CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Título do Artigo: ENGENHARIA SOCIAL COMO VETOR DE ATAQUES AO SISTEMA FINANCEIRO

Autores: Jeici Cristina Germano
jeici.germano@fatec.sp.gov.br

Orientador: Prof. Esp. Andre Castro Rizo
andre.rizo@fatec.sp.gov.br

Resumo

Este estudo aborda os impactos da engenharia social dentro da estrutura financeira e quais lacunas são aproveitadas para crescente ocorrência de golpes e fraudes. O objetivo é contribuir para a conscientização da sociedade sobre as principais técnicas na prática desse tipo de crime e oferecer orientações que promovam uma postura vigilante. A pesquisa adotou uma abordagem qualitativa, por meio de revisão bibliográfica em artigos científicos, livros e publicações recentes na área de tecnologia, comportamento humano e direito. Os resultados evidenciam que a maior parte de transações fraudulentas registradas, não ocorre uma intrusão nos sistemas de informação, mas sim uma atuação indireta, em que a própria vítima, ao ser enganada, colabora com a ação criminosa. Isso revela que os investimentos em segurança tecnológica, embora essenciais, são insuficientes para conter tais práticas. Apontando a necessidade de implementar medidas complementares que envolvam aspectos educativos e comportamentais.

Palavras-chave: Engenharia social, segurança, golpe, estrutura financeira, conscientização.

Abstract

This study addresses the impacts of social engineering within the financial structure and which gaps are exploited for the increasing occurrence of scams and frauds. The objective is to contribute to raising awareness in society about the main techniques used in the practice of this type of crime and to offer guidelines that promote a vigilant stance. The research adopted a qualitative approach, through a bibliographic review of scientific articles, books and recent publications in the areas of technology, human behavior and law. The results show that most of the fraudulent transactions recorded do not involve an intrusion into the information systems, but rather an indirect action, in which the victim himself, when deceived, collaborates with the criminal action. This reveals that investments in technological security, although essential, are insufficient to contain such practices. Pointing to the need to implement complementary measures that involve educational and behavioral aspects.

Keywords: Social engineering, security, scam, financial structure, awareness.

Araraquara, 2025

1. Introdução

Movidas pela necessidade de oferecer mais agilidade, praticidade e conectividade aos usuários, empresas de todos os setores, promovem continuamente o uso de soluções digitais.

Para Gonçalves (2014), a segurança da informação atua ativamente na prevenção e mitigação de riscos relacionados ao uso de dados, por meio de processos e tecnologias. Sua principal função é garantir a confidencialidade, integridade e disponibilidade de qualquer conteúdo ou conjunto de informações valiosas para uma organização ou pessoa.

Entre as ameaças mais preocupantes da SI, a engenharia social se destaca por explorar o comportamento humano como instrumento para fraudes e ataques cibernéticos. Ao enganar ou induzir usuários ao erro, cibercriminosos conseguem obter dados sensíveis, causar prejuízos financeiros e comprometer organizações inteiras.

O aumento significativo das tentativas de golpes cibernéticos está diretamente associado ao avanço digital, que, embora proporcione o desenvolvimento de mecanismos de segurança cada vez mais sofisticados, também facilita o acesso a esses recursos por indivíduos mal-intencionados. Esses agentes exploram, simultaneamente, as possibilidades oferecidas pela tecnologia e as fragilidades do fator humano, tornando a segurança da informação um desafio constante (Silva, 2025).

Em geral, os engenheiros sociais buscam obter vantagens financeiras ou competitivas, o que torna o setor financeiro um dos principais alvos, dada a elevada circulação de recursos nesse meio.

De acordo com dados recentes da FEBRABAN (2023), 70% dos golpes e fraudes em operações financeiras ilícitas que atingem os clientes do sistema financeiro derivam de ataques baseados em técnicas de engenharia social.

Com a modernização dos serviços bancários e a crescente digitalização das operações, surgiram também novas modalidades de fraude, que se aproveitam do uso massivo de dispositivos como computadores e smartphones, além da desinformação dos usuários, para induzi-los ao erro e obter acesso a informações restritas. (Bezzutti e Fernandes, 2023).

Considerando o contexto apresentado, este trabalho tem como objetivo apresentar um panorama atual das estratégias utilizadas por engenheiros sociais, as lacunas aproveitadas para crescente ocorrência de golpes e fraudes, bem como analisar os impactos gerados.

A pesquisa também busca expor padrões de comportamento e aspectos relevantes explorados por cibercriminosos, discutir responsabilidade civil das instituições financeira e

explorar medidas para coibir e mitigar esse tipo de prática, a fim de contribuir para a conscientização, a proteção dos usuários e a integridade do sistema financeiro.

A metodologia empregada neste estudo baseou-se em uma pesquisa bibliográfica, de natureza descritiva e abordagem qualitativa fundamentada na análise de produções acadêmicas, livros e periódicos especializados na área de tecnologia, comportamento humano e direito.

2. Revisão Bibliográfica

Esta seção do estudo é destinada à contextualização teórica, por meio da apresentação e discussão de autores e obras relevantes no assunto, com o objetivo de oferecer suporte conceitual e tornar compreensíveis os temas abordados ao longo da pesquisa.

2.1. Engenharia Social

De acordo com Alves (2024), engenharia social constitui uma modalidade de ataque cibernético que se aproveita de aspectos do comportamento e da psicologia humana com o objetivo de obter acesso a informações sigilosas, sistemas ou redes. Trata-se, portanto, de uma estratégia que manipula a confiança e a interação humana para se obter proveito ilícito.

Esse método se baseia na influência e na persuasão para manipular indivíduos, fazendo com que estes acreditem que o engenheiro social é alguém confiável ou pertencente a uma autoridade legítima. Por meio dessa manipulação psicológica, o atacante consegue induzir as vítimas a revelarem informações sensíveis ou a executarem ações que comprometem a segurança de dados e sistemas.

A principal habilidade de um engenheiro social é a de manipular comportamentos humanos para alcançar seus objetivos. A maioria das abordagens empregadas exploram o senso de urgência, a falsa autoridade ou a desinformação, buscando induzir respostas impulsivas.

Silva et al. (2012) explica que o ataque conduzido por um engenheiro social não depende do ambiente virtual e pode ocorrer de maneira discreta e informal, muitas vezes por meio de uma conversa amigável em ambientes descontraídos, durante uma ligação telefônica ou, em casos mais elaborados, por meio de estratégias de conquista.

O sucesso do engenheiro social consiste em inspirar confiança e não ser descoberto. Portanto, adotar uma postura vigilante e manter-se informado sobre as estratégias utilizadas por agentes mal-intencionados facilita a identificação de tentativas de golpe.

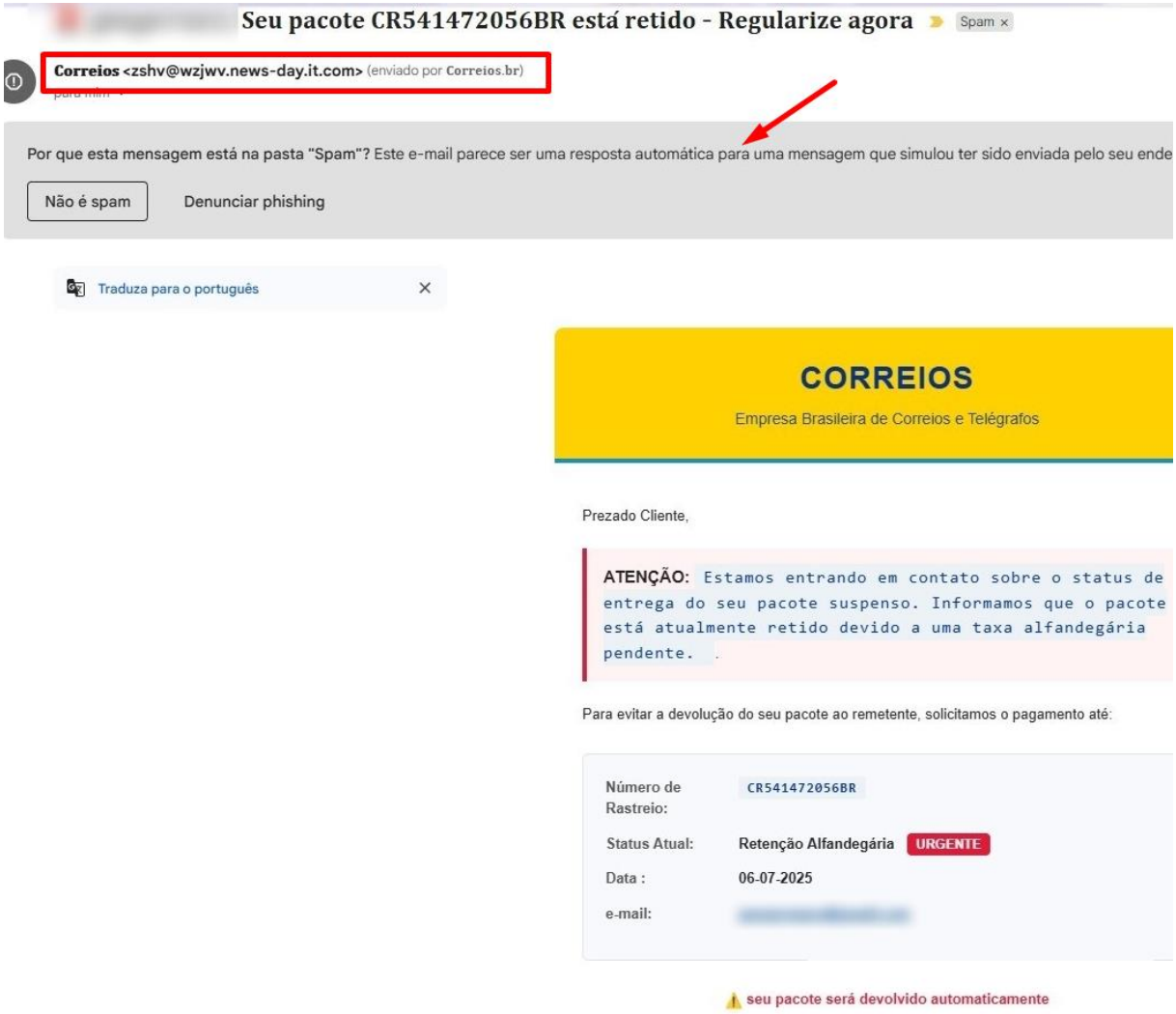
A seguir, destacam-se os golpes mais recorrentes praticados por engenheiros sociais contra clientes do sistema financeiro.

- ***Phishing* (por e-mail)**

O *phishing* por e-mail caracteriza-se pelo envio de mensagens fraudulentas que imitam comunicações de instituições legítimas, como bancos, lojas virtuais ou provedores de serviços. O objetivo é enganar os destinatários, induzindo-os a clicar em links maliciosos que replicam com fidelidade o layout de sites e e-mails oficiais, criando a falsa impressão de que a mensagem foi enviada por uma fonte confiável. A partir dessa estratégia, os golpistas buscam obter informações sigilosas (Alves, 2024).

A Figura 1 demonstra uma tentativa de *phishing* por e-mail em que o golpista simula um e-mail enviado pela empresa Correios e informa sobre a retenção de uma encomenda e solicita o pagamento de uma taxa até a data informada, para que o item não seja devolvido ao remetente. Observa-se, na Figura 1, que o endereço eletrônico não é institucional e que o próprio mecanismo de segurança do e-mail identificou a mensagem como possivelmente *phishing*.

Figura 1 – Ataque de *phishing* por e-mail



Fonte: Elaborado pelo autor (2025)

Para reduzir os riscos associados ao *phishing* por e-mail, é fundamental que os usuários adotem práticas de verificação cuidadosa das mensagens recebidas.

Notificações sobre compras não reconhecidas exigem atenção. A Figura 2 mostra que uma breve verificação no site oficial dos Correios confirmou que o código de rastreamento fornecido não é legítimo.

Figura 2 – Verificação do código de rastreamento

Fonte: Elaborado pelo autor (2025)

- ***Smishing* (*Phishing* por SMS)**

Conforme definido por Alves (2024), o *smishing* é uma variação do *phishing* na qual criminosos utilizam mensagens de texto (SMS) para enganar usuários de dispositivos móveis. Nessa prática, os golpistas enviam mensagens alarmantes, muitas vezes informando supostos bloqueios de contas bancárias ou clonagens de cartões. O propósito central dessas abordagens é induzir a vítima a fornecer dados pessoais e financeiros, além de possibilitar o acesso a sistemas internos. Em alguns casos, o *smishing* também é utilizado como meio de disseminação de códigos maliciosos, como *malware* ou *ransomware*, ampliando o impacto da fraude.

É fundamental ter cautela com links ou números suspeitos presentes nas mensagens, pois eles podem redirecionar o usuário para outras aplicações maliciosas. Em caso de dúvida, o contato com a empresa deve ser feito exclusivamente por meio de canais de comunicação oficiais.

A Figura 3 ilustra a forma como o atacante emprega um tom de urgência com o intuito de induzir o destinatário a uma resposta imediata.

Figura 3 – Ataque de *Smishing*

Fonte: Elaborado pelo autor (2025)

- ***Vishing* (*Phishing* por ligação telefônica)**

O *vishing* é uma técnica de *phishing* que utiliza ligações telefônicas para manipular as vítimas. Os atacantes simulam ser de empresas legítimas para obter acesso a redes sociais, contas bancárias ou convencer o alvo a transferir dinheiro, muitas vezes solicitando códigos de segurança enviados por SMS ou alegando falhas no sistema, descreve Alves (2024).

- **Golpe do PIX**

Embora o Pix seja amplamente reconhecido como um sistema de pagamentos seguro, ele também tem sido utilizado como meio para a movimentação de recursos provenientes de atividades ilícitas. De acordo com dados citados pelo presidente da Federação Brasileira de Bancos (Febraban), Isaac Sidney, os prejuízos relacionados a golpes envolvendo essa

tecnologia aumentaram 43% nos últimos anos, totalizando cerca de R$ 2,7 bilhões (Finsiders Brasil, 2025).

Em estudo, Silva e Cerewuta (2022) observaram que a vulnerabilidade de soluções financeiras digitais está relacionada ao próprio usuário, sobretudo em situações como o roubo de aparelhos celulares, a apropriação indevida de chaves Pix e outros mecanismos.

Os golpes relacionados ao Pix podem ocorrer de diferentes formas, sendo a captura de sessão e a apropriação indevida da imagem, os mais comuns. Enquanto um consiste no envio de um arquivo com código malicioso, que infecta o dispositivo e permite que o criminoso seja notificado assim que o aplicativo do banco for acessado, tornando possível a interceptação das credenciais bancárias da vítima, o outro captura ou cria um perfil com identidade falsa nas redes sociais. A partir disso, os criminosos entram em contato com pessoas próximas à vítima real, alegando ter trocado de número de telefone, como ilustrado na Figura 4, e em seguida, solicitam transferências via Pix, simulando uma situação emergencial ou de urgência financeira.

Figura 4 – Tentativa de golpe do PIX

Fonte: Elaborado pelo autor (2025)

- **Golpe da falsa central telefônica**

Um comunicado emitido pela FEBRABAN (2024) destaca que, assim como as fintechs vêm aprimorando o uso da tecnologia para oferecer soluções inovadoras aos consumidores, os golpistas também têm se apropriado desses recursos de forma estratégica, para adotar estratégias mais sofisticadas para enganar consumidores.

A Federação Brasileira de Bancos esclarece que nesse tipo de ação os criminosos utilizam gravações que simulam as Unidades de Resposta Audível (URAs) dos bancos para aplicar fraudes. Ao atender a ligação, o cliente é informado sobre uma suposta compra ou transação suspeita via Pix, sendo induzido a interagir com um falso atendente. Este, por sua vez, afirma que a operação está em análise e orienta a vítima a tomar medidas como realizar transferências, instalar aplicativos de acesso remoto e fornecer dados bancários sigilosos.

As instituições bancárias podem, eventualmente, entrar em contato com seus clientes para confirmar movimentações consideradas suspeitas. No entanto, é importante ressaltar que, nesses atendimentos, mas jamais solicitam informações sensíveis, como senhas, dados pessoais, atualizações de sistema, chaves de segurança, nem orientam a realização de pagamentos ou estornos (FEBRABAN, 2024).

2.2. Responsabilidade civil das instituições financeiras e bancárias

Para uma compreensão mais aprofundada deste capítulo, é importante entender os conceitos de “golpe” e “fraude” no contexto de transações financeiras. Conforme esclarece Menezes (2022), a fraude caracteriza-se pela subtração de recursos financeiros da conta da vítima sem seu conhecimento ou participação direta, geralmente mediante acesso indevido. Já o golpe envolve a manipulação da vítima por meio de narrativas enganosas, levando-a a realizar, de forma voluntária, uma transferência a favor do agente malicioso, sem perceber que está sendo enganada.

O estudo realizado por Silva e Cerewuta (2022) indica que as instituições financeiras passaram a ter o dever de responder por fraudes decorrentes de falhas em seus próprios sistemas de gerenciamento de riscos. Essa responsabilização abrange, inclusive, a omissão ou inadequação na adoção de medidas efetivas de prevenção e controle de riscos operacionais.

> [...] nos casos em que for caracterizada a fraude será garantido o direito ao consumidor ser indenizado pela instituição financeira, pois, nesses casos, é evidenciada falha no dever de segurança e a consequente responsabilidade civil objetiva, pautada no risco da atividade desenvolvida pela instituição financeira. Já nos casos de golpe, a responsabilização se dá apenas quando da falha de segurança da instituição financeira, caracterizada pela admissão de operações financeiras fora do perfil de transação normal do cliente, pela não realização de bloqueio cautelar dos recursos, pela não efetivação do mecanismo especial de devolução (MED) e, ainda, quando a vítima demonstra alguma hipervulnerabilidade, como ser idosa ou pessoa não alfabetizada (Menezes, 2022, p. 4).

Portanto, quando comprovada a ocorrência de fraude, tanto a jurisprudência quanto a legislação convergem no reconhecimento da responsabilidade civil objetiva das instituições financeiras, no entanto, aqueles identificados como “golpes”, as particularidades de cada caso exercem papel relevante na formação do entendimento do magistrado quanto à configuração — ou não — da responsabilidade civil das IFs (Menezes, 2022).

3. Metodologia

A metodologia adotada neste artigo incluiu uma pesquisa bibliográfica e uma pesquisa descritiva, com o objetivo de compreender como a engenharia social é utilizada como instrumento para ataques ao sistema financeiro.

A natureza descritiva se aplica na intenção de detalhar os mecanismos, práticas e impactos relacionados à engenharia social no cenário financeiro.

A abordagem utilizada foi qualitativa, por permitir uma análise mais direcionada de conteúdos que se concentram em interpretar as relações, padrões e comportamentos humano diante de situações que envolvem esse tipo de ataque.

A pesquisa foi fundamentada em revisão bibliográfica, com a análise crítica de trabalhos acadêmicos, livros, periódicos especializados e publicações recentes na área de tecnologia, comportamento humano e direito. A escolha dessas fontes visou reunir perspectivas atualizadas e multidisciplinares sobre o assunto, contribuindo para a construção de um panorama teórico, sólido e relevante.

4. Resultados Obtidos

Para facilitar a compreensão, os resultados foram segmentados com o propósito de oferecer maior clareza quanto às implicações decorrentes de crimes praticados por engenheiros

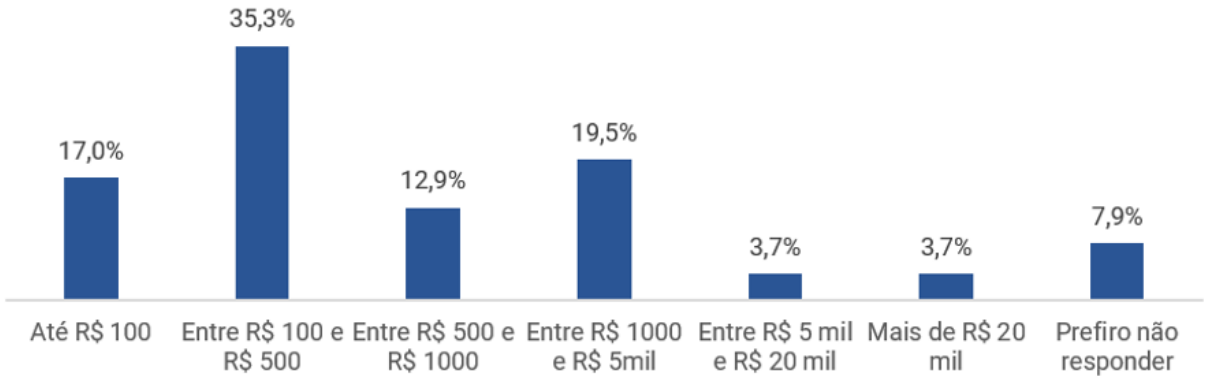
sociais, às iniciativas voltadas à contenção dessas ocorrências e os principais achados das pesquisas realizadas.

4.1. Os impactos decorrentes de golpes cibernéticos

De acordo com o Relatório de Identidade e Fraude 2025, publicado pelo Serasa Experian (2025), 51% dos brasileiros foram vítimas de fraude no último ano, visto que a maioria (54,2%) teve perdas financeiras.

Além disso, o Indicador de Tentativas de Fraude da Serasa Experian aponta que dentre os 54,2% de cidadãos que sofreram golpes e tiveram prejuízo financeiro, 20% correspondem a valores entre R1.000,00 e R$ 5.000,00, conforme demonstrado abaixo na Figura 5.

Figura 5 – Quantidade de perda financeira



Fonte: Serasa Experian (2025)

> Os ataques cibernéticos também influenciam negativamente a saúde mental das vítimas, a sensação de violação de privacidade, a perda de bens financeiros e a insegurança constante podem causar estresse, ansiedade e depressão, infelizmente, essas questões de saúde mental não apenas afetam os indivíduos, mas também seus relacionamentos e a dinâmica familiar (Silva, 2025, p. 33).

No âmbito econômico, além das perdas monetárias e custos com processos legais, os envolvidos podem ter que lidar com danos a relação de confiança e à reputação.

Os golpes cibernéticos também são responsáveis por onerar a estrutura financeira como um todo uma vez que essas organizações enfrentam uma crescente demanda por sistemas

robustos e por recursos eficazes que possibilitem a mitigação e a recuperação das perdas econômicas decorrentes dessas ameaças.

4.2. Medidas adotadas pelo sistema financeiro para inibição de golpes

Conforme descrito por Silva e Cerewuta (2022), com o objetivo de mitigar os riscos associados às atividades realizadas pelas instituições financeiras, especialmente no que se refere ao uso do Pix, os bancos vêm adotando uma série de medidas de segurança. Essas ações incluem desde a limitação dos valores permitidos para transações, campanhas educativas voltadas à conscientização dos usuários, e mecanismos que possibilitam o bloqueio de recursos transferidos ou, em alguns casos, a reversão de transações identificadas como fraudulentas (MED).

O MED (mecanismo especial de devolução) é um dos principais dispositivos contra transações fraudulentas, que viabiliza a devolução do dinheiro para a vítima, apresenta limitações e está em aprimoramento. Em nota publicada pela Finsiders Brasil (2024), a Federação Brasileira de Bancos (FEBRABAN) e o Banco Central (BC) anunciaram melhorias no Mecanismo Especial de Devolução (MED), com o objetivo de ampliar seu alcance para camadas mais complexas das transações financeiras. À época, o sistema atuava apenas na chamada "primeira camada" — ou seja, conseguia rastrear e reter valores apenas na conta que recebeu diretamente a transferência fraudulenta.

Um levantamento de dados do Mecanismo Especial de Devolução (MED), do Banco Central (BC), feito a pedido do Finsiders Brasil (2024), mostrou que ressarcimentos por valores transferidos via Pix e contestados como golpes e fraudes, em média, não ultrapassam 8%. Fica evidente que os prejuízos financeiros resultantes desses ataques são, em grande parte, suportados pelas próprias vítimas.

Mesmo que a vítima denuncie a ação criminosa e a transação financeira fraudulenta seja contestada, a maior parte dos prejuízos monetários decorrentes de golpes e fraudes são absorvidos pelas vítimas, acarretando impactos psicológicos, emocionais e financeiros.

As instituições financeiras contam com mecanismos de segurança que permitem identificar transações atípicas, fora de perfil do usuário, bloqueando para análise as transações suspeitas. A limitação de valores por transações financeiras através do PIX, é outro recurso que contribui para coibição de operações incompatíveis com o perfil do cliente .O investimento em

soluções robustas, como biometria, criptografia e validação de documentos, são fundamentais para proteger consumidores e empresas, mas não são suficientes.

Isaac Sidney, presidente da Federação Brasileira de Bancos (Febraban), aponta que ainda há fragilidades nos procedimentos de abertura de contas, as quais podem facilitar a atuação de agentes mal-intencionados. Nesse sentido, ele enfatiza a necessidade de fortalecer os mecanismos de controle e prevenção, a fim de evitar que o sistema bancário seja utilizado como instrumento para a prática de atividades ilícitas (Finsiders Brasil, 2025).

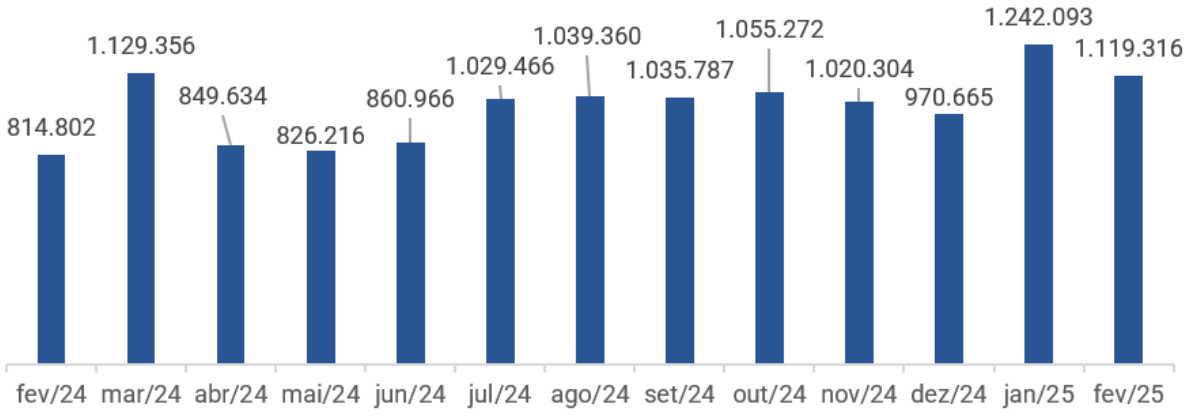
O Banco Central anunciou a criação de um novo serviço que estará disponível ao público a partir de dezembro de 2025. A medida consiste em um sistema que permite ao cidadão "travar" o uso do próprio CPF, impedindo, de forma voluntária, gratuita e reversível, a abertura de contas bancárias em seu nome. Instituído pela Resolução BCB nº 475, o serviço tem como principal finalidade coibir a criação de contas fraudulentas por meio de identidades falsas, bem como evitar a inclusão não autorizada de titulares em contas conjuntas ou a designação indevida de novos responsáveis (BRASIL. Banco Central, 2025).

4.3. Considerações complementares

Através dos estudos realizados, observa-se que apesar do grande investimento em mecanismos de segurança robustos, os números de tentativas de fraudes e golpes continuam crescendo.

Segundo um Indicador de Tentativas de Fraude da Serasa Experian, em fevereiro de 2025 o Brasil registrou mais de 1 milhão de tentativas de fraude. Os dados apresentados na Figura 6 representam uma alta de 37,4% em relação ao mesmo período do ano anterior.

Figura 6 – Quantidade de tentativas de fraude – Últimos 12 meses

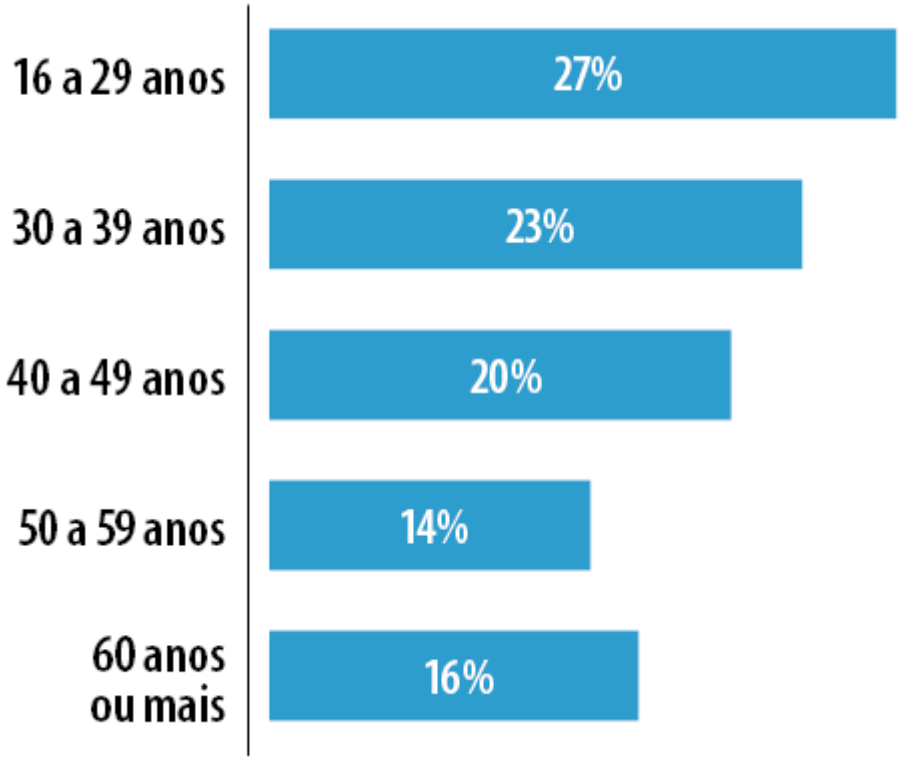


Fonte: Serasa Experian (2025)

Conforme apresentado no sub-título 2.2, Responsabilidade civil das instituições financeiras e bancárias, as instituições financeiras possuem maior responsabilidade quando a vítima demonstra alguma hipervulnerabilidade, como ser idosa ou pessoa não alfabetizada, apesar disso, a pesquisa realizada pelo Data Senado (2025), que entrevistou 22 mil pessoas em 2024, mostrou que os jovens entre 16 e 29 anos correspondem a 27% das vítimas. A faixa de idade com mais de 60 anos, considerada vulnerável, representa 16% de pessoas afetadas por esse tipo de crime. A pesquisa sugere que a presença constante no ambiente virtual está associada a uma maior exposição às ações de engenharia social.

Ainda de acordo com os achados da pesquisa do Data Senado (2025), observa-se uma diferença curiosa nos tipos de golpes aplicados a pessoas de faixas etárias diferentes. Indivíduos mais velhos tendem a ser alvo de fraudes mais sofisticadas, como clonagem de cartões, golpes relacionados ao Pix, falsas centrais bancárias e capturas de dados por meio de ligações telefônicas ou navegação na internet. Já entre os mais jovens, os golpes mais recorrentes envolvem promessas de emprego online e oportunidades de ganhos financeiros fáceis sem sair de casa. A Figura 7 apresenta, de forma mais detalhada, os percentuais de acordos distribuídos conforme as diferentes faixas etárias.

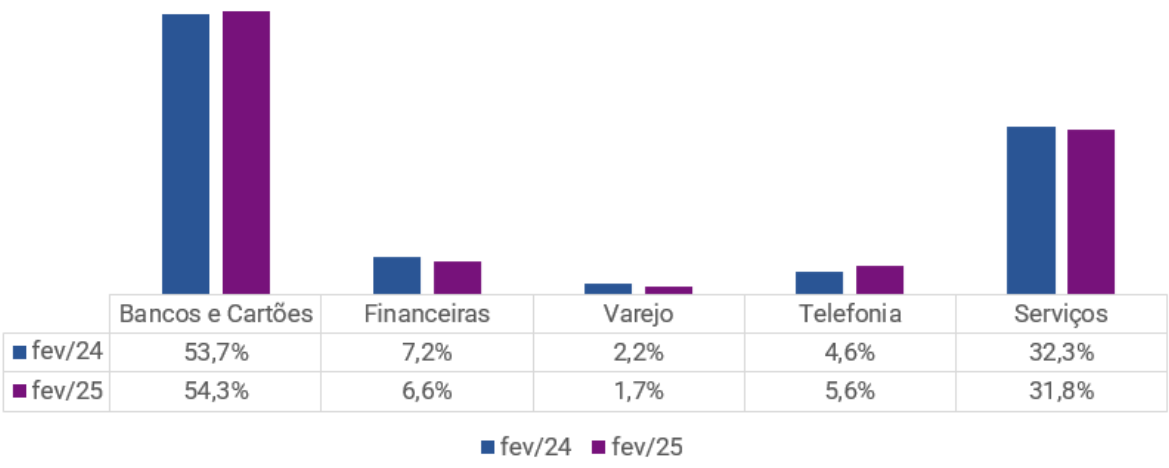
Figura 7 – Fraude na internet ou invasão de contas bancárias por faixa etária



Fonte: Instituto de Pesquisa DataSenado (2025)

Os dados obtidos pelo Serasa Experian revelam que a maior parte das tentativas de golpes e fraudes foi direcionada ao setor financeiro, responsável por 54,3% das ocorrências, seguido pelo segmento de “Serviços” (31,8%), como mostrado na Figura 8.

Figura 8 – Tentativas de fraude por setor (%)



	Bancos e Cartões	Financeiras	Varejo	Telefonia	Serviços
fev/24	53,7%	7,2%	2,2%	4,6%	32,3%
fev/25	54,3%	6,6%	1,7%	5,6%	31,8%

Fonte: Serasa Experian (2025)

A revisão da literatura evidenciou que as instituições financeiras têm direcionado esforços no combate às práticas criminosas que afetam os consumidores do sistema financeiro. No entanto, tais esforços concentram-se, principalmente, no aprimoramento de tecnologias de segurança digital, enquanto as ações voltadas para políticas de prevenção e campanhas de conscientização — fundamentais no enfrentamento das estratégias de engenharia social — ainda recebem atenção limitada e produzem pouco efeito.

A dificuldade em obter informações sobre as ações desenvolvidas pelas *fintechs* em campanhas educativas e de conscientização para a prevenção de golpes financeiros revela tanto a limitada adesão do público a essas iniciativas quanto a aparente baixa prioridade atribuída a esse tipo de ação.

A Tabela 1 foi desenvolvida pelo autor com a intenção de oferecer recomendações práticas e acessíveis sobre como reagir diante de tentativas de manipulação da engenharia social.

Tabela 1 - Golpes de Engenharia Social Mais Frequente

Golpe	**Exemplo Prático**	**Ação Preventiva**
Phishing	E-mail de uma empresa solicitando atualização de dados com link para uma página específica.	Verifique o remetente e nunca clique em links suspeitos. Acesse as plataformas oficiais para verificar possíveis pendências.
Vishing / Golpe da falsa central telefônica	Um indivíduo informa ser atendente do banco e solicita código de verificação e dados bancários para resolver uma situação.	Desconfie de ligações inesperadas e números desconhecidos. Nunca forneça senhas ou códigos por telefone. Em caso de receber ligação, desligue e entre em contato com a instituição utilizando outro número.
Smishing	SMS dizendo que a entrega foi cancelada, com link para "rastrear" pedido.	Jamais clique em links recebidos por SMS de remetentes desconhecidos. Consulte a entrega diretamente no site ou aplicativo da empresa responsável pela entrega.

Baiting	Oferta de brinde ou cupom em troca de dados pessoais ou download de app.	Evite fornecer dados em sites desconhecidos e não baixe arquivos suspeitos.
Golpe do PIX	Um parente ou amigo pede dinheiro via PIX, através das redes sociais, alegando emergência.	Confirme a identidade da pessoa por outro canal de comunicação ou pessoalmente antes de realizar transferências financeiras.

Fonte: Elaborado pelo autor (2025)

Saber identificar e como agir diante de um ataque de engenharia social para não se tornar uma vítima é extremamente importante, mas tomar algumas precauções para evitá-las é ainda melhor.

Alguns hábitos podem dificultar as ações de engenheiros sociais como reduzir a exposição de informações pessoais em redes sociais, usar senhas fortes e diversificadas, ativar a autenticação de dois fatores (2FA), usar conexões seguras, não compartilhar dados, não instalar aplicações de fontes desconhecidas, não salvar contatos telefônicos com informações de parentesco, conhecer e usar tecnologias que evitam ou diminuem as chances de uso indevido de dados e credenciais.

Operações fraudulentas são realizadas por vários meios e com diferentes conteúdos capazes de instigarem a curiosidade do receptor. Logo, mesmo com a conscientização das agências bancárias e do Governo Federal, ainda não são suficientes para evitar os crescimentos das vítimas dessa fraude, por isso é fundamental que os cidadãos se interessem e busquem conhecimento sobre ferramentas que contribuem com a segurança pessoal.

5. Considerações Finais

Esta pesquisa buscou abordar os impactos da engenharia social dentro da estrutura financeira e as lacunas exploradas para a crescente ocorrência de golpes e fraudes. O objetivo foi contribuir para a conscientização da sociedade sobre as principais técnicas utilizadas nesse tipo de crime e oferecer orientações que promovam uma postura diligente.

Os resultados evidenciaram que a maior parte das transações fraudulentas não envolve uma intrusão direta nos sistemas de informação, mas sim uma atuação indireta, em que a própria vítima, ao ser enganada, colabora com a ação criminosa. Isso revela que os investimentos em segurança tecnológica devem ser complementares aos aspectos educativos e comportamentais.

As principais contribuições deste estudo foram:

- Descreve as técnicas de engenharia social mais utilizadas em ataques ao sistema financeiro;
- Aborda as consequências sociais e econômicas geradas pelas ações de engenheiros sociais;
- Evidencia estratégias e instrumentos de proteção disponibilizados pelas entidades bancárias, com o objetivo de evitar ou reduzir os impactos de ações criminosas;
- Destaca a importância da conscientização dos usuários como complemento às soluções tecnológicas de segurança;
- Apresenta recomendações práticas para identificação e prevenção de golpes financeiros.

Em termos de implicações práticas, os resultados deste trabalho podem subsidiar a tomada de decisões por parte do poder judiciário e legislativo, no sentido de aprimorar a regulamentação e a fiscalização do setor financeiro, bem como fomentar políticas públicas voltadas à educação e proteção dos consumidores.

Para pesquisas futuras, sugere-se a análise das medidas adotadas pelo poder público e pelas instituições financeiras, com base nas decisões judiciais e na legislação vigente, a fim de avaliar a efetividade dessas ações no combate aos crimes de engenharia social no contexto financeiro.

Referências Bibliográficas

GONÇALVES, Wilson José. **Termos técnicos fundamentais** – teoria e prática. Campo Grande, MS: Universidade Federal de Mato Grosso do Sul, 2014. Disponível em: <https://www.academia.edu/download/34613700/Termos_Tecnicos_Fundamentais_-_2014-A.pdf#page=76>. Acesso em: 8 mar. 2025

BEZZUTTI, Michael Calgaro; FERNANDES, Elisiane Alves. Os golpes no sistema financeiro na ótica da engenharia social. ***Mercosur en Revista Educación, Tecnología y Sustentabilidad***, v. 2, n. 2, 2022. Disponível em: <https://ojs.uep.edu.py/index.php/mercosur/article/view/315>. Acesso em: 24 mai. 2025.

ALVES, Leonardo de Moura. **Engenharia social**: estudo de ataques e métodos de prevenção. 2024. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Escola Politécnica e de Artes, Pontifícia Universidade Católica de Goiás, Goiânia, 2024. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7976>. Acesso em: 24 mai. 2025.

SILVA, Clayton Silvestre da; ROSA, Adriano Carlos Moraes; CHAIM, Daniel Faria; CARVALHO, Roberto José; CHIMENDES, Vanessa Cristhina Gatto. Engenharia social: o elo mais frágil da segurança nas empresas. **Revista Brasileira de Contabilidade e Gestão**, Ibirama, v. 1, n. 2, p. 29–40, 2012. DOI: 10.5965/2764747101022012029. Disponível em: <https://www.revistas.udesc.br/index.php/reavi/article/view/2840>. Acesso em: 31 mai. 2025.

DE LUCA, Léa. Golpes com Pix dão prejuízos de quase R$ 3 bi em dois anos, diz Febraban. ***Finsiders* Brasil**, 11 mar. 2025. Atualizado em: 23 abr. 2025. Disponível em: <https://finsidersbrasil.com.br/eventos/golpes-com-pix-dao-prejuizos-de-quase-r-3-bi-em-dois-anos-diz-febraban>. Acesso em: 25 mai. 2025.

MENEZES, Ramon Emanuel Gonçalves de. **Fraudes e golpes mediante o uso do PIX**: delimitação da responsabilidade civil das instituições financeiras pelos danos causados aos consumidores. 2022. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal da Paraíba, Centro de Ciências Jurídicas, João Pessoa, PB. Disponível em: <https://repositorio.ufpb.br/jspui/handle/123456789/28629>. Acesso em: 1 jun. 2025.

SILVA, Ana Jasmim Barbosa da; CEREWUTA, Pollyanna Marinho Medeiros**.** A responsabilidade civil das instituições bancárias por danos sofridos no golpe do Pix. ***JNT – Facit Business and Technology Journal***, v. 4, n. 39, p. 71–90, ago./out. 2022. Faculdade de Ciências do Tocantins. Disponível em: <https://revistas.faculdadefacit.edu.br/index.php/JNT/article/view/1942>. Acesso em: 14 jun. 2025.

MORAES, Juliana. Mesmo com MED, só 8% dos valores roubados via Pix são devolvidos. ***Finsiders Brasil***, 20 ago. 2024. Atualizado em: 23 abr. 2025. Disponível em: <https://finsidersbrasil.com.br/noticias-sobre-fintechs/fraudes/mesmo-com-med-so-8-dos-valores-roubados-via-pix-sao-devolvidos>. Acesso em: 26 mai. 2025.

FEBRABAN. Febraban e bancos lançarão Selo de Prevenção a Fraudes das Instituições Financeiras. 2023. Disponível em: <https://portal.febraban.org.br/noticia/3996/pt-br>. Acesso em: 31 mai. 2025.

SERASA EXPERIAN. Brasil registra mais de 1 milhão de tentativas de fraude pelo segundo mês consecutivo em 2025, revela Serasa Experian. 2025. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/brasil-registra-mais-de-1-milhao-de-tentativas-de-fraude-pelo-segundo-mes-consecutivo-em-2025-revela-serasa-experian>. Acesso em: 5 jun. 2025.

SERASA EXPERIAN. Mais da metade dos brasileiros já foi vítima de fraude e 20% deles perderam até R$ 5 mil, revela estudo inédito da Serasa Experian. São Paulo, 2025. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/mais-da-metade-dos-brasileiros-ja-foi-vitima-de-fraude-e-20-deles-perderam-ate-rdollar-5-mil-revela-estudo-inedito-da-serasa-experian>. Acesso em: 15 jun. 2025.

MELO, Luiza. Golpes digitais aumentam e não fazem distinção de idade**. Agência Senado**, 11 abr. 2025. Disponível em: <https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade>. Acesso em: 14 jun. 2025.

SILVA, Guilherme Araújo. **Os impactos psicológicos, sociais e penais nas vítimas de crimes cibernéticos**. 2025. Monografia (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Escola de Direito, Negócios e Comunicação, Goiânia, 2025. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/handle/123456789/8902>. Acesso em: 27 jun. 2025.

BRASIL. Banco Central**.** Banco Central lança novos serviços para o cidadão. **Banco Central do Brasil**, 26 mai. 2025. Disponível em: <https://www.bcb.gov.br/detalhenoticia/20692/nota>. Acesso em: 27 jun. 2025.

FEBRABAN. Criminosos ligam para clientes com falsas gravações para aplicar golpes. 2024. Disponível em: <https://portal.febraban.org.br/noticia/4137/pt-br>. Acesso em: 28 jun. 2025.