e os critérios de inclusão e exclusão usados para selecionar os estudos desta revisão. A seção 5, traz respostas para cada questão de pesquisa e discute a distribuição geográfica, temporal e histórica dos ataques de *pishing*, além de estratégias de mitigação desses ataques. A seção 6, condensa todo o estudo, e por fim, levanta a importância de uma discussão mais forte sobre esse tema no Brasil, considerando a LGPD [13]. A última seção, lista as referências utilizadas na produção desse trabalho.

II. Fundamentação Teórica

A engenharia social recorre à manipulação psicológica para explorar vulnerabilidades humanas, levando usuários a decisões inseguras e ao vazamento de dados sensíveis. Os dispositivos móveis são ricos em informações pessoais e profissionais, tornando-os alvos frequentes de ataques [14]. A dependência e confiança dos usuários nesses dispositivos amplifica a eficácia dessas investidas [15].

O *phishing* combina persuasão e tecnologia para furtar credenciais e dados bancários. Registrado nos anos 1990 via *e-mail*, o método migrou para o cenário móvel, recorrendo a links encurtados e mensagens que exploram a crença do usuário na aparente legitimidade dessas mensagens [16]. Variações como *smishing*, *vishing* e *QRshing* evidenciam a diversificação dessas fraudes conforme evoluem a tecnologia e o comportamento social [5], [17].

A. Engenharia social e sua relação com dispositivos móveis

A engenharia social explora a persuasão para induzir vítimas a revelar dados ou adotar comportamentos prejudiciais, focando nas falhas humanas em vez de brechas técnicas [14]. A coleta massiva de dados (*Big Data*) permite traçar perfis detalhados e personalizar ataques, ampliando o sucesso dessas investidas [14]. O conceito de *human hacking* reforça esse caráter manipulativo, pois visa quebrar procedimentos de segurança por meio da interação social [18], [19].

Durante a pandemia de COVID-19, o tempo gasto *on-line* por usuários de *smartphones* cresceu e a falta de preparo em cibersegurança abriu espaço para mais ataques. Campanhas de *phishing* abusaram do medo e da incerteza, usando mensagens que imitavam organizações confiáveis para obter informações sensíveis [15], [20], [21].

Em 2017 o número de usuários de *smartphones* superou 4,9 bilhões [22]. A mobilidade, o uso intensivo de redes sociais, aplicativos bancários e mensageiros e a confiança depositada nesses serviços, tornam os dispositivos móveis alvos preferenciais para *phishing* e *smishing* [23], [24]. Fatores como ausência de treinamento em segurança, verificação insuficiente da autenticidade das mensagens e uso de *smartphones* para transações sensíveis elevam a vulnerabilidade dos usuários [14], [25].

B. Phishing

O *phishing* é amplamente descrito como um ataque baseado em engenharia social, no qual criminosos induzem vítimas a fornecer informações confidenciais por meio da personificação de entidades legítimas [5], [16], [26]. O termo deriva de *fishing*, aludindo ao uso de uma "isca" para capturar dados como senhas e informações bancárias [16].

Relatórios do *Anti-Phishing Working Group* (APWG) apontam um crescimento expressivo desses ataques: de cerca de 200.000 registros em abril de 2021, para 600.000 em março de 2023 [9]. Esse aumento se relaciona à digitalização acelerada de atividades cotidianas no século XXI [15], intensificada pela pandemia de COVID-19, que elevou em 47% o uso de banda

larga no pico da crise [27]. O cenário favoreceu ataques como *malware*, *ransomware* e especialmente *phishing*.

A origem do *phishing* remonta a 1996, com ataques direcionados a usuários da AOL, onde *hackers*, se passando por funcionários da empresa, solicitavam senhas via *e-mail*, explorando a confiança dos usuários [5]. Com o tempo, o avanço tecnológico e o uso massivo de dispositivos móveis tornaram os ataques mais sofisticados e direcionados [22]. A confiança dos usuários em seus aplicativos ampliam as vulnerabilidades exploradas pelos atacantes. Além de técnicas clássicas, como a clonagem de páginas de *login*, surgiram aplicativos maliciosos disfarçados de legítimos [22].

Segundo o relatório da APWG para o primeiro semestre de 2024, o *smishing* desponta como uma das abordagens mais frequentes em fraudes via telefone [3]. Diante disso, classificar as formas de *phishing* conforme os meios utilizados é essencial para o desenvolvimento de medidas específicas de proteção. As principais variantes incluem *smishing*, *vishing* e *QRshing* [4]. Já descrevemos o *smishing* anteriormente. Vamos descrever as demais:

Vishing: explora chamadas telefônicas como canal de ataque. Golpistas se passam por representantes de empresas e, por meio de persuasão, induzem vítimas a compartilhar dados sensíveis [28].

QRshing: envolve o uso de *QR codes* maliciosos que direcionam a páginas falsas, explorando a confiança excessiva do usuário na legitimidade e praticidade do escaneamento por dispositivos móveis [29].

Além dessas abordagens, existem formas tradicionais não necessariamente vinculadas a dispositivos móveis, como o *phishing* de clonagem, que replica páginas legítimas para capturar dados do usuário [1], e o *spear phishing*, um ataque direcionado com base em informações previamente obtidas sobre a vítima [30]. Muitos ataques combinam múltiplas técnicas, reforçando a necessidade de uma compreensão ampla e estratégica para enfrentamento dessas ameaças [21].

III. Trabalhos Relacionados

O aumento dos ataques de *phishing*, em especial do *smishing*, impulsionou a produção de estudos que buscam compreender essas ameaças e propor meios de mitigá-las. A literatura consultada fundamentou os objetivos deste trabalho ao apontar estratégias de defesa, lacunas de pesquisa e desafios regulatórios.

Naqvi et al. [31] revisam 248 estudos sobre *phishing* e classificam as soluções em sistemas *anti-phishing*, modelos ou *frameworks* e estratégias centradas no humano. Apenas seis investigações abordam *smishing*, revelando a predominância de pesquisas focadas em *websites* e *e-mails*. A ênfase em abordagens exclusivamente tecnológicas negligencia o fator humano, lacuna que reforça a necessidade de estudos voltados à vulnerabilidade do usuário.

Goenka et al. [4] apresenta uma taxonomia de meios, alvos e técnicas de *phishing*. O trabalho destaca o *smishing* como vetor emergente, associado a aumento de 70% nos ataques móveis em 2022. Fatores como a taxa de abertura de *SMS* de 98% e limitações inerentes às telas pequenas ampliam a exposição do usuário, tornando indispensável uma análise específica dessa modalidade.

Zieliński et al. [2] discutem o impacto de ataques móveis no contexto polonês, com ênfase em aspectos legais. O estudo mostra que a proximidade emocional dos usuários com seus *smartphones*, somada ao armazenamento de dados pessoais e financeiros, eleva a eficácia das fraudes. As taxas de resposta variam de 4% a 17,87%, influenciadas sobretudo por medo e ganância.

Esses trabalhos convergem ao evidenciar a relevância do *smishing*, mas divergem quanto ao foco principal: necessidades de pesquisa sobre o fator humano [31], vulnerabilidades técnicas dos dispositivos móveis [4] e aspectos psicossociais das vítimas [2]. O presente estudo busca integrar essas perspectivas, mapeando características de ataque e fraquezas humanas, para fomentar estratégias de defesa que combinem tecnologia, educação e regulamentação.

IV. Metodologia

Este estudo apresenta uma Revisão Sistemática da Literatura (RSL), caracterizada por uma metodologia estruturada e replicável, envolvendo uma busca abrangente para localizar todos os trabalhos publicados sobre um determinado tema; uma integração sistemática dos resultados dessa busca; e uma análise crítica da abrangência, natureza e qualidade das evidências em relação a uma específica questão de pesquisa. As RSLs sintetizam estudos para extrair conclusões teóricas amplas sobre o significado de uma literatura, conectando teoria e evidência [32].

Adotou-se a metodologia *PRISMA* em sua versão de 2020 [33] e o *Parsifal* para planejamento, execução, condução e documentação da pesquisa [34]. As palavras-chave foram selecionadas para abordar os diversos sinônimos de dispositivos móveis, bem como os de *smishing* e mensagens instantâneas.

As buscas foram realizadas nas seguintes bases de dados: *ACM Digital Library*, *EI Compendex*, *IEEE Digital Library*, *ISI Web of Science*, *Science Direct*, *Scopus*, *Sol SBC* e *Springer Link*. O processo de seleção dos estudos seguiu uma triagem em duas etapas, conduzida por dois revisores independentes, que avaliaram a elegibilidade dos trabalhos com base na presença das palavras-chave nos títulos e resumos. Em casos de discordância, um terceiro revisor foi consultado para garantir consenso e minimizar possíveis vieses.

A extração de dados foi sistemática e orientada para coletar informações relevantes de cada artigo selecionado. O foco principal foi analisar as características e adaptações dos ataques de *phishing* realizados por meio de mensagens instantâneas em dispositivos móveis. A análise dos dados incluiu uma avaliação qualitativa dos resultados, buscando padrões e temas recorrentes nos estudos, a fim de interpretar as evidências e garantir a consistência das conclusões extraídas.

A. Execução

Esta seção apresenta a execução da revisão sistemática da literatura (RSL) proposta para esse trabalho, conduzida em conformidade com as diretrizes do PRISMA 2020 [33], que reforça a transparência e o rigor no processo de identificação, triagem e seleção de estudos necessários para RSL. Foram utilizadas estratégias de busca abrangentes em bases de dados empregadas de forma recorrente em outros estudos dessa mesma categoria [2], [4], aplicando critérios bem definidos para incluir apenas artigos que abordassem ataques de *smishing* e excluindo estudos duplicados, literatura cinza e aqueles focados em detecção computacional, resultando na inclusão de 12 estudos elegíveis para análise aprofundada.

1) Questões de Pesquisa: Esta revisão tem como objetivo responder às seguintes questões de pesquisa:

`QP1`: Quais técnicas e estratégias têm sido descritas na literatura para a realização de ataques de *smishing*, considerando diferentes formas de engenharia social e variações nos meios de comunicação?

`QP2`: Como os ataques *smishing* que utilizam de plataformas de mensagem instantânea tem sido explorados pela comunidade acadêmica, considerando a distribuição temporal das publicações, os principais interesses de pesquisa identificados e a distribuição geográfica dos estudos?

`QP3`: Quais fatores humanos influenciam a suscetibilidade das pessoas a ataques de *smishing* e quais abordagens têm sido sugeridas para mitigar essa vulnerabilidade?

O interesse com a QP1 adentra-se na compreensão de técnicas *smishing*, possibilitando a identificação de métodos de ataque, desenvolvimento de medidas preventivas, e o aprimoramento da segurança de usuários e sistemas. Já na QP2, há o interesse em analisar esses fatores, fornecendo subsídios para ações educativas, políticas públicas e soluções tecnológicas que reduzam vulnerabilidades associadas ao comportamento humano. Por fim, a Qp3 se faz necessária tendo em vista o objetivo de obter uma avaliação da distribuição temporal, geográfica e dos focos de pesquisa ajuda a identificar lacunas no conhecimento e tendências das práticas criminosas.

2) Critérios de Inclusão: Afim de definir os critérios de inclusão (CI) de estudos para esta RSL, foram considerados os achados em trabalhos correlatos sobre o tema. Esses indicam que, apesar da alta relevância do tema, a literatura ainda demonstra estar aquém do ideal para a formulação de diretrizes claras que orientem o desenvolvimento de estratégias de mitigação, além de evidenciar uma escassez de estudos acerca do tema desta pesquisa [31].

Dessa forma, para a realização deste estudo, foi definido apenas um critério de inclusão mais abrangente, exigindo apenas que o estudo aborde o tema deste trabalho. Assim, foram selecionados os estudos de acordo com o seguinte critério de inclusão:

`CI1`: O estudo aborda ataques de *phishing* através de mensagens instantâneas em dispositivos móveis.

3) Critérios de Exclusão: Para exclusão de estudos, foram considerados alguns resultados de trabalhos correlatos, que indicam uma predominância de estudos relacionados a detecções baseadas em abordagens computacionais para mitigar o *smishing*. Considerando que o intuito desta pesquisa é entender características humanas que aumentam a suscetibilidade a esses golpes, serão excluídos os estudos baseados em abordagens de detecção computacional.

Foram excluídos os estudos de acordo com os seguintes critérios de exclusão (CE):

`CE1`: O estudo está duplicado.

`CE2`: O estudo não é um artigo primário.

`CE3`: O estudo é direcionado a métodos de detecção computacional.

`CE4`: O estudo é literatura cinza.

`CE5`: O estudo possui menos de 5 páginas.

`CE6`: O estudo é uma versão prévia de outro estudo pré-selecionado.

`CE7`: O estudo não é disponibilizado integralmente.

`CE8`: O estudo não contém, em seu resumo ou título, relação com o objetivo de pesquisa.

4) String de Busca: A *string* de busca utilizada nesta RSL foi elaborada de forma a abranger os conceitos centrais da pesquisa, permitindo a identificação de estudos relacionados ao uso de dispositivos móveis e mensagens instantâneas como vetores para ataques de *phishing*, com foco no *smishing*. Termos em português e inglês foram incluídos para ampliar a cobertura, e sendo considerada também a diversidade de terminologias utilizadas na literatura acadêmica sobre o tópico. Além disso, a combinação de palavras-chave que associam dispositivos móveis, serviços de mensagens instantâneas e técnicas de *phishing* busca assegurar a coleta de dados compatíveis com os objetivos de mapear características, analisar vulnerabilidades e, assim, categorizar essas práticas criminosas.

Considerando o intuito de atender aos objetivos deste trabalho e as observações citadas, a *string* de busca utilizada foi:

(“Dispositivos móveis” OR “Cellphones” OR “Celulares” OR “Dispositivos pessoais” OR “Dispositivos portáteis” OR “Mobile devices” OR “Mobile phones” OR “Smartphones” OR “Tablets” OR “Telefones móveis”) AND (“Mensagens instantâneas” OR “Facebook Messenger” OR “Mensagens de texto instantâneas” OR “SMS” OR “Signal” OR “Telegram” OR “Viber” OR “WeChat” OR ”Whatsapp” OR “iMessage” OR “Instant Messaging”) AND (“Phishing” OR “Ataques de engenharia social” OR “Fraudes eletrônicas” OR “Scam” OR “Smishing” OR “Social Engineering Attacks” OR “Spear Phishing”)

5) Bases de Dados: A definição das bases de dados a serem utilizadas nesta pesquisa foi realizada com base em trabalhos prévios sobre o tema e outras RSLs diversas, permitindo identificar as bases recorrentes em outros estudos acadêmicos semelhantes [2], [4]. Portanto, as bases de dados utilizadas foram: ACM Digital Library, EI Compedex, IEEE Digital Library, ISI Web of Science, Science Direct, Scopus, Sol SBC e Springer Link.

6) Processo de Seleção de Estudos: Inicialmente, foram identificados 10.891 estudos a partir da busca realizada nas bases de dados. A quantidade de resultados retornados e selecionados será apresentada a seguir, na Tabela I. Durante a etapa de identificação, foram removidos 405 estudos duplicados, 32 que apresentavam ausência de resumo ou metadados e 8.044 que não eram artigos primários, resultando em um total de 2.410 estudos triados para a etapa seguinte.

TABELA I
QUANTIDADE DE RESULTADOS RETORNADOS POR BASE DE DADOS E ESTUDOS SELECIONADOS.

Base	Resultados	Estudos Selecionados
ACM Digital Library	836	4
EI Compendex	32	1
IEEE Digital Library	48	0
ISI Web of Science	28	1
Science Direct	811	2
Scopus	1.854	4
Sol SBC	0	0
Springer Link	7.282	0
Total	**10.891**	**12**

O processo de seleção dos estudos seguiu uma análise em duas etapas, conduzida por dois revisores independentes, que avaliaram a elegibilidade dos trabalhos com base na presença das palavras-chave nos títulos e resumos. Nos casos onde houve discordância, um terceiro revisor foi consultado para garantir consenso e minimizar possíveis vieses.

Na fase de triagem, foram excluídos 2.355 estudos que não estavam direcionados a ataques de *phishing* realizados por meio de mensagens instantâneas e 41 estudos que tratavam exclusivamente de métodos de detecção técnica, alinhando-se aos critérios de exclusão estabelecidos. Dessa forma, 14 estudos foram considerados elegíveis para a etapa seguinte.

Por fim, durante a avaliação de elegibilidade, dois estudos foram excluídos por não estarem disponíveis integralmente, enquanto nenhum estudo adicional foi desqualificado nessa etapa. Assim, um total de 12 estudos foram incluídos na revisão, fornecendo uma base consolidada para a análise dos ataques de *smishing*. O processo de seleção de estudos está representado na Figura 1 abaixo.

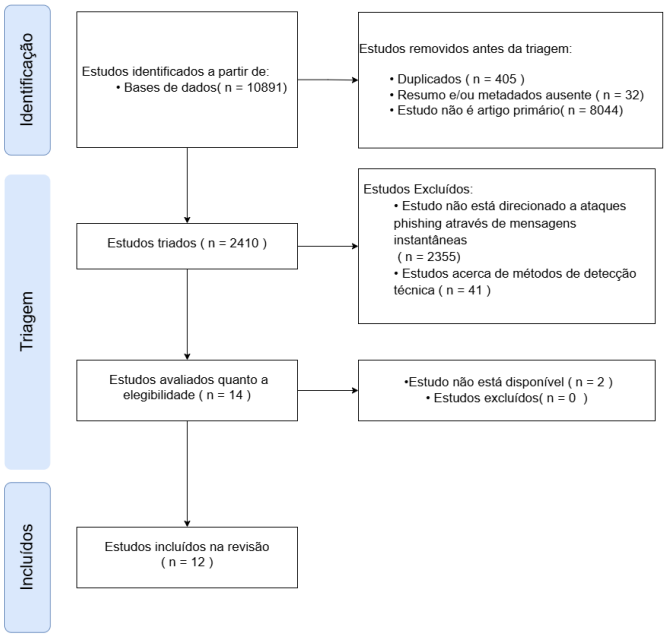

Fig. 1. Identificação de estudos através de bases de dados.

V. RESULTADOS

Os resultados obtidos exploram as técnicas e estratégias utilizadas por criminosos em ataques de *smishing*. Foram identificados, na análise dos estudos, fatores que aumentam a vulnerabilidade dos usuários. Além disso, também foi possível visualizar o panorama da pesquisa acadêmica sobre o tema. Os 12 estudos selecionados resultaram na identificação de alguns padrões de ataque, como o uso de URLs maliciosas, *spoofing* de identidade e exploração de contextos situacionais. Fatores como percepção de riscos, emoções e diferenças individuais foram

apontados como elementos que influenciam a suscetibilidade das vítimas a esses ataques.

A. *Respondendo à QP1*

Os estudos selecionados possibilitaram a identificação de diversas estratégias utilizadas por criminosos. Foi realizada uma caracterização de cada uma delas, com o objetivo de identificar elementos que evidenciem a abordagem de engenharia social e o meio empregado no ataque.

Uso de URLs maliciosas e encurtadas: A inclusão de *links* maliciosos em mensagens é uma técnica amplamente utilizada pelos atacantes, conforme identificado por Nakano et al. [35] em uma análise de relatos divulgados em redes sociais. O estudo de Chhabra et al. [36] também explora essa estratégia de ataque a partir de relatos publicados em redes sociais. Esses *links* são frequentemente encurtados para dificultar a identificação por parte dos usuários ou até mesmo embutidos em imagens, no caso de plataformas de mensagens instantâneas que permitem o envio desse tipo de conteúdo, como também foi observado por Lee et al. [37]. No estudo de Soykan et al. [38], é destacado que essa abordagem, não permite a extração de informações claras sobre o remetente, mas estimula a curiosidade dos usuários e assim os levando a acessarem o *link* malicioso.

***Spoofing* e falsificação de identidade**: Os criminosos frequentemente mascaram suas identidades, tornando-as semelhantes a remetentes confiáveis, como bancos e seguradoras. Haizam et al. [8] identificou que o uso dessa estratégia é altamente eficaz para aumentar a taxa de sucesso dos golpes. Nesse contexto, também é possível observar a exploração de relações sociais, em que os criminosos falsificam suas identidades e se passam por contatos conhecidos das vítimas. Essa abordagem explora a confiança social e reduz a percepção de risco. A eficácia dessa estratégia em plataformas de mensagens instantâneas foi evidenciada por Klütsch et al. [39].

O estudo de Liu et al. [21] lista algumas estratégias usadas por criminosos para aumentar suas taxas de sucesso, sendo identificadas: envios de testes prévios para checar se as mensagens vão efetivamente chegar aos usuários, a construção de narrativas através de múltiplas interações com a vítima, a variação no conteúdo das mensagens para confundir sistemas de detecção de *phishing*, além do uso de temas noticiados no contexto do usuário para persuadi-lo. A pesquisa ainda traz dados sobre a eficácia de ataques em que a vítima recebe mensagens contendo informações pessoais. Essa personalização reflete no aumento da taxa de sucesso do ataque.

Além dessas estratégias, os estudos também evidenciam a preocupação de acadêmicos com a adaptação a contextos específicos. Soykan et al. [40] destaca uma preocupação emergente associada aos Sistemas de Resposta a Demandas, que permitem aos consumidores ajustarem voluntariamente seu consumo em resposta a incentivos econômicos ou à sinalização da rede elétrica, ajudando a equilibrar oferta e demanda. No entanto, apesar da natureza positiva desse sistema, a comunicação com populações inteiras tem sido explorada por criminosos. Ao persuadir os usuários de que estão recebendo uma notificação legítima, esses atacantes os expõem ao risco de ataques de *smishing*. Esse cenário levanta um alerta quanto ao impacto potencial dessas ações, incluindo interrupções em redes críticas e o envio de alertas falsos a usuários em massa.

B. *Respondendo à QP2*

A nuvem de palavras exposta na Figura 2, gerada a partir das palavras-chave extraídas dos estudos analisados, fornece uma visão clara dos temas mais recorrentes na literatura sobre *smishing*. Nota-se o destaque do termo *phishing*, corroborando estudos que apontam para a escassez de referências acadêmicas relacionadas a abordagens específicas ao ataque através de mensagens instantâneas. Outros focos predominantes incluem cibersegurança, ataques, prevenção e alguns dos canais de *smishing*, como *WhatsApp*. A nuvem também oferece pistas sobre lacunas temáticas, sugerindo áreas que ainda não receberam a devida atenção acadêmica.

Fig. 2. Nuvem de palavras extraídas das palavras-chave.

O gráfico de estudos por país exposto na Figura 3, ilustra a distribuição geográfica das publicações, revelando as regiões que concentram maior interesse no estudo de ataques de *smishing*. Países como Índia e Malásia destacam-se como centros de produção acadêmica. A partir dessa análise, é possível observar uma predominância de estudos no sudeste asiático. O Brasil não figura nessa lista, demonstrando uma oportunidade para futuros trabalhos.

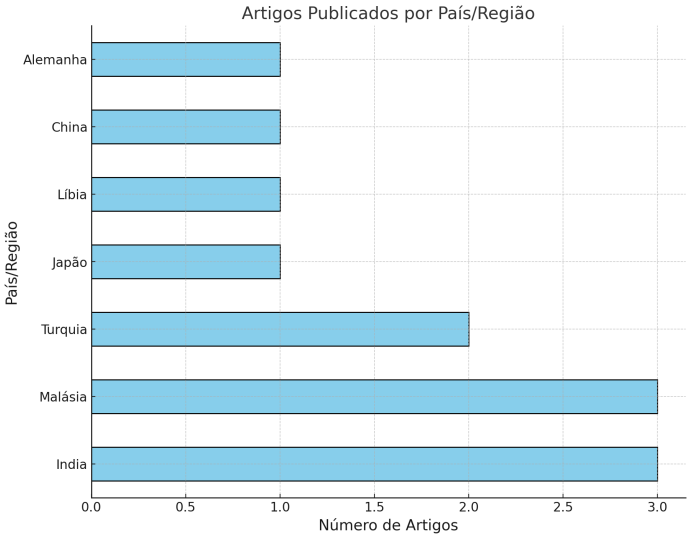

Fig. 3. Estudos distribuídos por país.

O número de estudos sobre *smishing* cresceu entre 2020 e 2024 (Figura 4), impulsionado pelo maior uso de dispositivos móveis e pela sofisticação dos ataques. Esse interesse intensificou-se a partir do pico da pandemia de Covid-19, período com aumento significativo na incidência de golpes. [41].

É importante ressaltar, como já identificado por Naqvi et al. [31], a existência de uma lacuna significativa em estudos voltados ao fator humano no contexto dos ataques de *phishing*, tendo sido identificados apenas seis estudos que tratavam especificamente de *smishing*.

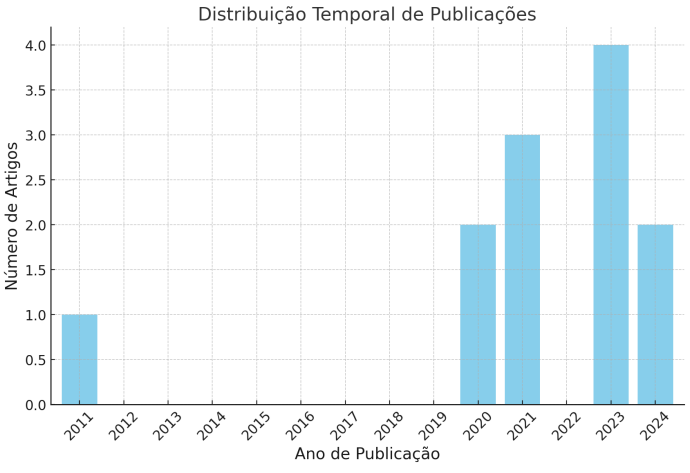

Fig. 4. Estudos distribuídos por ano de publicação.

Após a análise de cada estudo, foram mapeados seus interesses, e suas múltiplas inclinações. Assim, a Tabela II foi construída para uma visualização mais clara do resultado dessa análise, mapeando os seguintes interesses: aprimorar estratégias de detecção de *phishing* automáticas, mapear características de ataques de *phishing* através de mensagens instantâneas, propor estratégias de mitigação direcionadas ao fator humano, categorizar estratégias de ataque, identificar ameaças emergentes e trazer elementos históricos da evolução de ataques de *phishing* através de mensagens instantâneas.

Apenas três estudos [37], [39], [42] têm um olhar voltado para o fator humano nesse tipo de ataque, o que demonstra uma grande lacuna, dado que o ser humano é identificado como o elo mais frágil dessa relação. Outro interesse negligenciado é a identificação de elementos históricos que marcam a evolução dessa ameaça, o que é parte essencial do processo de desenvolvimento de estratégias de mitigação.

TABELA II
TABELA DE ESTUDOS CLASSIFICADOS POR INTERESSE EXPLORADO.

Estudo	I1	I2	I3	I4	I5	I6
[43]	X					
[21]	X	X		X		
[36]				X		
[44]					X	
[40]	X					
[39]			X	X		X
[42]		X	X			X
[37]		X	X			
[38]				X	X	
[41]		X		X	X	X
[8]	X	X		X	X	X
[35]					X	X

I1: Aprimorar estratégias de detecção de phishing automáticos.
I2: Mapear características de ataque phishing através de mensagens instantâneas.
I3: Propor estratégias de mitigação direcionadas ao fator humano.
I4: Categorizar estratégias de ataque.
I5: Identificar ameaças emergentes.
I6: Trazer elementos históricos da evolução de ataque phishing. através de mensagens instantâneas.

C. Respondendo à QP3

Percepção de risco: Klütsch et al. [39] demonstraram que a noção de risco é frequentemente reduzida quando as mensagens provêm de remetentes conhecidos ou aparentam ser de instituições confiáveis. Essa confiança reduz o nível de alerta das vítimas e prejudica sua análise crítica, aumentando a suscetibilidade a golpes. Além disso, a alta autoeficácia digital,

definida como a crença dos indivíduos na sua própria capacidade de realizar tarefas no ambiente digital, está associada à tendência de subestimar os riscos, tornando esses usuários mais vulneráveis a ataques sofisticados. Essa relação é corroborada por Lee et al. [37].

Outro fator agravante da suscetibilidade dos usuários a ataques é a exploração de emoções como urgência e medo, utilizadas para desencadear respostas impulsivas nos usuários. Mensagens que simulam emergências ou oferecem recompensas imediatas têm maior probabilidade de sucesso [42]. Além disso, o estudo de Klütsch et al. [39], realizado com uma amostra de jovens, identificou outra vulnerabilidade humana, associada ao medo de perder oportunidades. Esse comportamento aumenta a tendência desse grupo a ser vitimado por ataques [39].

Contexto situacional: Os estudos de Haizam et al. [8] e Soykan et al. [40] discutem os riscos do *smishing* em contextos nos quais os usuários esperam notificações legítimas relacionadas a emergências ou alertas críticos. Esses cenários evidenciam uma vulnerabilidade dos usuários, causada pela presunção de legitimidade das notificações recebidas. Outro contexto abordado no estudo de Lee et al. [42] associa notificações com promoções ou eventos populares ao aumento da eficácia dos ataques. Esse conjunto de evidências destaca uma abordagem de persuasão que explora a confiança dos usuários em notificações cujo remetente aparenta ser uma organização conhecida, com a qual já possuem alguma relação prévia.

Essa adaptação aos contextos também é observada por Shrilatha et al. [44], que, ao analisar o contexto indiano, identificaram uma relação entre o aumento de casos de *smishing* e o período da pandemia.

Diferenças individuais: Usuários com menor experiência digital demonstram maior suscetibilidade a ataques de *smishing*, devido à falta de familiaridade com práticas de segurança. Os estudos de Haizam et al. [8] e Lee et al. [37] afirmam que a literacia digital limitada está associada a maiores taxas de vulnerabilidade ao *smishing*. O estudo de Lee et al. [42] também aponta uma diferença na taxa de sucesso dos ataques entre alvos masculinos e femininos, com uma predominância de sucesso em mulheres. No entanto, o estudo ressalta limitações significativas relacionadas ao tamanho da amostra e a outros fatores demográficos dos participantes.

A Tabela III busca condensar algumas vulnerabilidades identificadas nos estudos analisados nesta revisão sistemática.

TABELA III
CARACTERÍSTICAS QUE AUMENTAM A VULNERABILIDADE.

Estudo	Características que Aumentam a Vulnerabilidade
[35]	Abuso de SMS para notificações legítimas; abuso de SMS para autenticação em dois fatores.
[43]	Falta de conhecimento sobre cibersegurança.
[21]	Vazamento de informações pessoais; URLs em mensagens; uso de SMS por instituições financeiras; uso de plataformas de envio de SMS em massa de baixo custo; envio de mensagens teste para *spear phishing* para mapear vítimas; ataques baseados no engano progressivo dos usuários.
[44]	Acesso à internet através de smartphones durante muitas horas do dia.
[40]	Uso de SMS por usuários para serviços.
[39]	Ansiedade explorada a partir de engenharia social.
[37]	Ataques direcionados a jovens adultos universitários, identificados como vulneráveis no contexto da pesquisa (Malásia).
[38]	Uso de SMS para notificações legítimas.
[41]	Vazamento de informações pessoais.
[8]	Uso de provedores de SMS em massa; ferramentas para mascarar a identidade do atacante, identificando-o como uma entidade ou organização confiável; uso de URLs curtas; construção de páginas com o uso de *phishing kits* que se assemelham a páginas oficiais de marcas conhecidas.

Os fatores humanos relatados como influentes na suscetibilidade a ataques de *smishing* incluem a confiança social explorada por meio da falsificação de identidade [8], [39], a curiosidade despertada por URLs maliciosas e encurtadas [38] e a personalização das mensagens, que aumenta a credibilidade dos ataques [21]. Além disso, a falta de educação em segurança digital dos usuários e a utilização de narrativas persuasivas adaptadas ao contexto das vítimas são elementos frequentemente explorados [21]. Para reduzir essas vulnerabilidades, os estudos sugerem iniciativas de educação digital, o aprimoramento dos sistemas de detecção baseados em métodos computacionais e campanhas que aumentem a conscientização sobre as técnicas empregadas pelos atacantes e os riscos [37], [40].

VI. CONCLUSÃO

Este estudo buscou analisar as características dos ataques de *smishing*, com foco nas estratégias utilizadas por cibercriminosos e nas vulnerabilidades exploradas no contexto de dispositivos móveis. A partir da revisão sistemática realizada, foi possível observar que algumas das práticas mais recorrentes incluem o uso de URLs encurtadas, falsificação de identidade e exploração de emoções humanas, como urgência e medo. Essas estratégias mostram um alto grau de adaptação dos criminosos às plataformas de mensagens instantâneas, como *WhatsApp*, *Telegram* e, principalmente, ao tradicional *SMS*, refletindo a necessidade de os usuários estarem constantemente atentos às mensagens fraudulentas.

Enquanto os trabalhos relacionados destacam estratégias computacionais para identificação de tais mensagens, este tra-

balho concentra-se nas nuances das abordagens de engenharia social associadas ao *smishing*, mapeando algumas das técnicas adaptadas ao contexto das mensagens instantâneas e os fatores humanos explorados nesse tipo de ataque, já observados pela comunidade acadêmica, particularidade essa que evidenciou que, uma vez que a barreira tecnológica tenha sido ultrapassada, os cibercriminosos exploram comportamentos sociais e contextos situacionais de maneira direcionada. Isso demanda abordagens preventivas mais abrangentes, que podem integrar educação digital e tecnologia.

Foram identificados fatores geográficos e temporais nos temas abordados pelos estudos selecionados e como em diferentes regiões existe uma disparidade no interesse sobre o tema, evidenciada pela concentração de publicações em países localizados no sudeste asiático. A análise também aponta um aumento no número de estudos sobre o tema nos últimos quatro anos, mas ainda insuficiente na investigação dessa modalidade de *phishing* e suas particularidades.

Além disso, este trabalho destaca que o *smishing* vai além do envio de mensagens fraudulentas via *SMS*, estendendo-se a plataformas diversificadas e explorando dinâmicas de comportamento dos usuários. A análise realizada evidencia que os ataques têm se tornado mais sofisticados, explorando não apenas vulnerabilidades tecnológicas, mas também emocionais e contextuais, se aproveitando da relação próxima que os usuários têm com seus dispositivos móveis para aumentar suas taxas de sucesso nos ataques. o que reforça a importância de um enfoque interdisciplinar na busca por soluções eficazes contra essa ameaça.

No entanto, a escassez de estudos específicos sobre *smishing*, em comparação com outras modalidades de *phishing*, dificulta a categorização completa das estratégias de ataque e expõe uma lacuna significativa na literatura acadêmica. Esse cenário reforça a necessidade de esforços futuros voltados para a ampliação do conhecimento sobre o tema e a ausência de dados mais amplos também apresenta desafios para o desenvolvimento de contramedidas direcionadas e eficazes.

Com base na revisão sistemática de literatura realizada, destaca-se a importância de integrar medidas tecnológicas com estratégias educacionais que promovam a conscientização digital dos usuários. Essa abordagem complementar pode ser determinante para mitigar os riscos associados ao *smishing*. O início de um mapeamento das características do *smishing*, apresentado neste trabalho, pode servir como um ponto de partida para estudos que busquem desenvolver diretrizes práticas de enfrentamento a esses ataques.

Considerando a ausência de estudos de origem brasileira, surgem oportunidades no contexto nacional para analisar o impacto da alfabetização digital no Brasil, investigar a eficácia da LGPD [45] na proteção contra ataques de *smishing* e avaliar o papel de campanhas públicas de conscientização digital voltadas a populações vulneráveis. Além disso, pesquisas de setor no contexto brasileiro, como no setor bancário e de serviços públicos, e o desenvolvimento de ferramentas específicas de detecção e mitigação de *smishing* podem oferecer conhecimento prático para fortalecer a segurança digital no país.

Referências

[1] G. Varshney, R. Kumawat, V. Varadharajan, U. Tupakula, and C. Gupta, "Anti-phishing: A comprehensive perspective," *Expert Systems with Applications*, vol. 238, p. 122199, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095741742302701X

[2] S. Zieliński, "Evolving threats, emerging laws: Poland's 2023 answer to the smishing challenge," *Computer Law and Security Review*, vol. 54, p. 106013, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364924000803

[3] APWG, "Phishing activity trends report: 1st quarter 2024," https://apwg.org/reports/apwg-phishing-activity-trends-report-q1-2024/, 2024, relatório sobre as tendências de atividades de phishing no primeiro trimestre de 2024.

[4] R. Goenka, M. Chawla, and N. Tiwari, "A comprehensive survey of phishing: mediums, intended targets, attack and defence techniques and a novel taxonomy," *International Journal of Information Security*, vol. 23, pp. 1–30, 10 2023.

[5] M. Jakobsson and S. Myers, *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken, NJ, USA: Wiley, 2006.

[6] 3GPP, "Serviço de mensagens curtas (sms)," https://www.3gpp.org, 2025, tecnologia de comunicação móvel utilizada para envio de mensagens de texto.

[7] WhatsApp Inc., "Whatsapp messenger," https://www.whatsapp.com, 2025, aplicativo de mensagens instantâneas.

[8] M. N. B. Haizam and N. H. binti Nik Zulkipli, "Analysing the impact of smishing attack in public announcement system on mobile phone," *Procedia Computer Science*, vol. 245, pp. 1165–1174, 2024, 9th International Conference on Computer Science and Computational Intelligence 2024 (ICCSCI 2024). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050924031545

[9] APWG, "Phishing activity trends report 4th quarter 2021," apwg.org, 2021.

[10] ——, "Phishing activity trends report: 1st quarter 2022," https://apwg.org/reports/apwg-phishing-activity-trends-report-q1-2022/, 2022, relatório sobre as tendências de atividades de phishing no primeiro trimestre de 2022.

[11] O. N. Akande, O. Gbenle, O. C. Abikoye, R. G. Jimoh, H. B. Akande, A. O. Balogun, and A. Fatokun, "Smsprotect: An automatic smishing detection mobile application," *ICT Express*, vol. 9, no. 2, pp. 168–176, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959522000868

[12] CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, *Cartilha de Segurança para Internet*, 2023, disponível em: https://cartilha.cert.br. Acesso em: 28 nov. 2024.

[13] "Lei geral de proteção de dados pessoais (lgpd), lei nº 13.709/2018," https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, 2018.

[14] J. Penêdo, *A fraude no campo da informação: Engenharia Social, Big Data e a manipulação do usuário na rede*. Belo Horizonte: Bibliotecas Universitárias, 2017.

[15] V. Sushruth, K. Rahul, and B. R. Chandavarkar, "Social engineering attacks during the covid-19 pandemic," *SN Computer Science*, 2021.

[16] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, p. 168, 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/10/168

[17] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019. [Online]. Available: https://doi.org/10.3390/fi11040089

[18] N. Conteh and P. Schmick, "Human hacking: Social engineering in the information age," *Journal of Cybersecurity*, 2020.

[19] I. Ghafir, V. Prenosil, and A. Ben Youcef, "Social engineering: A mechanism to breach security in cyberspace," *Journal of Computer Security*, 2020.

[20] R. Hoheisel, G. van Capelleveen, D. K. Sarmah, and M. Junger, "The development of phishing during the covid-19 pandemic: An analysis of over 1100 targeted domains," *Computers and Security*, vol. 128, p. 103158, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823000688

[21] M. Liu, Z. Yiming, B. Liu, Z. Li, H. Duan, and D. Sun, "Detecting and characterizing sms spearphishing attacks," in *Proceedings of the 37th Annual Computer Security Applications Conference*, 12 2021, pp. 930–943.

[22] B. Amro, "Phishing techniques in mobile devices," *Journal of Computer and Communications*, vol. 6, pp. 27–35, 2018. [Online]. Available: https://doi.org/10.4236/jcc.2018.62003

[23] W. Martins Junior, "Segurança cibernética e seus paradigmas na era digital," *RCMOS – Revista Científica Multidisciplinar O Saber*, 2023.

[24] K. Mitnick, *A arte de enganar*. São Paulo: Pearson Education, 2003.

[25] D. N. Pande and P. S. Voditel, "Spear phishing: Diagnosing attack paradigm," in *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017, pp. 2720–2724.

[26] A. Aleroud and L. Zhou, *Phishing environments, techniques, and countermeasures: A survey*. Elsevier, 2017, vol. 68.

[27] OpenVault, "Broadband insights report (ovbi)," https://openvault.com/wp-content/uploads/2022/03/OVBI_4Q21_Report_FINAL-1.pdf, 2021, relatório Analítico sobre Banda Larga.

[28] S. I. Hashmi, N. George, E. Saqib, F. Ali, N. Siddique, S. Kashif, S. Ali, N. U. H. Bajwa, and M. Javed, "Training users to recognize persuasion techniques in vishing calls," in *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI EA '23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi-org.ez49.periodicos.capes.gov.br/10.1145/3544549.3585823

[29] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Phishing with malicious qr codes," in *Proceedings of the 2022 European Symposium on Usable Security*, ser. EuroUSEC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 160–171. [Online]. Available: https://doi-org.ez49.periodicos.capes.gov.br/10.1145/3549015.3554172

[30] T. Xu, K. Singh, and P. Rajivan, "Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks," *Applied Ergonomics*, vol. 108, p. 103908, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0003687022002319

[31] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers and Security*, vol. 132, p. 103387, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823002973

[32] A. P. Siddaway, A. M. Wood, and L. V. Hedges, "How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses," *Annual Review of Psychology*, vol. 70, pp. 747–770, 2019.

[33] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, "The prisma 2020 statement: An updated guideline for reporting systematic reviews," *Journal of Clinical Epidemiology*, 2021.

[34] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research," *MethodsX*, vol. 9, p. 101895, 2022.

[35] H. Nakano, D. Chiba, T. Koide, N. Fukushi, T. Yagi, T. Hariu, K. Yoshioka, and T. Matsumoto, "Canary in twitter mine: Collecting phishing reports from experts and non-experts," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ser. ARES '23. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi-org.ez49.periodicos.capes.gov.br/10.1145/3600160.3600163

[36] S. Chhabra, A. Aggarwal, F. Benevenuto, and P. Kumaraguru, "Phi.sh/social: the phishing landscape through short urls," in *Proceedings of the 8th Annual Collaboration, Electronic Messaging, Anti-Abuse and Spam Conference*, ser. CEAS '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 92–101. [Online]. Available: https://doi-org.ez49.periodicos.capes.gov.br/10.1145/2030376.2030387

[37] Y. Y. Lee, C. Gan, and T. W. Liew, "Thwarting instant messaging phishing attacks: The role of self-efficacy and the mediating effect of attitude towards online sharing of personal information," *International Journal of Environmental Research and Public Health*, vol. 20, p. 3514, 02 2023.

[38] E. U. Soykan, M. Bagriyanik, and G. Soykan, "Disrupting the power grid via ev charging: The impact of the sms phishing attacks," *SUSTAINABLE ENERGY GRIDS and NETWORKS*, vol. 26, JUN 2021.

[39] J. Klütsch, J. Schwab, C. Böffel, V. Zimmermann, and S. Schlittmeier, "Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media," *Humanities and Social Sciences Communications*, vol. 11, 09 2024.

[40] E. U. Soykan and M. Bagriyanik, "The effect of smishing attack on security of demand response programs," *ENERGIES*, vol. 13, no. 17, SEP 2020.

[41] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, and S. Arthi, "Why is phishing still successful?" *Computer Fraud and Security*, vol. 2020, no. 9, pp. 15–19, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372320300981

[42] Y. Y. Lee, C. Gan, and T. W. Liew, "Susceptibility to instant messaging phishing attacks: does systematic information processing differ between genders?" *Crime Prevention and Community Safety*, vol. 25, pp. 1–25, 04 2023.

[43] Y. A. Younis and M. Musbah, "A framework to protect against phishing attacks," in *Proceedings of the 6th International Conference on Engineering and MIS 2020*, ser. ICEMIS'20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi-org.ez49.periodicos.capes.gov.br/10.1145/3410352.3410825

[44] S. Shrilatha, K. Aruna, and H. Christinal, "The role of social media apps and its cyber attacks in india," in *"title": "Proceedings of the Workshop on Computer Networks and Communications (WCNC 2022)"*,, vol. 3244, Virtual, Online, India, 2022, pp. 59 – 65, cOVID;Creative Commons;Cyber criminals;Cyber-attacks;Lockdown;Multiple networks;Single-networks;Smart phones;Social media;Whatsapp;.

[45] Presidência da República Federativa do Brasil, "Lei geral de proteção de dados pessoais (lgpd) — lei nº 13.709, de 14 de agosto de 2018," https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm, 2018, estabelece regras sobre o tratamento de dados pessoais no Brasil.