

Engenharia social e phishing: proposta de um framework para análise dos impactos da exploração de vulnerabilidades humanas na segurança de dados pessoais sensíveis

Social engineering and phishing: a proposed framework for analyzing the impacts of exploiting human vulnerabilities on the security of sensitive personal data

Letícia Oliveira Corrêa – leticiaacor@gmail.com
Douglas Rodrigues – douglasrodrigues@unimar.br

INTRODUÇÃO

A crescente dependência das tecnologias digitais tem ampliado a exposição de indivíduos e organizações a ameaças cibernéticas. Entre essas ameaças, o phishing e as técnicas de engenharia social destacam-se por explorar vulnerabilidades humanas em vez de falhas exclusivamente tecnológicas. A manipulação psicológica de usuários representa um dos principais desafios para a segurança da informação, uma vez que pode comprometer sistemas mesmo quando mecanismos técnicos de proteção estão presentes. Este trabalho tem como objetivo investigar os impactos do phishing e da engenharia social sobre indivíduos e organizações, considerando aspectos técnicos, financeiros, sociais e psicológicos. Busca-se compreender os danos decorrentes dessas práticas e discutir estratégias de prevenção fundamentadas na educação digital e na conscientização em segurança da informação. A pesquisa adota abordagem qualitativa e exploratória, baseada em revisão bibliográfica e análise crítica da literatura especializada sobre phishing, engenharia social e segurança da informação, fundamentando-se em relatórios técnicos do setor, como os da APWG (2024) e de Kosinski (2024), e em análises especializadas sobre os mecanismos psicológicos da manipulação, como a de Andersen (2025). Os detalhes metodológicos e a construção do framework proposto serão apresentados na seção de Desenvolvimento. Espera-se evidenciar que os impactos do phishing e da engenharia social extrapolam o campo técnico, alcançando as dimensões financeira, social e psicológica, o que reforça a relevância de estratégias de prevenção fundamentadas na educação digital e na conscientização em segurança da informação.

DESENVOLVIMENTO

Com base na revisão bibliográfica e na análise crítica dos relatórios técnicos citados, propõe-se um framework original, composto por cinco categorias de impacto (técnica, financeira, social, psicológica e organizacional), que relaciona o tipo de dado exposto ao perfil da vítima e aos vetores comportamentais envolvidos, como os diferentes tipos de ataque descritos por Kosinski (2024). Os critérios de criticidade serão definidos com base na combinação de três dimensões: (a) extensão do dano, medida pelo volume de dados comprometidos ou pelo número de vítimas afetadas; (b) reversibilidade, considerando a possibilidade de recuperação dos ativos ou da reputação; e (c) impacto residual, avaliando consequências persistentes como sequelas psicológicas ou exposição prolongada de dados. A escala resultante (baixo, moderado, alto e crítico) permitirá cruzar indicadores quantitativos dos relatórios setoriais com o referencial teórico de engenharia social.

CONCLUSÃO

Ao final da pesquisa, o framework proposto deverá oferecer uma ferramenta sistemática para classificar e priorizar riscos associados à exploração do fator humano, reforçando que os impactos do phishing e da engenharia social extrapolam o prejuízo financeiro imediato e subsidiando ações de conscientização em segurança da informação. Como próximos passos, prevê-se a validação do framework a partir do cruzamento dos dados dos relatórios técnicos com o referencial teórico adotado, além da redação de um artigo científico para submissão a evento ou periódico da área.

REFERÊNCIAS

ANDERSEN, G. The psychology of social engineering. [S.l.]: Coalition, 2025. Disponível em: <https://www.coalitioninc.com/blog/security-labs/the-psychology-of-social-engineering>. Acesso em: 9 setembro 2026.

ANTI-PHISHING WORKING GROUP (APWG). Phishing activity trends report: 3rd quarter 2024. [S.l.]: APWG, 2024.

KOSINSKI, M. O que é phishing? [S.l.]: IBM, 2024. Disponível em: <https://www.ibm.com/br-pt/think/topics/phishing>. Acesso em: 10 setembro 2026.