CONEPA
CONGRESSO NACIONAL DE ESTUDANTES E PROFISSIONAIS DE ADMINISTRAÇÃO

10ª Edição 2024 | 22 e 23 de novembro de 2024
João Pessoa, Paraíba (Região Nordeste)

AS FRAUDES BANCÁRIAS NO BRASIL E COMO OS BANCOS ALERTAM SEUS CLIENTES

Guilherme de Castro Gonçalves
Mestrando em Administração
Universidade Federal da Paraíba
guilhermedecastrogoncalves@yahoo.com.br

ISSN: 2764-7226

Resumo

As fraudes bancárias representam um desafio substancial no sistema bancário brasileiro, impactando diretamente as operações financeiras, segurança do cliente e confiança nas instituições. Os crimes financeiros afetam diretamente o resultado operacional dos bancos, que precisam destinar recursos para prevenção, monitoramento de transações, reembolsos para clientes e ações de marketing para o prevenir o público em geral. O aumento das fraudes digitais através de *phishing* e fraudes cometidas com técnicas de engenharia social somadas à complexidade das técnicas utilizadas por criminosos fazem com que as instituições financeiras invistam continuamente em tecnologias de segurança, monitoramento e em práticas de prevenção. As fraudes bancárias apresentam riscos ao bem estar das pessoas além dos riscos financeiros. Os clientes que sofrem perdas causadas por fraudes bancárias podem reduzir a confiança nos serviços realizados de forma digital. A relevância na pesquisa sobre fraudes bancárias no Brasil vem da digitalização do setor financeiro, transformação digital e do aumento das transações digitais, com utilização de *mobile banking* e *internet banking*, apresentando grandes oportunidades, mas também com seus riscos associados, com impacto na esfera social, prática e teórica. O presente adota uma abordagem qualitativa e exploratória, com o objetivo de analisar as práticas de segurança adotadas pelos principais bancos brasileiros para alertar os clientes contra fraudes bancárias, com amostra de 06 grandes bancos no Brasil através de pesquisa documental nos sites oficiais destas empresas. o setor bancário brasileiro permaneça em posição privilegiada é indispensável que a segurança dos canais digitais esteja em constante evolução os bancos não só fortalecerão suas relações com os clientes, mas também contribuirão para a promoção da inclusão digital no país.

Palavras-chave: Bancos. Fraudes Bancárias. Phishing. Engenharia social.

Abstract

Bank fraud represents a substantial challenge in the Brazilian banking system, directly impacting financial operations, customer security and trust in institutions. Financial crimes directly affect the operating results of banks, which need to allocate resources to prevention, transaction monitoring, customer refunds and marketing actions to prevent the general public. The increase in digital fraud through phishing and fraud committed with social engineering techniques, combined with the complexity of the techniques used by criminals, means that financial institutions are continually investing in security technologies, monitoring and prevention practices. Bank fraud poses risks to people's well-being in addition to financial risks. Customers who suffer losses caused by bank fraud may reduce their trust in digital services. The relevance of research on bank fraud in Brazil comes from the digitalization of the financial sector, digital transformation and the increase in digital transactions, with the use of mobile banking and internet banking, presenting great opportunities, but also with their associated risks, with impact on the social, practical and theoretical spheres. This study adopts a qualitative and exploratory approach, with the objective of analyzing the security practices adopted by the main Brazilian banks to alert customers against banking fraud, with a sample of 06 large banks in Brazil through documentary research on the official websites of these companies. For

the Brazilian banking sector to remain in a privileged position, it is essential that the security of digital channels is constantly evolving. Banks will not only strengthen their relationships with customers, but will also contribute to the promotion of digital inclusion in the country.

Keywords: Banks. Bank Fraud. Phishing. Social Engineering

1. INTRODUÇÃO

As fraudes bancárias representam um desafio substancial no sistema bancário brasileiro, impactando diretamente as operações financeiras, segurança do cliente e confiança nas instituições. A fraude é um crime grave que envolve engano intencional, truque, manipulação, trapaça, mentira ou roubo. As vítimas de fraude podem ser indivíduos e organizações (WELLS, 2011). O aumento das fraudes digitais através de *phishing* que é um tipo de ataque cibernético que usa e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar pessoas a compartilhar dados confidenciais ou expor a crimes cibernéticos de outras formas (IBM, 2024) e fraudes cometidas com técnicas de engenharia social que são maneiras de manipular vítimas para conseguir informações pessoais com o fim de realizar um ataque que pode comprometer a segurança pessoal ou segurança de uma rede corporativa (IBM, 2024) somadas à complexidade das técnicas utilizadas por criminosos fazem com que as instituições financeiras invistam continuamente em tecnologias de segurança, monitoramento e em práticas de prevenção. Os crimes financeiros afetam diretamente o resultado operacional dos bancos, que precisam destinar recursos para prevenção, monitoramento de transações, reembolsos para clientes e ações de marketing para o prevenir o público em geral. Percebe-se a necessidade de ferramentas adequadas para gerenciar riscos como segurança da informação e riscos dos clientes, sendo necessário implementar ações preventivas para tentar acompanhar a velocidade da digitalização bancária (JADWANI; PARKHI; MITRA, 2024). Embora as fraudes possam aumentar os custos operacionais dos bancos, o desenvolvimento de ferramentas e procedimentos baseados na ampliação da digitalização bancária pode aumentar o lucro dos bancos (DIENER, 2020).

As fraudes bancárias apresentam riscos ao bem estar das pessoas além dos riscos financeiros. Os clientes que sofrem perdas causadas por fraudes bancárias podem reduzir a confiança nos serviços realizados de forma digital, dificultando a adoção a tais canais e comprometendo a expansão de novas tecnologias apresentadas pelos bancos, apresentando um grande desafio para os clientes e instituições financeiras (DINO, 2024). Um aspecto fundamental para manter a confiança dos clientes é a prevenção de fraudes, que visa reduzir custos operacionais associados a reembolsos dos prejuízos, podendo fortalecer a lealdade dos clientes e se faz necessária a comunicação eficaz das medidas de segurança para desempenhar um papel crucial na retenção e satisfação dos clientes, especialmente para aqueles que já sofreram fraudes (HOFFMANN; BIRNBRICH, 2012).

No Brasil verifica-se que um alvo constante das tentativas de fraudes são os clientes mais idosos. Em um estudo realizado por Gamble *et al.* (2014) no contexto americano, a suscetibilidade dos idosos a golpes financeiros está associada a alguns elementos, como o declínio cognitivo e a confiança excessiva em sua capacidade financeira. Também foi constatado que ser vítima de algum tipo de golpe aumenta a probabilidade de assumir riscos financeiros, o que, por sua vez, os torna mais vulneráveis a outras formas de fraude.

A digitalização dos serviços bancários, impulsionada pelo uso crescente de transações em aparelhos *mobile* e *internet banking* oferece praticidade, acessibilidade e conforto para os clientes, porém, a disseminação de novas tecnologias ampliou a exposição à riscos, o que torna um grande desafio para as instituições financeiras. Com a expansão das transações digitais, as vulnerabilidades aumentaram o que aumenta o nível de sofisticação dos criminosos para aplicação de golpes cibernéticos e bancários (AGUAYO; ŚLUSARCZYK, 2020). Porém, para mitigar esse risco, percebe-se o uso de novas tecnologias como a Inteligência Artificial para melhorar sistemas de segurança de dados. (MISHRA, 2023).

Um grande exemplo de inovação tecnológica foi a criação do PIX no sistema financeiro brasileiro. O pix é a transferência imediata de recursos entre contas com utilização de chaves personalizadas, como CPF, telefone e e-mail, com funcionamento

durante as 24 horas de todos os dias da semana. Segundo o relatório do impacto econômico e inclusão financeira desenvolvido pela ACI Worldwide em parceria com The Centre for Economics and Business Research, o PIX deve impulsionar o Produto interno Bruto (PIB) do Brasil em R$ 280,7 bilhões até 2028 (ARAUJO, 2024) e contou com mais de 161 milhões de usuários entre empresas e pessoas de acordo com dados do Banco Central do Brasil (BACEN).

Porém, tal inovação também traz o aspecto negativo do aumento de fraudes, com impacto no setor regulatório. O Banco Central do Brasil e outros setores do governo estão empenhados em estabelecer normas de segurança e proteção, exigindo adaptações contínuas por parte das instituições financeiras. Com o surgimento do PIX e a aumento de bancos e carteiras digitais de pagamentos, a pressão regulatória aumenta, exigindo que os bancos monitorem e relatem atividades suspeitas de forma frequente e transparente.

Dessa forma, as fraudes bancárias não só afetam os resultados financeiros dos bancos, mas também definem como o setor bancário opera e age em relação às crescentes demandas de segurança e confiança por parte dos clientes.

A relevância na pesquisa sobre fraudes bancárias no Brasil vem da digitalização do setor financeiro, transformação digital e do aumento das transações digitais, com utilização de *mobile banking* e *internet banking*, apresentando grandes oportunidades, mas também com seus riscos associados. A análise dos tipos de fraudes bancárias e das práticas de proteção adotadas pelos bancos brasileiros é essencial para compreender como o setor lida com as ameaças e suas ramificações. A justificativa deste artigo está baseada em três aspectos: a relevância teórica, prática e social.

O presente estudo apresenta relevância na esfera social ao informar os principais tipos de fraudes bancárias que ocorrem no Brasil para tentar aumentar a proteção do consumidor, já que a fraude acarreta em resultados negativos além da esfera financeira, mas também com efeitos físicos, psicológicos e emocionais. À medida que a utilização de canais digitais vai se popularizando e um país de dimensões continentais como o Brasil que possui áreas de difícil acesso físico é fundamental que se tenha preocupação com a

segurança nas transações bancárias dos clientes. A eficácia na prevenção de fraudes não é apenas do interesse do negócio, pois encoraja as transações, mas também da sociedade em geral, pois garante que haja espaços seguros para transações financeiras e amplia a inclusão digital da economia. De acordo com estudos da Accenture (2023) o Brasil reforça seu papel de liderança na América Latina e no mundo em relação ao desenvolvimento de novas tecnologias e o sucesso do sistema bancário brasileiro.

Na esfera acadêmica, o estudo sobre fraudes bancárias contribui para a literatura sobre os tipos de fraudes como *phishing* e as fraudes com utilização de engenharia social no contexto brasileiro com a pesquisa focada nos maiores bancos do Brasil ao apontar as tipologias das fraudes bancárias a fim de avaliar a eficácia das medidas de prevenção realizadas pelas instituições financeiras. Na esfera prática, a contribuição é para funcionários de bancos que podem saber se suas estratégias de prevenção de fraudes estão tendo a eficácia desejada junto aos seus clientes.

Após contextualização do problema, surge o seguinte problema de pesquisa:

Quais os tipos de fraudes bancárias sofridas por clientes de bancos no Brasil e como essas instituições financeiras efetuam mecanismos de prevenção de fraudes e comunicam para seus clientes?

OBJETIVO GERAL

Investigar as principais tipologias de fraudes bancárias no Brasil com ênfase nas práticas de prevenção a fraudes adotadas pelos bancos para proteger os clientes.

OBJETIVO ESPECÍFICO

I - Apontar os principais tipos de fraudes bancárias nas instituições financeiras brasileiras.

II - Analisar as medidas de prevenção a fraudes divulgadas a clientes pelos principais bancos no Brasil.

ISSN: 2764-7226

2. REFERENCIAL TEÓRICO

Engenharia social é fazer com que usuários comprometam sistemas de informação. Em vez de ataques técnicos a sistemas, engenheiros sociais miram humanos com acesso a informações, manipulando-os para divulgar informações confidenciais ou mesmo para executar seus ataques maliciosos por meio de influência e persuasão (KROMBHOLZ *et al*., 2015). Os ataques maliciosos podem sucesso dependendo do estado psicológico das pessoas, tais como: reciprocidade, compromisso, comportamento social, autoridade, simpatia, escassez.

Quadro 01 – Princípios psicológicos

Princípio	Descrição
Reciprocidade	As pessoas retribuem favores para não sentir-se em dívida.
Compromisso	As pessoas gostam de manter um comportamento consistente.
Comportamento social	As pessoas tendem a seguir o comportamento de terceiros, especialmente em situações de incerteza.
Autoridade	As pessoas concordam com especialistas confiáveis ou figuras hierárquicas superiores.
Simpatia	As pessoas preferem dizer sim para aqueles com quem têm empatia.
Escassez	As pessoas tendem a aceitar ofertas quando estão em falta.

Os princípios acima podem ser exemplificados da forma abaixo:

ISSN: 2764-7226

Quadro 02 – Exemplos de fraudes por princípio

Princípio	Exemplo
Reciprocidade	A vítima fornece informações como forma de retribuir alguma informação dada pelos bandidos.
Compromisso	Cliente recebe ligação de falsa central telefônica de banco e permanece em linha com os bandidos.
Comportamento Social	Cliente realiza procedimento solicitado pelos bandidos, pois é dito que "todo mundo está fazendo".
Autoridade	Bandidos se identificam como gestores ou responsáveis por setores, fazendo a vítima acreditar em seu poder.
Simpatia	Cliente permanece em linha após receber ligação, pois o atendimento dos bandidos é empático.
Escassez	Cliente realiza procedimento com a promessa de que uma promoção de troca de pontos está se esgotando.

A engenharia social pode ser categorizada em física, técnica, social e sociotécnica (KROMBHOLZ *et al*., 2015). A física envolve a interação entre vítima e criminoso de forma presencial ou uma invasão à um banco para verificar documentos à mostra para roubo de informações (GRANGER, 2001). A técnica é através da internet como páginas falsas e e-mails para roubar senhas. A social envolve técnicas de manipulação para conseguir dados da vítima, como uma ligação de alguém se passando pelo gerente bancário do cliente e sociotécnica é um mix da social e da técnica.

E em relação aos tipos de fraudes, temos as fraudes de cartão de crédito como compras realizadas em site através do roubo do número do cartão de crédito, fraudes em caixas eletrônicos como instalação de equipamentos de roubo de dados, fraudes com transferência de dinheiro com alteração do nome do beneficiário, fraude com documentos falsos para transferência para bancos estrangeiros, *phishing* como tentativa de obter informações de vítimas como usuário e senha através de sites ou e-mails falsos e roubo de identidade quando informações são roubadas para criar novos documentos de identificação e abertura de contas bancárias falsas (AMOH; AWUNYO-VITOR; OFORI-BOATENG, 2021).

ISSN: 2764-7226

Todas essas formas de fraudar vítimas tem um impacto imenso no nível individual dos clientes. Segundo Kassem (2024) as fraudes podem impactar a saúde mental, emocional e social das vítimas, pode gerar: a) estresse, ansiedade, raiva e medo, podendo levar a estados de pânico e depressão, b) baixa autoestima e vergonha por se sentirem culpadas por terem sido vítimas de golpes, c) problemas físicos como insônia, aumento de pressão arterial e redução da imunidade, d) redução da confiança em questões financeiras por desconfiança dos canais digitais, e) problemas graves de saúde mental. f) problemas para socializar e se relacionar com outras pessoas em virtude da perda de confiança e g) redução da felicidade e satisfação com a vida. Para mitigar os efeitos na confiança dos clientes é necessário que os bancos realizem mecanismos de prevenção a fraudes e que os bancos informem aos clientes tais medidas visando a satisfação do cliente, confiança, lealdade e comprometimento com a empresa (HOFFMANN; BIRNBRICH, 2012).

3. METODOLOGIA

O presente adota uma abordagem qualitativa e exploratória, com o objetivo de analisar as práticas de segurança adotadas pelos principais bancos brasileiros para alertar os clientes contra fraudes bancárias. Tal abordagem é necessária quando o tema está em constante evolução e quando o interesse é de entender o porquê está acontecendo aquele fenômeno (CRESWELL, 2007). O processo metodológico baseou-se em três pilares: coleta de dados, análise das práticas para informar aos clientes sobre fraudes bancárias e análise comparativa entre os bancos.

A amostra foi de 06 grandes bancos no Brasil, sendo 05 tradicionais e um banco digital: Banco do Brasil, Itaú, Santander, Bradesco, Caixa econômica Federal e Nubank. A amostra representa os bancos com maior quantidade de clientes segundo relatório mensal disponibilizado pelo BACEN. A coleta de dados foi realizada através de pesquisa documental nos sites oficiais dos bancos e matérias disponibilizadas na internet sobre as medidas para informar os clientes sobre as fraudes mais comuns que estão ocorrendo.

Após isso foi realizada a análise dos dados coletados para verificar a eficácia da maneira como são divulgadas as políticas de prevenção a fraude bancárias para os clientes

e em fase posterior, foi realizada a análise de forma comparada para identificar se algum banco se destaca com algum mecanismo disruptivo de comunicação ou se são todos similares.

O estudo teve como limitação o fato de a pesquisa ter sido realizada com as informações disponibilizadas de forma públicas e não mais detalhadas sobre as politicas de seguranças especificas, pois entende-se que tais políticas seriam sigilosas e ao serem divulgadas, poderia causar danos para as instituições bancárias.

4. RESULTADOS E DISCUSSÕES

A Federação Brasileira dos Bancos (FEBRABAN) disponibiliza uma lista dos principais tipos de fraudes bancárias que estão ocorrendo com os clientes, que em virtude do avanço da tecnologia, cada vez mais as fraudes vão se tornando mais sofisticadas e complexas.

Quadro 03 – Tipos de fraudes bancárias

Golpe	Descrição
Golpe do Pix Errado	O golpista simula ter enviado um Pix para a vítima por engano e solicita o reembolso do valor.
Golpe da Falsa Central de Atendimento	Criminosos se passam por atendentes de banco e pedem dados sensíveis para “corrigir” supostos problemas.
Golpe do Falso Motoboy	O golpista envia um motoboy à casa da vítima para recolher um cartão supostamente "clonado" ou "bloqueado".
Golpe da Troca de Cartão	Durante uma compra, o golpista troca o cartão da vítima por outro semelhante, ficando com o verdadeiro.
Golpe da Maquininha Quebrada	Em estabelecimentos, a máquina é manipulada para cobrar valores mais altos ou duplicados.
Golpe do Falso Leilão	Golpistas criam sites de leilão falso, onde as vítimas “compram” produtos que nunca são entregues.

ISSN: 2764-7226

Golpe do WhatsApp	Criminosos se passam por amigos ou familiares pedindo dinheiro urgente para resolver uma emergência.
Golpe do Link Falso	A vítima recebe links que simulam páginas de bancos ou serviços e, ao clicar, fornece dados ao golpista.
Golpe do Acesso Remoto ou Mão Fantasma	Golpista convence a vítima a instalar aplicativos de acesso remoto, assumindo controle do dispositivo.
Golpe do Falso Empréstimo	Oferecem empréstimos com condições vantajosas, mas pedem pagamento antecipado de "taxas".
Golpe do Falso Investimento	Prometem ganhos altos e rápidos em investimentos, captando dinheiro das vítimas e desaparecendo.
Golpe da Restituição do Imposto de Renda	Golpistas alegam ser da Receita Federal e pedem dados para "liberar" a restituição.

As fraudes tendem a ficar mais complexas com uso de inteligência artificial e combinação com técnicas de engenharia social, fazendo com que os bancos necessitem ampliar suas defesas e manter seus clientes informados para redução de ocorrências. (NETO, 2024).

Ao analisar as formas de prevenção de fraudes comunicadas para clientes nos grandes bancos no Brasil, verifica-se que os métodos são semelhantes, como a divulgação em sites dos bancos e propagandas nas mídias como televisão e redes sociais. Abaixo serão elencadas as formas de divulgação por cada banco.

Quadro 04 – Divulgação sobre segurança

ISSN: 2764-7226

Banco	Divulgação de Informações sobre Segurança e Prevenção de Fraudes
Caixa Econômica Federal	Informações no site caixa.gov.br/seguranca com cartilha de segurança e dicas de prevenção.
Banco do Brasil	Informações no site bb.com.br/seguranca com tipos de fraudes, vídeos explicativos, dicas de prevenção, podcast *Segurança em Rede*, e manual de segurança.
Itaú	Informações no site itau.com.br/seguranca com tipos de fraudes e e-mail específico para envio de suspeitas de fraudes.
Santander	Informações no site santander.com.br/seguranca com tipos de fraudes e dicas de prevenção.
Bradesco	Informações no site bradesco.com.br/seguranca com tipos de fraudes e dicas de prevenção.
Nubank	Informações no site nubank.com.br/seguranca com tipos de fraudes, dicas de prevenção e vídeos explicativos.

Todos os bancos com exceção do Nubank realizam propagandas na televisão sobre fraudes bancárias, porém, todos fazem divulgação em redes sociais de forma interativa para facilitar o entendimento dos clientes e usuários. Verifica-se que todos utilizam as mesmas formas de divulgação para os clientes que pode ser um fator que ajuda a entender o porquê das mesmas fraudes ocorrem em todos os bancos. Analisando a forma de comunicação no site, entende-se que o Nubank e Banco do Brasil utilizam mais recursos como vídeos explicativos para se comunicar com seus clientes.

Ao tentar entender porque algumas técnicas fraudulentas tem alta propensão de sucesso junto à clientes como o *phishing,* percebe-se que os clientes não possuem entendimento suficiente de indicadores da possibilidade de fraude. Em estudo realizado por Dhamija; Tygar; Hearst (2006) verificou-se que para aumentar a segurança do usuário é necessário criar interfaces que destaquem com maior facilidade os sinais de segurança, pois encontrou resultados de alta porcentagem de usuários que não percebe indicadores de segurança como a barra de endereços e o cadeado SSL, levando-os a cair em golpes.

Sob ótica diferente, em estudo no contexto holandês realizado por Junger; Montoya; Overink (2017) descobriu-se que avisos não são eficazes para que usuários não forneçam informações pessoais em situações de tentativas de fraudes já que tentativa de

interceder na situação de forma superficial é ineficaz e que uma forma mais eficaz seria a realização de treinamentos de forma mais profundas.

5. CONSIDERAÇÕES FINAIS

O presente estudo sobre fraudes bancárias no Brasil nos mostra um cenário complexo com o processo de digitalização que está avançando globalmente e sendo bastante evoluído no segmento de serviços financeiros aumentando a exposição de clientes e instituições financeiras em relação à segurança e confiança. A análise dos principais tipos de fraudes bancárias, especialmente as técnicas de *phishing* e engenharia social, e das estratégias de comunicação e prevenção adotadas pelas instituições financeiras demonstra que há espaço para inovações e melhorias. A uniformidade nas estratégias de divulgação apresenta uma oportunidade para métodos mais personalizados e interativos, objetivando a conscientização e capacitação dos clientes.

As fraudes bancárias impactam diretamente a rentabilidade dos bancos, mas possui um poder bem mais devastador na vida dos clientes, podendo mudar para sempre seu comportamento. Há necessidade das instituições financeiras investirem mais em ferramentas e manter um contato próximo com o cliente, melhorando cada vez mais a experiência e jornada do cliente. Concluindo, para que o setor bancário brasileiro permaneça em posição privilegiada é indispensável que a segurança dos canais digitais esteja em constante evolução. Não se pode focar em apenas divulgar em sites maneiras de se evitar ser vítima de fraudes, mas há a necessidade de estratégias educacionais para os clientes terem maiores condições de se defender. Com isso, os bancos não só fortalecerão suas relações com os clientes, mas também contribuirão para a promoção da inclusão digital no país.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ACCENTURE, 2023. Disponível em: HTTPS://VALOR.GLOBO.COM/CONTEUDO-DE-MARCA/ACCENTURE/NOTICIA/2023/06/26/BRASIL-E-PROTAGONISTA-NA-TRANSFORMACAO-DA-INDUSTRIA-FINANCEIRA-MUNDIAL.GHTML Acesso em 15/09/2024.

AGUAYO, F. Z; ŚLUSARCZYK, B. (2020) Risks Of Banking Services' Digitalization: The Practice Of Diversification And Sustainable Development Goals. Sustainability, V. 12, N. 10, P. 4040.

AMOH, J. K; AWUNYO-VITOR, D; OFORI-BOATENG, K. (2021). Customers' Awareness And Knowledge Level Of Fraudulent Acts In Electronic Banking In Ghana: Evidence From A Universal Bank. Journal Of Financial Crime, V. 28, N. 3, P. 870-882.

BACEN, 2024. Disponível em HTTPS://WWW.BCB.GOV.BR/DETALHENOTICIA/744/NOTICIA. Acesso em 20/10/2024.

BACEN, 2024. Disponível em HTTPS://WWW3.BCB.GOV.BR/RANKING/HISTORICO.DO. Acesso em 20/10/2024

CIALDINI, R.B. (2021). Influence: The Psychology Of Persuasion, Harper Business, Manhattan, Ny.

DHAMIJA, R; TYGAR, J. D; HEARST, M. (2006). Why Phishing Works. In: Proceedings Of The SIGCHI Conference On Human Factors In Computing Systems. Montréal, Quebec, Canada: ACM. P. 581-590

CRESWELL, J. W. (2007). Qualitative Inquiry And Research Design: Choosing Among Five Approaches (2nd Ed.). Thousand Oaks, Ca: Sage Publications.

DIENER, F. (2020) Empirical Evidence Of A Changing Operating Cost Structure And Its Impact On Banks' Operating Profit: The Case Of Germany. Journal Of Risk And Financial Management, V. 13, N. 10, P. 247.

DINO, 2024. Disponível em: HTTPS://VALOR.GLOBO.COM/PATROCINADO/DINO/NOTICIA/2024/05/17/FRAUDES-BANCARIAS-AUMENTAM-E-PREJUDICAM-CLIENTES-E-BANCOS.GHTML. Acesso em 15/09/2024.

FEBRABAN, 2024. Disponível em https://antifraudes.febraban.org.br/. Acesso em 01/10/2024.

GAMBLE, K. J; BOYLE, P; YU, L; BENNETT, D. (2014) The Causes And Consequences Of Financial Fraud Among Older Americans. Chestnut Hill, Ma: Center For Retirement Research At Boston College, 2014

GRANGER, S. (2001) Social Engineering Fundamentals, Part I: Hacker Tactics. Securityfocus.

HOFFMANN, A. O. I.; BIRNBRICH, C. (2012). The Impact Of Fraud Prevention On Bank-Customer Relationships: An Empirical Investigation In Retail Banking. International Journal Of Bank Marketing, V. 30, N. 5, P. 390-407.

IBM, 2024. Disponível em HTTPS://WWW.IBM.COM/BR-PT/TOPICS/PHISHING. Acesso em 22/09/2024.

JADWANI, B; PARKHI, S; MITRA, P. K. (2024). Operational Risk Management In Banks: A Bibliometric Analysis And Opportunities For Future Research. Journal Of Risk And Financial Management, V. 17, P. 95.

JUNGER, M.; MONTOYA, L.; OVERINK, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, v. 66, p. 75-87.

KASSEM, R. (2024). HOW FRAUD IMPACTS INDIVIDUALS' WELLBEING – ACADEMIC INSIGHTS AND GAPS. JOURNAL OF FINANCIAL CRIME, V. 31, N. 5, P. 1261-1268, 2024.

KROMBHOLZ, K. HOBEL, H.; HUBER, M.; WEIPPL, E. (2015), ADVANCED SOCIAL ENGINEERING ATTACKS. JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, V. 22, P. 113-122.

ARAUJO, M. L (2024). Disponível em: HTTPS://WWW.CNNBRASIL.COM.BR/ECONOMIA/MACROECONOMIA/PIX-DEVE-IMPULSIONAR-PIB-DO-BRASIL-EM-R-2807-BILHOES-ATE-2028-APONTA-ESTUDO/?HIDEMENU=TRUE#:~:TEXT=O%20PIX%2C%20SISTEMA%20DE%20PAGAMENTO,FOR%20ECONOMICS%20AND%20BUSINESS%20RESEARCH. Acesso em 20/10/2024

MISHRA, S. (2023). EXPLORING THE IMPACT OF AI-BASED CYBER SECURITY FINANCIAL SECTOR MANAGEMENT. APPLIED SCIENCES, 13(10), 5875.

NETO, 2024. Disponível em: https://exame.com/bussola/5-tendencias-preocupantes-em-fraudes-bancarias-em-2024/ Acesso em 07/08/2024.

WELLS, J.T. (2011), CORPORATE FRAUD HANDBOOK: PREVENTION AND DETECTION, 3RD ED., JOHN WILEY AND SONS, HOBOKEN, NJ.

ISSN: 2764-7226