ENGENHARIA SOCIAL EM APLICATIVOS DE MENSAGENS: ANÁLISE DE TÉCNICAS, ELEMENTOS PSICOLÓGICOS E MECANISMOS DE DEFESA EM AMBIENTES DIGITAIS

SOCIAL ENGINEERING IN MESSAGING APPLICATIONS: ANALYSIS OF TECHNIQUES, PSYCHOLOGICAL ELEMENTS, AND DEFENSE MECHANISMS IN DIGITAL ENVIRONMENTS

Alice Prado e Silva [1], i
Eliane Portalone Crescenti [2], ii
Adriano de Souza Alvares[3], iii
Paulo José Rodolpho[4], iv
Luciene Cristina Chiari Déo [5], v

RESUMO

Este estudo tem como objetivo investigar como ataques de engenharia social são realizados em aplicativos de mensagens e propor medidas técnicas e comportamentais para aumentar a proteção dos usuários. A metodologia adotada é qualitativa e aplicada, estruturada em cinco etapas: pesquisa teórica, análise de casos reais, levantamento técnico dos aplicativos, simulações controladas e produção de material educativo. Os resultados parciais concentram-se na primeira etapa, pesquisa teórica, que define a engenharia social como a exploração de vulnerabilidades humanas e manipulação psicológica e a ciberpsicologia, campo que investiga os impactos da interação humana com a tecnologia e ferramenta para compreender o comportamento em ambientes digitais. Espera-se contribuir na elaboração de um conjunto de boas práticas e orientações de defesa digital e transformação do conhecimento obtido em ações preventivas para a educação digital e a redução de vulnerabilidades.

Palavras-chave: Engenharia social; Aplicativos de mensagens; Ambientes digitais; Ciberpsicologia; Defesa cibernética.

ABSTRACT

This study aims to investigate how social engineering attacks are carried out in messaging applications and propose technical and behavioral measures to increase user protection. The methodology adopted is qualitative and applied, structured in five stages: theoretical research, analysis of real cases, technical survey of applications, controlled simulations, and production of educational material. The partial results focus

[1] Graduanda em Análise e Desenvolvimento de Sistemas pela Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe. E-mail: alice.prados07@gmail.com.
[2] Doutora em Educação pela UFSCar e Professora da Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe. E-mail: eliane.crescenti@gmail.com.
[3] Doutor em Biotecnologia pela Universidade Federal de São Carlos (UFSCar) e Professor da Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe. E-mail: aalvares@sp.senai.br.
[4] Mestre em Ciências pela Universidade de São Paulo (USP) e Professor da Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe. E-mail: paulo.rodolpho@sp.senai.br
[5] Docente, Dra em Engenharia de Materiais, da Faculdade SENAI de Tecnologia Mecatrônica. E-mail: lucienedeo@gmail.com.

on the first stage, theoretical research, which defines social engineering as the exploitation of human vulnerabilities and psychological manipulation, and cyberpsychology, a field that investigates the impacts of human interaction with technology and a tool for understanding behavior in digital environments. It is hoped that this will contribute to the development of a set of best practices and guidelines for digital defense and the transformation of knowledge gained into preventive actions for digital education and the reduction of vulnerabilities.

Keywords: Social Engineering; Messaging Applications; Digital Environments; Cyberpsychology; Cyber Defense.

1 INTRODUÇÃO

No cenário digital contemporâneo, os aplicativos de mensagens instantâneas tornaram-se ferramentas essenciais de comunicação, tanto no âmbito pessoal quanto profissional e a comunicação digital tornou-se uma ferramenta essencial no cotidiano informal e profissional pela facilidade do uso, conectividade, comunicação rápida, assíncrona e em tempo real. Mas, se tornaram alvos de cibercriminosos que utilizam engenharia social para manipular usuários e obter dados sensíveis. Torna-se, então, fundamental a compreensão dos mecanismos que se estabelecem por trás das interações online.

1.1 Problema de pesquisa

O problema de pesquisa configura-se na proposição de uma análise abrangente das principais estratégias de engenharia social aplicadas em aplicativos de mensagens com destaque para fatores cognitivos e emocionais envolvidos e discussão de mecanismos de defesa e práticas de conscientização que podem mitigar os riscos associados a essas ameaças.

1.2 Objetivo(s)

O objetivo geral consiste em investigar como os ataques de engenharia social são executados em aplicativos de mensagens. Outros objetivos se colocam: avaliar os mecanismos de segurança existentes nas plataformas; desenvolver simulações controladas para identificar vulnerabilidades; propor medidas técnicas e comportamentais por meio de guia de boas práticas para aumentar a proteção.

1.3 Justificativa

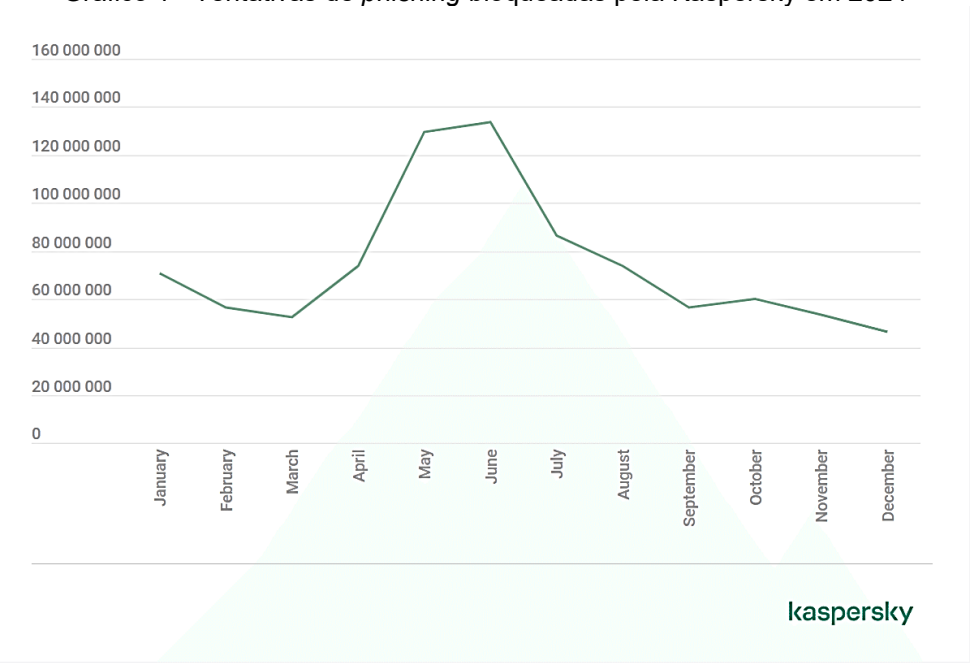
A escolha deste tema justifica-se pela crescente incidência de ataques que exploram vulnerabilidades humanas em plataformas digitais. A relevância social do estudo concentra-se na necessidade de proteger usuários expostos a fraudes e manipulações de dados sensíveis que comprometem sua segurança e privacidade. Nessa direção, o impacto prático desse estudo concentra-se em subsidiar estratégias mais eficazes de prevenção, conscientização e resposta a incidentes, uma vez que estudos sobre engenharia social se concentram em ambientes corporativos ou ataques por e-mail, o que reforça a importância de uma abordagem interdisciplinar que integre segurança digital, psicologia e comunicação.

2 REVISÃO DE LITERATURA

O referencial desse trabalho pauta-se em estudos e produções sobre ataques de cibercriminosos que se utilizam de técnicas de engenharia social e ciberpsicologia, área multidisciplinar na busca de compreender os hábitos, usos e abusos da tecnologia (SABATER, 2021). Esses ataques exploram falhas humanas por meio de táticas psicológicas sofisticadas que tornam as vítimas cúmplices involuntárias de crimes digitais. Dutra (2024), destaca que a gestão efetiva da segurança da informação está ligada ao fator humano, uma vez que criminosos, servindo-se da engenharia social, exploram a psicologia humana para obter acesso indevido a informações confidenciais com táticas como manipulação, persuasão e exploração da confiança. Brasil (2021) aponta que “instituições nacionais, públicas ou privadas são alvo constante de ações de engenharia social, método que busca acesso de forma dissimulada a informações sensíveis e não disponíveis” (p.5), bem como para a população.

Nos últimos anos, observa-se um crescimento expressivo das tentativas de golpes digitais baseados em *phishing*. Apenas em 2024, as soluções da Kaspersky registraram o bloqueio de mais de 893 milhões de tentativas desse tipo de ataque, um aumento de 26% em relação a 2023, que foram aproximadamente 710 milhões. Entre os meses de maio e julho, por exemplo, há uma intensificação das ações fraudulentas, comumente vinculada à temporada de férias e festas, período em que usuários são alvos de falsas ofertas de pacotes de viagem, hospedagens e promoções que parecem vantajosas demais (KASPERSKY, 2025).

Gráfico 1 - Tentativas de *phishing* bloqueadas pela Kaspersky em 2024



Fonte: Kaspersky (2025)

3 METODOLOGIA

A metodologia do estudo é de abordagem qualitativa e aplicada, dividida em cinco etapas principais: (1) pesquisa teórica e revisão bibliográfica sobre conceitos de engenharia social e ciberpsicologia, comportamento humano diante

de fraudes digitais, técnicas de golpes em aplicativos de mensagens e fundamentos de cibersegurança. (2) coleta e análise de casos reais de golpes como clonagem de contas e *phishing* para identificação de padrões comportamentais e linguísticos. (3) avaliação técnica dos aplicativos de mensagens para mapear suas funcionalidades de segurança, como autenticação em duas etapas e criptografia. (4) simulações controladas de ataques em um ambiente seguro para observar as reações dos usuários e identificar falhas de percepção ou comportamento. (5) criação de recomendações e materiais educativos, como um guia prático de defesa contra a engenharia social, com base nas análises realizadas.

O trabalho encontra-se na fase (1) pesquisa teórica e revisão bibliográfica sobre conceitos de engenharia social e ciberpsicologia, comportamento humano diante de fraudes digitais, técnicas de golpes em aplicativos de mensagens e fundamentos de cibersegurança. Para mapeamento da interseção entre engenharia social, ciberpsicologia, comportamento humano diante de fraudes digitais, técnicas de golpes em aplicativos de mensagens e fundamentos de cibersegurança, foram consultadas as bases Google Acadêmico, Scielo e Science Direct. Os descritores foram: engenharia social; ciberpsicologia; fraudes digitais; fundamentos da cibersegurança; engenharia social e ciberpsicologia; engenharia social e ciberpsicologia e fraude digital; engenharia social e ciberpsicologia e fundamentos da segurança; ciberpsicologia e frandes digitais e fundamentos da segurança; engenharia social e ciberpsicologia e fraude digital e fundamentos de cibersegurança, com operador lógico AND. Os critérios de inclusão foram artigos publicados em periódicos avaliados por pares. O período de busca foi de 2015 a 2025 e os idiomas considerados foram português, inglês e espanhol. Até o momento, foram identificados 61 estudos relevantes que dialogam com os objetivos do estudo e fornecem subsídios teóricos e práticos para a etapa seguinte.

4 RESULTADOS E DISCUSSÕES

Os resultados deste estudo configuram-se até o momento como parciais, concentrando-se na primeira etapa: pesquisa teórica e revisão bibliográfica sobre conceitos de engenharia social e ciberpsicologia, comportamento humano diante de fraudes digitais, técnicas de golpes em aplicativos de mensagens e fundamentos de cibersegurança. Foram encontrados 61 artigos, sendo 12 no idioma português, 41 em inglês e 8 em espanhol.

Os artigos trouxeram informações teóricas, técnicas e práticas. Os que tratam sobre engenharia social tratam sobre abordagem de *phishing*, impactos da engenharia social na segurança da informação, engenharia social em segurança cibernética, ataques avançados de engenharia social, mecanismos de efeito, vulnerabilidades humanas e métodos de ataque. A engenharia social distingue-se dos ataques técnicos por atuar diretamente sobre a psicologia humana com foco na prestatividade, ausência de conhecimento sobre segurança e medo, conforme discutem os trabalhos de Wang (2020, 2021). Além disso, com o avanço das tecnologias digitais e a disponibilidade online de dados sensíveis, mais facilmente se consegue mapear o comportamento das pessoas (PEREIRA, 2022).

Os artigos sobre cibersegurança abordam sobre intersecção entre o uso da tecnologia computacional e o comportamento humano, fatores humanos no *phishing*, suscetibilidade e resiliência, golpes de *phishing* nas redes sociais, avaliação do impacto e da eficácia da educação cibernética. Nessa direção, a ciberpsicologia, campo interdisciplinar emergente, estuda como a interação com tecnologias digitais

afeta o comportamento humano. Torres e Fernandes (2024) e Santos, Donard e Torres (2025) destacam a relevância dessa área no cenário atual caracterizado por relações mediadas por dispositivos digitais. Sabater (2021) destaca a sua importância em uma sociedade hiperconcetada, enquanto Ancis (2020) aponta para os novos transtornos psicológicos e crimes associados ao uso inadequado da tecnologia.

Os artigos sobre fraudes digitais fazem referência aos crimes cibernéticos e trazem questões como *phishing* que vão ao encontro que Pinto (2025) e Khadka (2024) trazem sobre a importância do conhecimento a respeito de sobre *phishing*, vulnerabilidade social de idosos frente a golpes no âmbito digital, golpes e crimes no aplicativo de mensagens WhatsApp, detecção de golpes e fatores humanos no *phishing*. A literatura traz também outros tipos de fraudes como roubo de identidade, clonagem de cartões, fraudes bancárias, entre outros. Essas fraudes iniciam-se, frequentemente, com técnicas de engenharia social, o que reforça a necessidade de educação digital e conscientização sobre segurança, uma vez que, segundo Siddiqi, Pak e Siddiqi (2022), ataques cibernéticos baseados em engenharia social são extremamente difíceis de combater, pois não seguem padrões ou abordagens específicas para a condução de um ataque, o que os torna abordagens altamente eficazes, eficientes, fáceis e obscuras para comprometer qualquer organização.

Os artigos sobre fundamentos da cibersegurança trazem questões como a cibersegurança envolve mais do que apenas segurança de sistemas, envolve aspectos legais, humanos, sociais e políticos; público-alvo dos golpes: infanto juvenil e idosos em virtude da falta de habilidade, inocência e falta de conhecimento; trazem também cuidados com a área de finança. Assim, os fundamentos da cibersegurança tornam-se essenciais, pois incluem princípios como confidencialidade, integridade, disponibilidade, autenticidade e responsabilidade, como colocam Mail (2025), Pinto (2025), Santos (2024), Palma et. al. (2024).

A integração de aspectos técnicos da segurança da informação com os fatores psicológicos estudados pela ciberpsicologia, bem como a compreensão das fraudes digitais, permite uma abordagem mais completa e eficaz para o enfrentamento de riscos no ambiente digital.

5 CONCLUSÃO

Diante da crescente sofisticação dos ataques de engenharia social em aplicativos de mensagens, este estudo evidencia a urgência de compreender aspectos técnicos de segurança digital, bem como fatores emocionais e cognitivos que tornam s usuários mais vulneráveis aos ataques.

Os estudos encontrados possibilitaram identificar que o cibercriminosos exploram falhas humanas por meio de táticas psicológicas como manipulação da confiança, do medo e da prestatividade. Também, mostrou que a interseção entre engenharia social, ciberpsicologia e fraudes digitais forma um campo interdisciplinar promissor e necessário para a construção de estratégias mais eficazes de prevenção.

Os resultados parciais deste trabalho reforçam que a segurança digital não deve se limitar à implementação de tecnologias, mas precisa considerar o comportamento humano como elemento central. Aponta para a importância de ações educativas e de conscientização voltadas para públicos mais vulneráveis, como idosos e jovens, bem como a necessidade de medidas técnicas e comportamentais que envolvam os próprios usuários na proteção de seus dados. A continuidade da pesquisa, com simulações práticas e proposição de boas práticas, contribuirá para o

desenvolvimento de um guia eficaz de enfrentamento à engenharia social e promoção de uso mais seguro e consciente das plataformas digitais de comunicação.

REFERÊNCIAS

ANCIS, J. R. A era da ciberpsicologia: uma visão geral. **Tecnologia, Mente e Comportamento**, v.1, n.1, 2020. Disponível em: https://doi.org/10.1037/tmb0000009. Acesso em: 05 ago. 2025.

BRASIL. Departamento de Contrainteligência. Programa Nacional de Proteção do Conhecimento Sensível (PNPC). **Engenharia social**: guia para proteção de conhecimentos sensíveis. 2021. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 10 ago. 2025.

DUTRA, J. **Engenharia social**: como identificar ameaças e proteger informações. 2. ed. Brasília: [s.n.], 2024. [e-book Kindle].

KHADKA, K. **Persuasion and *Phishing***: Analysing the Interplay of Persuasion Tactics in Cyber Threats. Faculty of Science and Technology, University of Canberra, 2024. DOI:10.48550/arXiv.2412.18485. Acesso em: 21 set. 2025.

KASPERSKY**. Kaspersky reports nearly 900 million phishing attempts in 2024 as cyber threats increase**. 2025. Disponível em: https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase. Acesso em: 21 set. 2025.

MAIL, R. **Fundamentos da cibersegurança**: entre firewalls e brechas: uma jornada pela cibersegurança. 2025. [eBook Kindle].

PALMA, L.; COSTA, F.; SABINO, A.; MARINHO, F.; SANTOS, T. **Cibersegurança**: o guia definitivo - um guia atemporal para a construção de uma carreira em cibersegurança. BARUERI, SP: Editora Hackone, 2024.

PEREIRA, L. A. de S.; VICENTINE, A. L.; RIZO, A. C. Impactos da engenharia social na segurança da informação. **RBTI - Revista Brasileira em Tecnologia da Informação**, Campinas, SP, v.4, n.1, p.1-58, jan./jun. 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/75. Acesso em: 08 ago. 2025.

PINTO, O. P. **Fundamentos de cibersegurança**: da teoria à prática: estratégias para defesa cibernética eficaz. 2025. [eBook Kindle].

SABATER, V. O que é a ciberpsicologia? **A mente é maravilhosa.** 2021. Disponível em: https://amenteemaravilhosa.com.br/ciberpsicologia/. Acesso em: 07 jul. 2025.

SANTOS, A. de A., DONARD, V., TORRES, M. de S. (Orgs.). **Ciberpsicologia e Humanidades Digitais**. São Paulo: Pimenta Cultural, 2025. DOI:

10.31560/pimentacultural/978-85-7221-286-1.

SANTOS, M. **Fundamentos e Práticas de Cibersegurança**: Abordagem Prática para Profissionais de Cibersegurança. 2024. [eBook Kindle].

SIDDIQI, M. A., PAK, W., & SIDDIQI, M. A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. **Applied Sciences**, v. 12, n. 12, art. 6042, 2022. DOI: 10.3390/app12126042. Acesso em: 21 set. 2025.

TORRES, M. de S.; FERNANDES, S. C. S. Ciberpsicologia: impactos no comportamento e saúde mental. In: SOCIEDADE BRASILEIRA DE PSICOLOGIA. 54. Reunião Anual, 2024, Curitiba. **Anais**... Curitiba, 22 a 25 out. 2024. p. 19. Disponível em: https://www.sbponline.org.br/arquivos/Anais_2024_-_Resumos_de_comunicação_científica_1.pdf. Acesso em: 07 jul. 2025.

WANG, Zuoguang; SUN, Limin; ZHU, Hongsong. Defining social engineering in cybersecurity. **IEEE Access**, v. 8, p. 85094-85115, 2020. DOI: 10.1109/ACCESS.2020.2992807. Disponível em: https://ieeexplore.ieee.org/document/9087851. Acesso em: 08 ago. 2025.

WANG, Zuoguang; ZHU, Hongsong; SUN, Limin. Social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods. **IEEE Access**, 2021. DOI: 10.1109/ACCESS.2021.3051633. Disponível em: https://ieeexplore.ieee.org/document/9323026. Acesso em: 08 ago. 2025.

AGRADECIMENTOS

À Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe pelo apoio ao desenvolvimento deste trabalho.

SOBRE O(S)AUTOR(ES)

[i] **ALICE PRADO E SILVA**

Graduanda do curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas na Faculdade SENAI Antonio Adolpho Lobbe. Técnica em Mecatrônica na mesma instituição. Possui experiência no desenvolvimento de projetos voltados às tecnologias atuais. CV: https://lattes.cnpq.br/3947099700882217. Orcid: https://orcid.org/0009-0005-3477-6792.

[ii] **ELIANE PORTALONE CRESCENTI**

Doutora em Educação pela UFSCar, Graduada em Pedagogia, possui licenciatura em Matemática e graduanda no curso de psicologia pela UNICEP. Professora da Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe. CV: http://lattes.cnpq.br/7287574807580165 Orcid: https://orcid.org/0000-0002-8572-8038

[iii] **ADRIANO DE SOUZA ALVARES**

Doutor em Biotecnologia na UFSCar, Graduado em Sistemas de Informação e Engenharia Elétrica pelo Centro Universitário Central Paulista – UNICEP. Professor da Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe. CV: http://lattes.cnpq.br/0734593128098221 Orcid: https://orcid.org/0009-0002-2375-3462

[iv] **PAULO JOSÉ RODOLPHO**

Graduado em Ciência da Computação, UNICEP (2001). Especialista em Formação Pedagógica para Educação Profissional pela UNIMEP (2004). Mestre em Ciências pelo PPGEM/EESC/USP (2013). Professor de Educação Superior na Faculdade de Tecnologia SENAI Antonio Adolpho Lobbe de São Carlos. CV: http://lattes.cnpq.br/3915529378619804 Orcid: https://orcid.org/0009-0008-3234-0620

[v] **LUCIENE CRISTINA CHIARI DÉO**

Doutora (2009) em Ciência e Engenharia de Materiais pelo PPGCEM/UFSCar. Atua como docente na Faculdade SENAI Antonio Adolpho Lobbe nas em áreas relacionadas à Tecnologia dos Materiais e Gestão. CV: http://lattes.cnpq.br/7728256316655962. Orcid: https://orcid.org/0009-0008-8802-239X.