Mapeamento e Análise de Metodologias de Fraude Aplicadas ao Pix no Brasil

Glener Lanes Pizzolato, Brenda Medeiros Lopes, Claudio Schepke, Diego Kreutz

[1] Programa de Pós-graduação em Engenharia de Software (PPGES)
Laboratório de Estudos Avançados em Computação (LEA)
Universidade Federal do Pampa (UNIPAMPA) – Alegrete – Brazil

{glenerpizzolato,brendalopes}.aluno@unipampa.edu.br
{claudioschepke,diegokreutz}@unipampa.edu.br

Abstract. *This work presents a review of attack methodologies targeting Pix, the instant payment system launched by the Central Bank of Brazil in 2020. The study aims to identify and classify the main types of fraud affecting users and financial institutions, highlighting the evolution and increasing sophistication of these techniques. The methodology combines a structured literature review with exploratory interviews conducted with professionals from the banking sector. The results show that fraud schemes have evolved from purely social engineering approaches to hybrid strategies that integrate human manipulation with technical exploitation. The study concludes that security measures must advance at the same pace as the growing complexity of attack methodologies, with particular emphasis on adaptive defenses and continuous user awareness.*

Resumo. *Este trabalho apresenta uma revisão das metodologias de ataques relacionadas ao Pix, sistema de pagamentos instantâneos lançado pelo Banco Central do Brasil em 2020. O estudo tem como objetivo identificar e classificar os principais tipos de ataques utilizados contra usuários e instituições financeiras, destacando a evolução e a sofisticação das técnicas empregadas. A metodologia inclui uma revisão bibliográfica e entrevistas exploratórias com profissionais do setor bancário. Os resultados indicam que as fraudes evoluíram de abordagens puramente sociais para estratégias híbridas que combinam manipulação humana e exploração técnica. Conclui-se que o avanço das medidas de segurança deve acompanhar a complexidade crescente das metodologias de ataque.*

1. Introdução

O Pix, lançado pelo Banco Central do Brasil (BCB) em novembro de 2020, tornou-se rapidamente o meio de pagamento mais utilizado no país, superando modalidades tradicionais como TED, DOC, boletos e transações com cartão. Sua adoção em larga escala decorre da disponibilidade contínua, transferências instantâneas e simplicidade operacional por meio das chaves Pix [BCB 2025c]. Desde seu lançamento, os números de transações e de valores movimentados crescem de forma acelerada, alcançando dezenas de bilhões de operações anuais [BCB 2025a].

A expansão desse sistema, entretanto, trouxe desafios relevantes de segurança. Apesar dos mecanismos implementados pelo BCB, incidentes envolvendo vazamento de

dados cadastrais [BCB 2025b], golpes de engenharia social e sequestros-relâmpago cresceram significativamente após a introdução do Pix. Além disso, a redução do uso de dinheiro físico modificou a dinâmica criminal no país, como apontado por estudos internacionais que associam pagamentos digitais a menores índices de criminalidade patrimonial. Casos recentes, como os ataques envolvendo a empresa Sinqia [G1 2025], e o maior roubo por Pix já registrado no Brasil explorado através da empresa C&M Software [Exame 2025], mostram essa tendência.

Realizou-se uma busca sistemática na literatura utilizando o protocolo SMS. Porém não foram encontrados trabalhos relevantes diretamente relacionados ao tema. Diante desse contexto, o objetivo deste trabalho é identificar e descrever as principais tentativas de ataques envolvendo transações Pix, mapear suas características e propor uma taxonomia que agrupe golpes por tipo ou semelhança. Busca-se também analisar o papel da Inteligência Artificial tanto na execução de fraudes quanto nas estratégias de mitigação adotadas pelas instituições financeiras. Para isso, são investigadas metodologias de ataque, classificações existentes e técnicas de segurança implementadas na proteção das transações.

A contribuição central inclui: (a) descrição das metodologias empregadas nos principais golpes; (b) mapeamento e classificação dos ataques; (c) análise do uso de IA em estratégias ofensivas; e (d) levantamento das técnicas de segurança utilizadas por instituições parceiras; Essas análises fornecem uma visão abrangente sobre o panorama de ameaças ao Pix e subsidiam avanços na prevenção, detecção e resposta a fraudes digitais.

2. Metodologia

A metodologia deste trabalho compreendeu, inicialmente, um levantamento de casos de incidentes e golpes relacionados ao Pix, realizado por meio de buscas em sites de notícias, portais especializados e estatísticas oficiais de vazamentos divulgadas pelo Banco Central [BCB 2025b]. Após a coleta, os dados passaram por um processo de limpeza, eliminando duplicatas e consolidando descrições equivalentes provenientes de diferentes fontes, o que permitiu criar um conjunto uniforme de ataques para análise.

Com base neste conjunto consolidado, foi proposta uma taxonomia estruturada em três pilares principais: motivação, meio e execução. A classificação dos ataques foi realizada manualmente e validada com o auxílio de três modelos de LLM: GPT-*4o* [OpenAI 2025], Gemini 2.5 Pro [Google 2025] e DeepSeek-V3 [DeepSeek 2025]. Cada ataque recebeu uma categorização quanto à motivação explorada, ao meio utilizado pelo atacante e ao método de execução empregado. Adicionalmente, avaliou-se o potencial uso de inteligência artificial como elemento facilitador ou amplificador do golpe, especialmente em etapas de geração de conteúdo convincente ou criação de identidades falsas.

Em paralelo à análise dos golpes, foi conduzido um levantamento das técnicas de segurança adotadas por instituições financeiras. Esse processo envolveu buscas abertas, consultas a LLMs, contato com representantes de agências bancárias, conversas com profissionais da área de segurança e interações pelos canais institucionais de atendimento. Para garantir a diversidade e a representatividade, foram selecionadas treze instituições, abrangendo bancos públicos, privados, digitais, cooperativas e instituições de grande capitalização. As técnicas identificadas também foram categorizadas de acordo com o uso ou não de inteligência artificial, permitindo estabelecer relações entre os mecanismos

defensivos e as metodologias de ataque previamente classificadas.

3. Resultados

O levantamento identificou 15 metodologias distintas de golpes envolvendo o Pix, consolidadas a partir de 18 registros iniciais após a remoção de duplicatas. Embora ocorram no contexto do Pix, muitos desses ataques não são exclusivos desse meio de pagamento e podem surgir em outros cenários. Os golpes identificados vão desde engenharia social remota até fraudes estruturadas e abordagens físicas diretas. Entre os principais, estão: golpe do QR Code adulterado; golpes com interação física, como assaltos e sequestros-relâmpago; fraude envolvendo celebridades (golpe da Madonna); falso recibo; falso agendamento; golpe da mão fantasma (acesso remoto); "bug do Pix"; falsas centrais telefônicas; engenharia social via WhatsApp; perfis falsos; falso funcionário de banco; clonagem de WhatsApp; Pix errado; falso leilão; e golpes de preços baixos. A análise permitiu organizá-los em uma taxonomia baseada nos pilares de motivação, meio e execução, e posteriormente agrupá-los em quatro categorias temáticas sintetizadas na Tabela 1.

1. **QR Code adulterado**: Criminosos baixam transmissões legítimas (como lives de ONGs) e as retransmitem com um QR Code fraudulento para desviar doações [UFRJ 2021].
2. **Ataques com Interação Física**: Incluem assaltos, furtos, invasões domiciliares e sequestros-relâmpago nos quais as vítimas são coagidas a realizar transferências Pix [SindicoNet 2025, BBC News Brasil 2022].
3. **Esquema da Madonna**: Golpistas enviam mensagens em nome de celebridades solicitando doações via Pix, explorando empatia e confiança [O Tempo 2025].
4. **Falsificação de Recibo (Pix)**: Falsificação de comprovantes de Pix com alto realismo, induzindo vítimas a acreditarem em pagamentos inexistentes [SPC Brasil 2025].
5. **Fraude do Falso Agendamento**: O criminoso envia um comprovante falso de Pix agendado e solicita a devolução imediata do valor; após receber, cancela o agendamento [Data Rudder 2023].
6. **Mão Fantasma**: Também chamado de "acesso remoto", um *malware* é instalado no celular o que permite ao golpista operar a conta da vítima [Nubank 2025].
7. **Golpe do "Bug do Pix"**: Circulação de vídeos e mensagens afirmando falsamente sobre um suposto erro no sistema Pix, que multiplicaria valores transferidos [Serasa 2025].
8. **Falsas Centrais Telefônicas**: A vítima é induzida a ligar para números fraudulentos após receber alertas falsos sobre supostas atividades suspeitas [UFRJ 2021].
9. **Golpe por Engenharia Social no WhatsApp**: O golpista usa foto e nome da vítima em um número novo e pede dinheiro aos contatos, alegando emergências [Mídia Max 2021].
10. **Golpe do perfil falso**: Criação de perfis falsos em redes sociais usando dados básicos da vítima para solicitar Pix a seus contatos [Data Rudder 2023].
11. **Falso Funcionário de Banco**: O criminoso se faz passar por atendente bancário, oferecendo suporte ao Pix, para obter acesso à conta [FCDL/SC 2023].
12. **Clonagem do WhatsApp**: O golpista engana a vítima a fornecer o código SMS de ativação, clonando o aplicativo e pedindo Pix aos contatos [Stone 2025b].

13. **Golpe do Pix Errado**: A vítima recebe um Pix inesperado e depois, é induzida a devolver o valor, sem perceber a manipulação envolvida [Seu Dinheiro 2024].
14. **Golpe do Falso Leilão**: Sites de leilão falsos exigem pagamento via Pix para garantir produtos inexistentes, explorando urgência e descontos irreais [Stone 2025a].
15. **Esquema dos Preços Baixos**: Após comprometer redes sociais, criminosos anunciam produtos com valores atrativos e pedem pagamento antecipado [G1 2022].

Tabela 1. Agrupamento temático dos golpes mapeados

Grupo	Ataques Relacionados
Engenharia Social Baseada em Autoridade e Confiança	[03] Golpe da Madonna; [08] Falsas centrais telefônicas; [09] Engenharia social via WhatsApp; [10] Perfil falso; [11] Falso funcionário de banco; [12] Clonagem do WhatsApp
Engenharia Social por Devolução, Benefício ou Urgência	[01] QR Code adulterado; [04] Falso recibo; [05] Falso agendamento; [07] Bug do Pix; [13] Pix errado; [14] Falso leilão; [15] Preços baixos
Ataques com Interação Física	[02] Golpes de interação física: assalto, sequestro-relâmpago, extorsão
Ataques Baseados em Software e Acesso Remoto	[06] Mão fantasma / acesso remoto

Engenharia Social Baseada em Autoridade e Confiança. Os ataques deste grupo exploram relações pessoais, figuras de autoridade ou canais de confiança previamente estabelecidos. Golpes como WhatsApp clonado, perfis falsos, falsos atendentes bancários e falsas centrais telefônicas operam com base na credibilidade percebida. Esses ataques tendem a ser altamente eficazes, sobretudo quando combinados a dados vazados ou mensagens personalizadas, criando um cenário de confiança artificial que favorece o erro humano.

Engenharia Social por Devolução, Benefício ou Urgência. Os golpes deste grupo estruturam-se na criação de situações que exigem ações rápidas da vítima. Narrativas envolvendo devoluções, oportunidades financeiras, ofertas irrecusáveis ou recebimentos inesperados dependem de pressões emocionais, como ganância, reciprocidade e urgência. São ataques facilmente escaláveis, muitas vezes acompanhados de comprovantes ou páginas falsificadas, e se beneficiam da automação e da personalização para atingir grandes volumes de vítimas simultaneamente.

Ataques com Interação Física. Aqui, a fraude depende da coação direta da vítima, como em assaltos e sequestros-relâmpago. Embora a execução seja essencialmente presencial, podem existir elementos prévios habilitados por tecnologia, como a seleção de alvos a partir de dados públicos ou rotinas inferidas. O risco é elevado, e as contramedidas requerem integração entre mecanismos bancários de bloqueio rápido e políticas de segurança pública.

Ataques Baseados em Software e Acesso Remoto. O golpe da mão fantasma representa o componente mais técnico, combinando engenharia social inicial com execução baseada em *malware*. Ele se destaca por contornar as proteções bancárias ao obter controle direto do dispositivo da vítima, permitindo transferências mesmo sem interação humana. Esse

tipo de ataque tende a crescer à medida que ferramentas de automação e IA se tornam mais acessíveis.

A investigação também confirmou que todos os golpes mapeados podem ser potencializados por técnicas modernas de inteligência artificial, incluindo a geração de mensagens personalizadas, *deepfakes* de áudio e vídeo, criação automática de sites falsos, perfis sintéticos e *bots* de interação adaptativa. As entrevistas com profissionais do Banco do Brasil, Sicredi e Banrisul reforçam que fraudes por engenharia social são predominantes e que os mecanismos de prevenção incluem 2FA, monitoramento contínuo, modelos de detecção baseados em IA e campanhas intensivas de conscientização. As instituições destacam a rapidez dos criminosos como o principal obstáculo à recuperação de valores, reforçando a necessidade de sistemas de bloqueio mais ágeis e a educação contínua dos usuários.

4. Considerações Finais e Trabalhos Futuros

O presente trabalho realizou uma revisão abrangente das metodologias de ataques envolvendo o sistema Pix, mapeando quinze golpes distintos e propondo uma taxonomia estruturada que organiza esses incidentes segundo motivação, meio e execução. A análise evidencia que a maior parte das fraudes ocorre por engenharia social, destacando a centralidade do fator humano na superfície de ataque. Os resultados mostram uma evolução clara das estratégias criminosas, que migraram de métodos simples para abordagens híbridas cada vez mais sofisticadas, combinando manipulação psicológica, exploração técnica e uso intensivo de mecanismos automatizados. A investigação também confirma que a inteligência artificial desempenha hoje um papel dual: amplia significativamente a capacidade ofensiva dos criminosos, ao mesmo tempo em que fortalece as estratégias defensivas adotadas por instituições financeiras.

As entrevistas com representantes do Banco do Brasil, Sicredi e Banrisul reforçam que golpes apoiados por engenharia social permanecem como o maior desafio operacional, uma vez que a rapidez das transações do Pix e a pulverização imediata dos valores dificultam a recuperação. As instituições utilizam autenticação multifatorial, sistemas de detecção baseados em IA e campanhas de conscientização, mas há consenso de que a velocidade dos criminosos e a vulnerabilidade emocional dos usuários ainda constituem gargalos críticos. Dessa forma, o trabalho contribui ao sistematizar um panorama atual e multifacetado das ameaças ao Pix, oferecendo uma base conceitual consistente para estudos futuros e para o aprimoramento das estratégias de prevenção, detecção e resposta.

Como desdobramentos deste estudo, propõem-se várias frentes de investigação. Primeiramente, recomenda-se aprofundar a modelagem comportamental das vítimas e dos atacantes, permitindo o desenvolvimento de sistemas preditivos capazes de identificar interações suspeitas antes da efetivação de transações. Além disso, considerando o avanço de *deepfakes* aplicados a golpes financeiros, pesquisas futuras podem explorar técnicas de detecção automática de conteúdo sintético (texto, áudio e vídeo) gerados pela IA. Outra direção promissora envolve o estudo de mecanismos de verificação contextual de transações, combinando análise de risco em tempo real e limites dinâmicos de operação, ajustados conforme os padrões históricos dos usuários.

Também se sugere investigar o impacto de políticas públicas e regulamentações específicas que possam reduzir a superfície de ataque em cenários de engenharia social

e interação física, incluindo protocolos unificados de bloqueio de emergência no sistema financeiro. Finalmente, o trabalho pode ser expandido com a criação de um *dataset* nacional de golpes relacionados ao Pix, anonimizados e padronizados, servindo como base para pesquisa em segurança digital, aprendizado de máquina e criação de simuladores de fraude para testes controlados. Essas iniciativas têm potencial para fortalecer significativamente a resiliência do ecossistema Pix, acompanhando a crescente sofisticação das ameaças observadas.

Agradecimentos

Este trabalho contou com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Esta pesquisa recebeu também apoio parcial da Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul (FAPERGS), por meio dos termos de outorga 24/2551-0001368-7 e 24/2551-0000726-1.

Referências

[BBC News Brasil 2022] BBC News Brasil (2022). Vítima de 'sequestro do Pix' relata cárcere de 8h na mata: 'R$ 160 mil em saques e empréstimos'. https://www.bbc.com/portuguese/brasil-62045088.

[BCB 2025a] BCB (2025a). Estatísticas do Pix. https://www.bcb.gov.br/estabilidadefinanceira/estatisticaspix.

[BCB 2025b] BCB (2025b). Registro de incidentes com dados pessoais. https://www.bcb.gov.br/acessoinformacao/lgpd?modalAberto=registro_de_incidentes_com_dados_pessoais.

[BCB 2025c] BCB (2025c). Site do Banco Central do Brasil. https://www.bcb.gov.br/estabilidadefinanceira/pix.

[Data Rudder 2023] Data Rudder (2023). Como funcionam as táticas de engenharia social no pix? https://datarudder.com/como-funcionam-as-taticas-de-engenharia-social-no-pix/.

[DeepSeek 2025] DeepSeek (2025). DeepSeek Chat: AI Language Model. https://www.deepseek.com.

[Exame 2025] Exame (2025). Dinheiro que some em segundos: o roubo de R$ 1 bilhão e as lições para o futuro da cibersegurança. https://exame.com/tecnologia/dinheiro-que-some-em-segundos-o-roubo-de-r-1-bilhao-e-as\-licoes-para-o-futuro-da-ciberseguranca/. Acessado em: 4 de agosto de 2025.

[FCDL/SC 2023] FCDL/SC (2023). Conheça os golpes com Pix e saiba como evitá-los. https://www.fcdl-sc.org.br/fcdl-blog/conheca-os-golpes-com-pix-e-saiba-como-evita-los/.

[G1 2022] G1 (2022). Em novo golpe do pix, criminosos invadem contas em rede social e simulam vendas com mega descontos; saiba como se proteger. https://g1.globo.com/sp/vale-do-paraiba-regiao/noticia/2022/03/15/em-novo-golpe-do-pix-criminosos-invadem-contas-em-rede-\social-e-simulam-vendas-com-mega-descontos-saiba-como-se\-proteger.ghtml.

[G1 2025] G1 (2025). Ataque hacker desviou R$ 710 milhões, diz empresa que opera sistema PIX. https://g1.globo.com/economia/noticia/2025/09/02/ataque-hacker-sinqia.ghtml. Acessado em: 08 de setembro de 2025.

[Google 2025] Google (2025). Gemini - Large Language Model. https://gemini.google.com.

[Mídia Max 2021] Mídia Max (2021). Pix: Conheça os golpes mais frequentes e como evitar fraudes na transferência de dinheiro. https://midiamax.uol.com.br/cotidiano/economia/2021/pix-conheca-\os-golpes-mais-frequentes-e-como-evitar-fraudes-na-\transferencia-de-dinheiro/.

[Nubank 2025] Nubank (2025). Golpe da mão fantasma: o que é e como se proteger do acesso remoto? https://blog.nubank.com.br/golpe-mao-fantasma-acesso-remoto/.

[O Tempo 2025] O Tempo (2025). Golpe da Madonna finge que ela foi assaltada e pede Pix: 'Hello, friend'. https://www.otempo.com.br/brasil/golpe-da-madonna-finge-que-ela-foi-assaltada-e-pede-pix\-hello-friend-1.3524426.

[OpenAI 2025] OpenAI (2025). ChatGPT: Modelo de linguagem da OpenAI. https://openai.com/chatgpt. Acessado em: 17 fev. 2025.

[Serasa 2025] Serasa (2025). Golpes do pix: como se proteger? https://www.serasa.com.br/premium/blog/golpes-do-pix-como-se-proteger/.

[Seu Dinheiro 2024] Seu Dinheiro (2024). Novo golpe do pix: bandidos abusam de mecanismo que serve para prevenir fraudes; veja como se proteger. https://www.seudinheiro.com/2024/financas-pessoais/novo-golpe-do-pix-bandidos-abusam-de-mecanismo-que-serve\-para-prevenir-fraudes-veja-como-se-proteger-jesc/.

[SindicoNet 2025] SindicoNet (2025). Criminoso invade prédio e obriga morador a fazer Pix em SP. https://www.sindiconet.com.br/informese/criminoso-invade-predio-obriga-morador-fazer-pix-sp-\noticias-seguranca.

[SPC Brasil 2025] SPC Brasil (2025). Golpe do pix: veja quais são e saiba como se proteger. https://www.spcbrasil.org.br/blog/golpe-do-pix.

[Stone 2025a] Stone (2025a). Como se prevenir contra o golpe do falso leilão? https://blog.stone.com.br/como-se-prevenir-contra-o-golpe-do-falso-leilao/.

[Stone 2025b] Stone (2025b). Golpe do WhatsApp clonado: veja como funciona e o que fazer. https://blog.stone.com.br/golpe-do-whatsapp-clonado/.

[UFRJ 2021] UFRJ (2021). Pix: 6 golpes mais frequentes. https://seguranca.tic.ufrj.br/noticias/pix-6-golpes/.