Contrainteligência em Engenharia Social: Aprimorando a Defesa Cibernética da Sociedade

Demis D. Gomes[1], **Gustavo H. Motta**[1]

[1]Programa de Pós-Graduação em Informática
Centro de Informática
Universidade Federal da Paraíba (UFPB)
58.055-000 – João Pessoa – PB – Brazil.
demisgomes@ieee.org, gustavo@ci.ufpb.br

Abstract. *Social engineering represents a significant challenge for advancing information security, especially when considering the human factor in information systems. The literature describes a framework for how social engineering works that addresses mechanisms of action and human emotions. On the other hand, this work proposes a counterintelligence framework with the objective of neutralizing attacks or mitigating damage caused by social engineering. The research in question is ongoing and requires more robust validations to comprehensively provide the validated and properly tested framework, following established ethical and legal parameters.*

Resumo. *A engenharia social representa um desafio significativo para o avanço da segurança da informação, especialmente quando se considera o fator humano nos sistemas de informação. A literatura descreve um framework de funcionamento da engenharia social que aborda mecanismos de ação e emoções humanas. Por outro lado, este trabalho propõe um framework de contrainteligência com o objetivo de neutralizar ataques ou mitigar danos causados pela engenharia social. A pesquisa em questão está em andamento e necessita de validações mais robustas para fornecer de maneira abrangente o framework validado e devidamente testado, seguindo os parâmetros éticos e legais estabelecidos.*

1. Introdução

A engenharia social é um dos entraves para o avanço na segurança da informação quando se considera o fator humano em sistemas de informação. Tratar o problema da segurança da informação com ênfase em aspectos técnicos, em detrimento dos fatores humanos, abre o flanco para ataques de engenharia social nas organizações. Propõe-se neste trabalho um framework baseado no conceito de contrainteligência que visa mitigar os danos causados por ataques de engenharia social. O framework proposto parte da premissa de que atitudes comportamentais de natureza proativa e reativa, baseadas em conhecimento de contrainteligência desses ataques, são eficazes para redução de danos. Ele se contrapõe à inteligência presente em ataques de engenharia social, consolidada em um framework proposto por [Wang et al. 2021], que explica o funcionamento da engenharia social a partir da combinação, por atacantes, de efeitos de mecanismos externos e das vulnerabilidades humanas às técnicas de invasão para alcançar os fins desejados.

O restante deste trabalho está estruturado da seguinte maneira. A seção 2 apresenta a fundamentação teórica da pesquisa em andamento. A seção 3 traz o framework de contrainteligência proposto, incluindo as defesas ativas e passivas como meios para mitigar os danos causados por ataques de engenharia social. A seção 4 descreve a metodologia em curso na condução da pesquisa. Finalmente, na seção 5, discute-se as contribuições esperadas com os resultados deste trabalho, oferecendo uma visão abrangente do impacto da abordagem proposta.

2. Fundamentação Teórica

A engenharia social é uma forma de ataque que compreende a aplicação de técnicas que visam manipular e explorar a psicologia humana para obter informações, influenciar comportamentos ou obter acesso não autorizado a sistemas e recursos [Grbic and Dujlovic 2023]. Baseia-se na interação e manipulação das pessoas, ao invés de explorar diretamente vulnerabilidades técnicas [Eftimie et al. 2022].

Os engenheiros sociais, geralmente, atacam utilizando táticas de persuasão, manipulação emocional, intimidação ou engano para convencer pessoas a realizar ações específicas [Wang et al. 2021]. Essas ações podem incluir a divulgação de senhas, acesso a sistemas protegidos, revelação de informações pessoais ou corporativas sensíveis [Davis and Grant 2023]. Desse modo, pode-se ter como referência o uso variado da engenharia social, desde ataques direcionados a indivíduos ou organizações específicas até campanhas mais amplas, como *phishing* em massa ou fraudes por telefone. Ela explora a confiança e a tendência natural das pessoas em seguir instruções ou fornecer informações quando solicitadas por uma fonte aparentemente legítima [Sanchez-Paniagua and Fernandez 2022].

Entretanto, isso não significa que atacar via engenharia social seja um trabalho fácil, pois implica o atacante possuir habilidades sociais de manipulação e ludíbrio para obter informações ou realizar ações através de suas vítimas. Tais atacantes devem ser hábeis em manipular suas vítimas, como mágicos, atuando para obter informações sensíveis [Uplenchwar et al. 2022]. Em geral, as técnicas de manipulação visam obter a confiança da vítima, por exemplo, com a personificação de uma boa pessoa, para ter acesso a dados, etc. De acordo com [Hossain et al. 2022], a maioria das ameaças de ataques cibernéticos é resultado de engenharia social que, embora exija menos conhecimento técnico, é um método eficaz e não deve ser subestimado. Apenas 3% dos *malwares* tentam explorar aspectos exclusivamente técnicos, os outros 97% visam os usuários por meio de engenharia social [Davis and Grant 2023]. Para [Gong 2023], a maioria dos atacantes são hábeis nos testes de vulnerabilidades em sistemas complexos e seguros e possuem alta probabilidade de sucesso em suas incursões, nas quais conseguem encontrar pontos fracos em sistemas, redes, servidores, etc. Esses dois trabalhos apontam que a união de conhecimentos técnicos em explorar vulnerabilidades com a engenharia social potencializa o sucesso da investida ofensiva.

A Figura 1 ilustra sucintamente o framework conceitual proposto por [Wang et al. 2021] para explicar como ocorrem ataques de engenharia social. Visando alcançar um objetivo, um atacante emprega um método de ataque que tem por base um mecanismo de ação que explora alguma vulnerabilidade da vítima, que resulta em con-

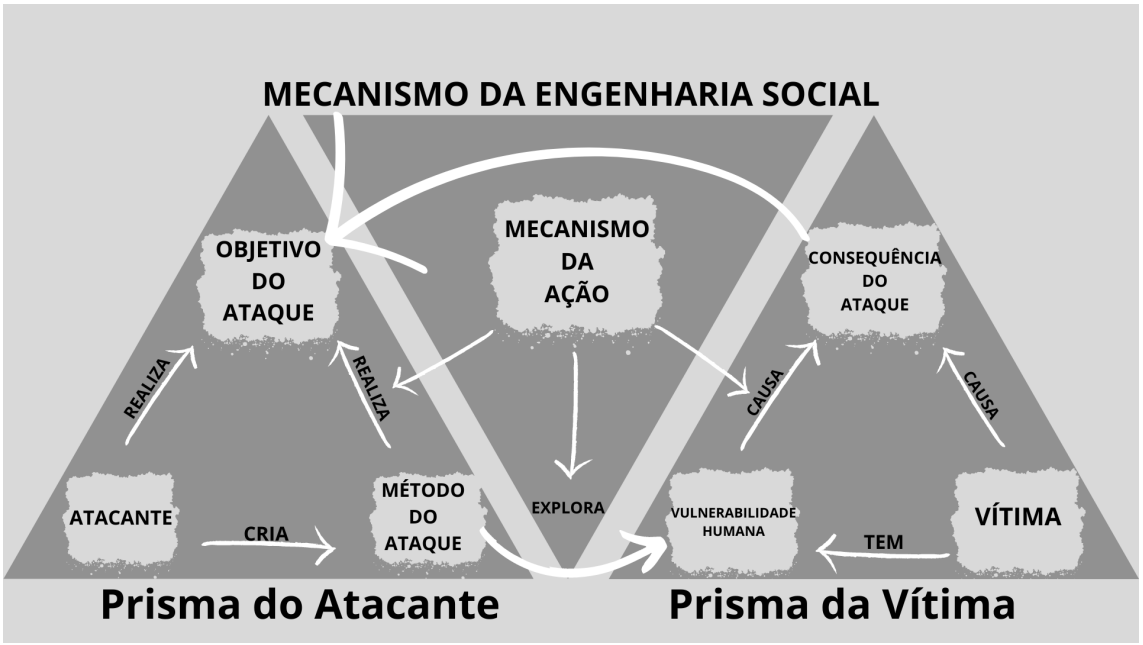

Figura 1. Framework conceitual para explicar a ocorrência ataques de engenharia social. Fonte: [Wang et al. 2021].

sequências (e.g., revelação de informações sensíveis, realização de ações críticas para segurança) que, direta ou indiretamente, permitem ao atacante realizar o objetivo pretendido.

De forma complementar, a Figura 1, apresenta dois prismas, o primeiro sendo o prisma do atacante e o prisma da vítima. Sob o prisma do atacante, podemos dizer que ele cria e executa o ataque com o objetivo de alcançar seu propósito, utilizando um método que concretiza essa intenção. Sob o prisma da vítima, suas vulnerabilidades humanas contribuem para as consequências do ataque. O autor sugere que a própria vítima, ao ser manipulada, pode ser responsável pelo sucesso do ataque. Por fim, o mecanismo de ação que opera em ambos os prismas, consolidando o objetivo do ataque, consiste em um método que explora diretamente as vulnerabilidades humanas específicas, resultando nas consequências do ataque.

3. Framework de Contrainteligência

Entende-se por contrainteligência a atividade de identificar, prevenir e neutralizar as ações de serviços de inteligência adversários [Shpiro 2023]. Com base nesse conceito, o framework aqui proposto estende o framework ilustrado na Figura 1 a partir da premissa de que o conhecimento de contrainteligência de ataques de engenharia social permitirá às vítimas reduzir danos por meio de atitudes comportamentais de natureza proativa e reativa. Ou seja, o conhecimento por parte da vítima sobre os mecanismos de ação e das suas próprias vulnerabilidades em um ataque de engenharia social (Figura 2) tem o efeito de neutralizar o ataque ou mitigar os eventuais danos pretendidos pelo atacante (adversário).

A aquisição do conhecimento de inteligência para se contrapor aos ataques de engenharia social ocorre, segundo [Shpiro 2023, Tuinier et al. 2023], mediante um processo de desenvolvimento de habilidades compreendidas nas seguintes etapas (Figura 3):

1. **Coleta de informações**: Primordial para aquisição de conhecimento em contrainteligência, consiste em manter uma atitude permanente de busca por informações sobre os mecanismos de ação dos ataques de engenharia social, que podem ser obtidas em diversas fontes, como consultas a sites especializados, notícias na mídia, relatos de pessoas conhecidas, cursos de capacitação no contexto organizacional, etc.
2. **Análise de informações**: Compreende analisar as informações coletadas para identificar padrões, tendências e ameaças (potenciais e recorrentes) dos mecanismos de ação.
3. **Produção de resistência e inteligência**: Com base na análise de informações, constitui-se em promover o desenvolvimento de uma resistência em face do conhecimento do mecanismo de ação. A precisão e a relevância desse conhecimento é fundamental para uma tomada de decisão efetiva em um ataque de engenharia social.
4. **Proteção de fontes e métodos**: Consiste em assegurar que os dados coletados no passo inicial foram corretamente compreendidos de modo a produzir resistência que promova uma estrutura de defesa efetiva. Isso porque uma compreensão incorreta poderá gerar a falsa percepção de se estar preparado para se antepor a um ataque, podendo um indivíduo, em virtude disso, colocar-se em situação de maior risco.
5. **Cooperação Social**: Compreende compartilhar (e.g., com as autoridades, instâncias superiores, membros do círculo social mais próximo) experiências vivenciadas de ataques de engenharia social envolvendo mecanismos de ação diversos, para retroalimentar e enriquecer o processo de aquisição de conhecimento.

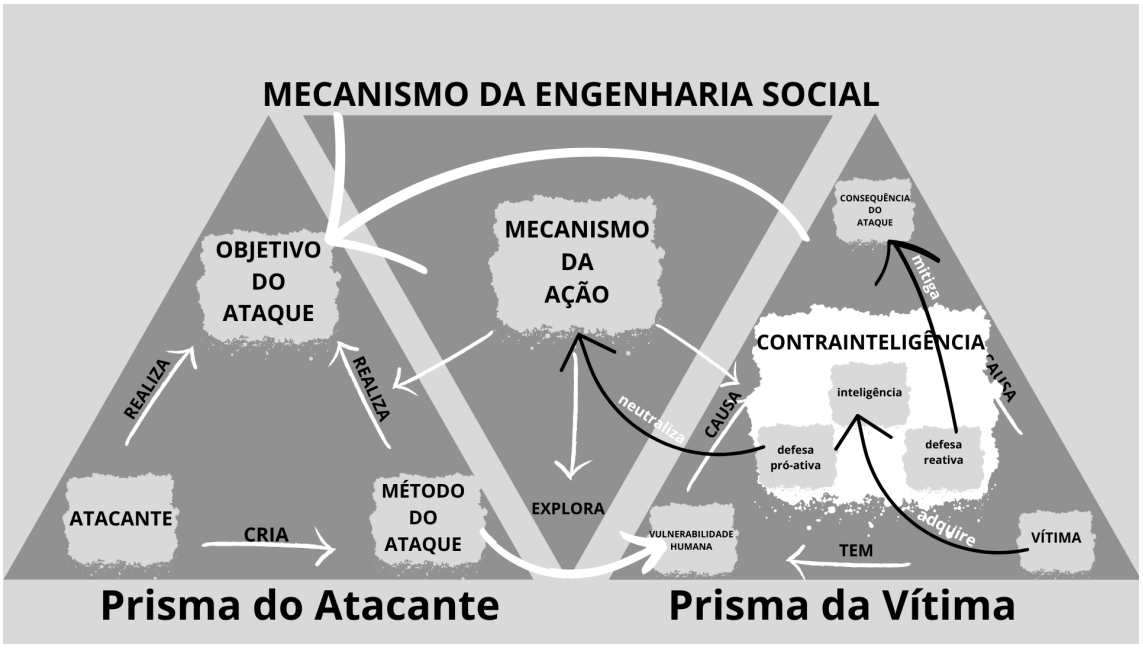

Figura 2. Framework estendido com a contrainteligência. Fonte: elaborado pelo autor e adaptado de [Wang et al. 2021]

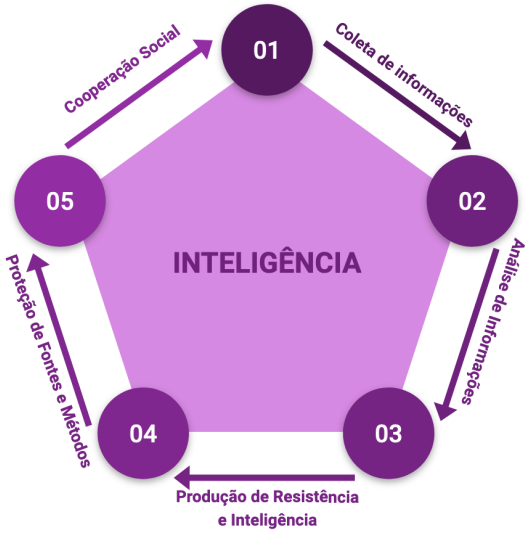

Figura 3. Processo de aquisição de conhecimento de contrainteligência

A incorporação desse conhecimento de contrainteligência é determinante para que uma vítima de ataque de engenharia social tome atitudes efetivas de defesa (proativa e reativa) de modo a neutralizar o ataque ou mitigar os danos decorrentes. Os conceitos de defesas proativa e reativa são comumente associados à segurança, em particular ao contexto da segurança cibernética [Hughes-Wilson 2016].

A defesa proativa refere-se a tomar medidas preventivas de modo a identificar e responder a ameaças na iminência de sua ocorrência, a fim de neutralizar o ataque. Ou seja, trata-se de uma resposta rápida de uma vítima contra tentativas de ataques a ela direcionados. Por exemplo, um indivíduo recebe uma ligação de um operadora de cartão de crédito informando que sua compra foi autorizada e que, caso a desconheça, entre em contato com um número telefônico citado. Sabendo previamente sobre este tipo de ataque, percebe que é uma manobra maliciosa de *phishing* e encerra imediatamente a comunicação com o atacante. A ideia, portanto, é que o conhecimento do mecanismo de ação por parte da vítima reduza suas vulnerabilidades, possibilitando-a se antecipar ao comportamento do atacante de forma a frustrar o ataque.

Por outro lado, a defesa reativa refere-se a tomada de medidas de sustação de um ataque em andamento e de redução de danos, ataque este que a vítima só consegue identificar quando já está ludibriada pelo mecanismo de ação. Ou seja, trata-se de uma reação para mitigar danos e cessar um ataque parcialmente bem sucedido. Por exemplo, no mesmo contexto da situação anterior ilustrada, o indivíduo entra em contato com o número fornecido pelo atacante e começa a ceder suas informações pessoais e, em determinado momento, percebe que está sob ataque de engenharia social. Nessa situação, com as informações já fornecidas, o indivíduo reage cessando imediatamente a comunicação com o atacante para, em seguida, trocar suas senhas, acionar o serviço de atendimento ao consumidor do cartão e informar as autoridades. A expectativa, portanto, é que a vítima, quando se percebe envolvida em um ataque, seja capaz reconhecer o mecanismo de ação de modo a reagir sustando o ataque e tomando medidas apropriadas para mitigar danos.

Observa-se que a defesa proativa é mais efetiva por ser capaz de neutralizar o ataque antes dele produzir danos, dado seu caráter preventivo. Já a defesa reativa acaba sendo menos efetiva por ser acionada após um ataque em andamento ter produzido danos. Em ambas as defesas, o conhecimento de contrainteligência por parte da vítima é fundamental para que o atacante não alcance a totalidade dos seus objetivos.

4. Metodologia

A metodologia empregada nesta pesquisa para verificar o framework proposto fundamenta-se em uma abordagem qualitativa exploratória baseada em entrevistas como ferramenta investigativa, seguindo as diretrizes presentes em [Leitao and Prates 2017, Leitao 2021]. A ideia é verificar, junto a indivíduos que tenham sofrido tentativas de ataques ou ataques de engenharia social, se o conhecimento prévio de mecanismos de ação foram determinantes para neutralizar ou mitigar danos, conforme pressuposto no framework proposto. Segundo tais autoras, essa abordagem metodológica permite uma compreensão aprofundada dos fenômenos estudados e oferece flexibilidade para explorar nuances e perspectivas diversas. As entrevistas são conduzidas com indivíduos selecionados de acordo com critérios de inclusão e exclusão previamente estabelecidos, visando garantir a relevância e representatividade dos participantes. Por outro lado, orientam que devem ser evitados os participantes que não atendem aos critérios de inclusão ou que se enquadrem em um dos critérios de exclusão, a fim de manter a coerência e a precisão dos resultados. Ademais, essa abordagem metodológica proporciona uma análise detalhada e contextualizada dos temas investigados, permitindo a emergência de *insights* significativos e a construção de um conhecimento robusto sobre o objeto de estudo.

5. Considerações Finais

Esta investigação tem como objetivo alcançar, em seus resultados futuros, uma análise detalhada do perfil das pessoas vulneráveis. Além disso, busca preencher a lacuna existente no estado atual da arte no tema de ”engenharia social”. O framework mais atualizado disponível na época da elaboração deste trabalho concentrou-se em descrever as nuances dos ataques, deixando um vazio significativo a ser explorado. Estamos empenhados em suprir essa lacuna, abordando a defesa dos indivíduos na sociedade contra ataques de engenharia social. Nossa intenção é fornecer estratégias e medidas de proteção eficazes para reduzir a vulnerabilidade das pessoas a esses tipos de ataques, contribuindo assim para a segurança e resiliência da sociedade como um todo. O protocolo de pesquisa do presente estudo encontra-se em processo de submissão na Plataforma Brasil do Conselho Nacional de Saúde, número CAAE: 79474624.0.0000.5188, a fim de cumprir os ditames da ética em pesquisa. Após a aprovação, será iniciada as fases de entrevistas para coleta de dados, análise e conclusões. Por fim, espera-se que os resultados deste trabalho possam contribuir para ampliar a compreensão do papel da contrainteligência na defesa dos ataques de engenharia social, podendo auxiliar indivíduos da sociedade civil e organizações a melhor se defenderem contra esse tipo de ataque cibernético.

Referências

Davis, N. and Grant, E. S. (2023). Simulated phishing training exercises versus gamified phishing education games. pages 1–8. Institute of Electrical and Electronics Engineers (IEEE).

Eftimie, S., Moinescu, R., and Racuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. *IEEE Access*, 10:73548–73561.

Gong, X. (2023). Asymmetric information dissemination in double-layer networks helps explain the emergence of cooperation. *IEEE Access*, 11:13202–13210.

Grbic, D. V. and Dujlovic, I. (2023). Social engineering with chatgpt. pages 1–5. IEEE.

Hossain, M. J., Rifat, R. H., Mugdho, M. H., Jahan, M., Rasel, A. A., and Rahman, M. A. (2022). Cyber threats and scams in fintech organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in bangladesh. pages 190–195. Institute of Electrical and Electronics Engineers Inc.

Hughes-Wilson, J. (2016). The secret state: A history of intelligence and espionage. *Pegasus Books, Ltd*.

Leitao, C. F. (2021). *Jornadas de Atualização em Informática 2021, Cap. 7. A entrevista como instrumento de pesquisa científica: planejamento, execução e análise*. Sociedade Brasileira de Computação - SBC, Florianópolis/SC.

Leitao, C. F. and Prates, R. O. (2017). *Jornadas de Atualização em Informática 2017, Cap. 2. A Aplicação de Métodos Qualitativos em Computação*. Sociedade Brasileira de Computação - SBC, Porto Alegre/RS.

Sanchez-Paniagua, M. and Fernandez, E. F. (2022). Phishing url detection: A real-case scenario through login urls. *IEEE Access*, 10:42949–42960.

Shpiro, S. (2023). Blinding the bear: Israeli double agents and russian intelligence. *International journal of intelligence and counterintelligence*, 36(1):1–19.

Tuinier, P., Zaalberg, T. B., and Rietjens, S. (2023). The social ties that bind: Unraveling the role of trust in international intelligence cooperation. *International journal of intelligence and counterintelligence*, 36(2):386–422.

Uplenchwar, S., Sawant, V., Surve, P., Deshpande, S., and Kelkar, S. (2022). Phishing attack detection on text messages using machine learning techniques. Institute of Electrical and Electronics Engineers Inc.

Wang, Z., Zhu, H., and Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, 9:11895–11910.