UNIVERSIDADE FEDERAL DE VIÇOSA

DEPARTAMENTO DE ECONOMIA RURAL

TRABALHO DE CONCLUSÃO DE CURSO

JOÃO PEDRO RABELO DE CARVALHO

GOLPES FINANCEIROS E O SISTEMA FINANCEIRO NACIONAL

VIÇOSA, MINAS GERAIS

2023

JOÃO PEDRO RABELO DE CARVALHO

GOLPES FINANCEIROS E O SISTEMA FINANCEIRO NACIONAL

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Viçosa como exigência para aprovação na disciplina de ERU 489, TCC II.
Orientador: Professor Brício dos Santos Reis

VIÇOSA, MINAS GERAIS

2023

AGRADECIMENTOS

Ao meu orientador, professor Brício dos Santos Reis pela disponibilidade e colaboração;
Ao meu avô, Enuque Dias de Carvalho pelas orações e torcida inabalável.

RESUMO

A informação é um dos recursos mais valiosos, tanto para indivíduos quanto para organizações. Este trabalho, compreende-se como uma ferramenta de informação, essencial para compreender os principais ataques de engenharia social nas Instituições Financeiras. Inicialmente, a pesquisa buscou identificar artigos relacionados à engenharia social, apresentando, em seguida, as principais formas de ataques desse tipo, para isso, foi realizada uma pesquisa exploratória, com o intuito de elucidar o problema em questão com a abordagem qualitativa, uma vez que busca uma compreensão não numérica dos temas estudados. A contribuição teórica reside na exposição dos diversos tipos de ataques, que merecem atenção como objeto de estudo. A contribuição prática é alertar os usuários e clientes sobre os possíveis ataques de engenharia social.

Palavras-chave: Segurança da Informação, Engenharia Social, Sistema Financeiro, Golpes, Phishing.

ABSTRACT

Information is one of the most valuable resources, both for individuals and organizations. This work is understood as an informational tool essential for comprehending the main social engineering attacks in financial institutions. Initially, the research sought to identify articles related to social engineering, subsequently presenting the main forms of such attacks. To achieve this, an exploratory research was conducted, aiming to clarify the issue at hand with a qualitative approach, as it seeks a non-numeric understanding of the studied topics. The theoretical contribution lies in exposing the various types of attacks, which deserve attention as a subject of study. The practical contribution is to alert information about potential social engineering attacks.

Keywords: Information Security, Social Engineering, Financial System, Scams, Phishing.

SUMÁRIO

1. INTRODUÇÃO 7

1.1. O PROBLEMA E SUA IMPORTÂNCIA 8
2. OBJETIVOS 9
2.1. OBJETIVO GERAL 9
3. FUNDAMENTAÇÃO TEÓRICA 10
3.2. SEGURANÇA DA INFORMAÇÃO 11
3.3. A ENGENHARIA SOCIAL 12
3.4. FRAUDES FINANCEIRAS 13
4. METODOLOGIA 14
5. RESULTADOS E DISCUSSÃO 15
5.1. A CARACTERIZAÇÃO DO GOLPE PARA A ENGENHARIA SOCIAL 15
5.1.1. PHISHING 16
5.1.2. SMISHING 16
5.1.3. VISHING 17
5.1.4. SPAM 17
5.1.5. PHARMING 18
5.2. OS GOLPES BANCÁRIOS NO SISTEMA FINANCEIRO BRASILEIRO 18
6. REFERÊNCIAS 28

1. INTRODUÇÃO

Nos últimos anos, a popularização da internet banking, impulsionada pela globalização e pelos avanços tecnológicos, tem se manifestado de maneira notável. O internet banking, definido como a oferta de serviços bancários eletrônicos, predominantemente por meio de computadores pessoais (PCs) e outros dispositivos conectados à Internet (GKOUTZINIS, 2019), experimentou uma rápida evolução. A velocidade e o progresso no fornecimento de serviços bancários pela internet propiciaram a transição do acesso via internet banking para o

acesso por meio do mobile banking. Este último se caracteriza principalmente pela oferta de serviços bancários através de dispositivos móveis, como celulares, smartphones e tablets (LIN, 2018; YU, 2016).

A transição dos serviços bancários para a internet representa um marco significativo na evolução do setor financeiro para instituições bancárias e não bancárias. Para os usuários, foi possível testemunhar uma alteração progressiva no paradigma, estimulada pela cada vez mais ampla adoção da internet e pelas inovações tecnológicas. Nesse contexto, ocorreu a transição das práticas bancárias convencionais, como consultas de saldo, transferências e pagamentos, das estruturas físicas das agências para os ambientes virtuais das plataformas online, como os aplicativos.

O avanço tecnológico e as mudanças ágeis nas demandas dos clientes desempenham um papel crucial no estímulo ao crescimento do setor bancário, promovendo a criação de novos produtos e serviços direcionados para atendimento em larga escala. Essa evolução tem reduzido a necessidade da presença física dos clientes nas agências para a realização de operações. Ou seja, as instituições financeiras só estão na internet porque as pessoas estão na internet.

O crescente número de transações bancárias realizadas por meio do internet banking e mobile banking tem sido acompanhado por um aumento significativo nas fraudes bancárias eletrônicas contra as instituições financeiras (PATROCÍNIO, 2018). Diante desse cenário, as autoridades públicas, por meio de suas forças de segurança, precisam manter uma vigilância constante sobre a evolução e diversificação das atividades criminosas. É crucial acompanhar e aprimorar suas estratégias conforme os agentes criminosos ajustam seus comportamentos de maneira inadequada à conduta social. Isso implica enfrentar os desafios proporcionados pela tecnologia, o volume crescente de informações e a popularização contínua dos serviços oferecidos aos usuários do sistema bancário por meio da internet.

A vantagem do investimento nos espaços da Internet é simples, anualmente, o número de utilizadores de smartphones, tablets e outros dispositivos móveis está em constante crescimento. Seja para trocar mensagens, utilizar as redes sociais, usar para trabalho ou entretenimento, é inegável que essa tecnologia ocupa um espaço de considerável relevância no cotidiano da maior parte dos brasileiros.

Assim, com uma cartela extensa de possibilidades que a internet permite às Instituições Financeiras, existem numerosas ameaças que exploram as vulnerabilidades inerentes à internet e às suas tecnologias. Esse terreno fértil de desenvolvimento, propiciado pela digitalização das instituições financeiras e pela maior impessoalidade na relação com o cliente, vem acompanhada de múltiplas modalidades de golpes contra os correntistas desses

estabelecimentos. Isso resulta na exigência de reforçar significativamente a segurança no setor bancário, dada a sua crescente relevância no cotidiano dos clientes.

As Instituições Financeiras brasileiras vêm enfrentando diversas práticas ilegais realizadas por indivíduos ou grupos a fim de roubar informações ou dinheiro de maneira fraudulenta chamadas de Fraudes Externas. Essas práticas ilegais tomam maiores proporções com o alcance ilimitado da internet e sua pouca segurança. O crescimento do número de casos de fraudes e golpes externos bancários é cada vez mais reportado às autoridades competentes e isso expõe as instituições financeiras à desconfiança e medo por parte dos usuários.

1.1. O PROBLEMA E SUA IMPORTÂNCIA

Os incidentes de golpes financeiros que utilizam técnicas de Engenharia Social, como mencionado anteriormente, estão em constante crescimento. Houve um aumento significativo de 165% no primeiro semestre de 2021 em comparação com o segundo semestre de 2020, como relatado por (CRESCEM..., 2021). Esses golpes têm causado danos devastadores às vítimas e suas famílias, frequentemente resultando em consequências irreparáveis.

Para as instituições bancárias, esses golpes têm causado danos à sua reputação e à confiança, elementos cruciais para a manutenção de seus negócios. Embora várias instituições tenham implementado medidas visando a prevenção desses golpes, segundo DINIZ (2021), tais ações se revelaram insuficientes. Além disso, há uma escassez de publicações nacionais relacionadas às vítimas de golpes financeiros, bem como às práticas adotadas pelas instituições bancárias para enfrentar esse problema. Isso pode ser atribuído à possibilidade de essas instituições optarem por não divulgar suas estratégias de combate a essas ameaças por razões de confidencialidade.

Um estudo sobre vítimas de fraudes e golpes financeiros realizado por Kadoya et al. (2021), identificou que o perfil das vítimas varia conforme o tipo de golpe, indicando que uma abordagem uniforme não é eficaz na luta contra a fraude e ainda ressalta a importância de uma estratégia de comunicação em massa. Com as novas tecnologias, desenvolvem-se cada vez mais, novas maneiras para práticas prejudiciais. Com a internet, por exemplo, é possível maior alcance de aplicações de golpes, sobretudo os de cunho financeiro, por isso, relatar os golpes e o modo de aplicação deles se faz muito importante.

2. OBJETIVOS

2.1. OBJETIVO GERAL

O objetivo geral desta pesquisa é identificar e relatar os principais golpes bancários externos que acometem as Instituições Financeiras brasileiras e expõem certos desafios ao Sistema Financeiro Nacional.

Especificamente, pretende-se:

- Descrever e analisar os principais e mais comuns tipos de fraudes financeiras contra pessoas físicas e jurídicas;

- Descrever esses golpes, as abordagens, os perfis das vítimas e suas competências;

- Identificar problemáticas que sustentam a existência dos golpes financeiros no Brasil.

3. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os principais conceitos para a compreensão do tema, uma vez que o assunto golpe financeiro envolve categorias técnicas como a segurança da informação e a engenharia social.

3.1. O SISTEMA FINANCEIRO NACIONAL

O Sistema Financeiro Nacional (SFN) pode ser descrito como um conjunto de instituições financeiras cuja função primordial é facilitar a transferência de recursos dos agentes poupadores para os agentes tomadores, impulsionando, dessa forma, o crescimento econômico. A função desempenhada por esse sistema é evidente tanto em termos econômicos quanto sociais. A intermediação financeira, que permite a alocação eficiente de recursos excedentes dos poupadores nas mãos dos agentes tomadores para financiar projetos de investimento, resulta em benefícios para todos os participantes desse mercado. Os poupadores recebem rendimentos como contrapartida aos empréstimos, enquanto os tomadores conseguem desenvolver e operar suas atividades e projetos.

Conforme Assaf Neto (2011, p. 37), a necessidade de compreender o SFN tem aumentado ao longo do tempo devido à importância do setor empresarial em uma economia e à crescente complexidade de suas operações. A evolução histórica do Sistema Financeiro Nacional é segmentada em quatro fases, que serão discutidas posteriormente. O objetivo

primordial do SFN, de acordo com Faria (2003, p. 1), é facilitar a aproximação entre tomadores e aplicadores de recursos da maneira mais segura, objetiva e transparente possível. A estrutura do SFN proporciona segurança e agilidade nas operações de troca de recursos, oferecendo opções diversas para a alocação desses recursos, promovendo, assim, o desenvolvimento equilibrado do país.

Assaf Neto (2003, p. 74) acrescenta que o SFN viabiliza a relação entre agentes que necessitam de recursos para investimentos e agentes capazes de gerar poupança e, por conseguinte, financiar o crescimento econômico. Considerando que a maior parte do dinheiro que circula no SFN está nos bancos, que representam uma parte crucial do sistema, todas as atividades econômicas são, inevitavelmente, direcionadas por meio deles (FARIA, 2003, p.1). Dessa forma, os bancos oferecem uma variedade de produtos financeiros para movimentar esse fluxo financeiro, incluindo produtos para tomadores de recursos, como empréstimos para capital de giro, e produtos para agentes aplicadores de recursos, como a caderneta de poupança. Em resumo, é um conjunto de instituições responsáveis pela captação de recursos financeiros, pela distribuição e circulação de valores e pela regulação de processos. Na próxima seção, conheceremos um pouco da sua origem e da sua evolução histórica.

O SFN é dividido em dois grandes subsistemas: o normativo e o de intermediação. O subsistema normativo é encarregado de supervisionar e regulamentar as atividades do mercado financeiro e de suas instituições. Essas funções são desempenhadas pelo Conselho Monetário Nacional (CMN) e pelo Banco Central do Brasil (BACEN). A Comissão de Valores Mobiliários (CVM) desempenha um papel de apoio como órgão normativo, concentrando-se especialmente no controle e fiscalização do mercado de valores mobiliários, incluindo ações e debêntures. Além disso, três outras instituições financeiras com funções especiais no mercado financeiro integram esse sistema: Banco do Brasil (BB), Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e Caixa Econômica Federal (CEF).

Já os bancos múltiplos são considerados instituições bancárias. Essas instituições são constituídas obrigatoriamente como sociedades anônimas e compreendem os bancos comerciais, os múltiplos e as caixas econômicas. Eles compõem o Sistema Financeiro Nacional.

3.2.SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é a prática de proteger informações contra acesso não autorizado, divulgação, alteração ou destruição. Os principais conceitos que configuram a segurança da informação são a Confidencialidade, que visa garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis, a Integridade, compreende em manter a

precisão e a integridade das informações, prevenindo alterações não autorizadas; e por fim, a Disponibilidade, que significa assegurar que as informações estejam acessíveis quando necessário, evitando interrupções não planejadas. Esses conceitos visam proteger dados valiosos e sistemas de informação contra ameaças e riscos cibernéticos, como situa Benetti (2015).

À medida que o controle e as restrições para acessar informações aumentam, de acordo com Silva (2011), o nível de desconforto do usuário tende a crescer. Esse desconforto está correlacionado diretamente com o nível de segurança, podendo comprometer a segurança, dependendo das reações dos usuários e das medidas adotadas pelas organizações.

Antes de iniciar qualquer estratégia de segurança, é crucial compreender o que estamos resguardando e contra o que estamos protegendo. A segurança da informação é alcançada por meio da aplicação de um conjunto apropriado de controles, políticas, processos, procedimentos e estruturas organizacionais. Esses controles devem ser estabelecidos, implementados, monitorados, revisados e aprimorados conforme necessário, assegurando que os objetivos de segurança da organização sejam devidamente atendidos (ROMUALDO, 2020).

A confidencialidade garante que a informação seja protegida contra acessos não autorizados. Isso é feito por meio de um controle de acesso rigoroso, permitindo o acesso apenas a pessoas autorizadas. A implementação de políticas que reforçam a confidencialidade inclui restrições de acesso com base na hierarquia dos funcionários e a limitação do acesso a dados específicos de acordo com as necessidades de cada setor (SOUZA, 2022).

No que diz respeito à Integridade, ela assegura que as informações permaneçam na sua forma original, conforme criadas pelo autor, e estejam resguardadas contra qualquer alteração não autorizada. Isso implica que as informações devem ser sempre precisas e completas quando acessadas. Qualquer modificação indevida em um dado é considerada uma perda de integridade, podendo acarretar consequências significativas e prejuízos (FINKLER; AMARAL, 2022).

Os fundamentos essenciais em qualquer programa de Segurança da Informação são representados pelos pilares conhecidos como a tríade CIA, composta por confidencialidade, integridade e disponibilidade (SOUZA, 2022).

Segundo Costa (2019), a segurança das informações cada vez mais está fragilizada por conta da diversificação de ações de engenharia social, citadas nos próximos tópicos.

3.3. A ENGENHARIA SOCIAL

De acordo com a definição de Costa (2019), os engenheiros sociais são indivíduos com a habilidade de manipular a confiança de outras pessoas a fim de obter acesso a informações

privadas. A definição do termo "engenharia social" sugere um conceito literal em que "engenharia" refere-se à construção de algo e "social" envolve interações com pessoas, ocorrendo em um ambiente específico. Ainda segundo Costa (2019) essa construção está relacionada ao desenvolvimento de táticas para acessar informações que não estão naturalmente disponíveis, explorando vulnerabilidades comportamentais das pessoas. O engenheiro social utiliza artifícios como o engano, influência e persuasão para adquirir informações comerciais ou pessoais, explorando as vulnerabilidades de potenciais vítimas. O objetivo é obter dados relevantes e que possibilitem o acesso não autorizado a sistemas de valor e às informações armazenadas neles, como contas bancárias.

Clientes de instituições financeiras são crescentemente atingidos por este fenômeno, fornecendo informações confidenciais, como dados pessoais, senhas e até mesmo entregando seus cartões para os criminosos (DINIZ, 2021). Estes criminosos aproveitam das fragilidades na segurança de informações e nas bases de dados e aprofundam no processo de persuasão até conseguir subtrair algum recurso da vítima (DINIZ, 2021).

3.4. FRAUDES FINANCEIRAS

Conforme Fligstein e Roehrkasse (2013, citados por REURINK, 2018), a fraude pode ser definida como a falsificação e manipulação ilegal de informações financeiras. Nas transações financeiras, a importância das informações e do entendimento para interpretá-las é crucial. Assim, para proteger os participantes que não possuem esse conhecimento, as autoridades estabelecem regras e leis (REURINK, 2018).

Ainda segundo Reurink (2018), fraudes são as ações e declarações através das quais os participantes do mercado financeiro desinformam ou ludibriam outros participantes, fornecendo intencional ou imprudentemente informações falsas, incompletas ou manipuladoras sobre bens financeiros, serviços ou oportunidades de investimento de uma maneira que viole qualquer disposição legal, seja ela uma norma regulatória, lei estatutária, direito civil ou direito penal.

Normalmente, o uso de divulgações financeiras falsas tem dois objetivos: elas podem ser empregadas para encobrir a má utilização, ou apropriação indevida ou a aplicação indevida de fundos em uma organização, ou então, por parte dos administradores, para iludir investidores ou reguladores sobre o desempenho financeiro de um negócio. Declarações falsas de uma organização podem surgir em apresentações, relatórios financeiros, entre outros. Dado o caráter das demonstrações financeiras, as divulgações financeiras falsas feitas por uma organização são geralmente tratadas como fraude contábil.

O segundo tipo, Golpes Financeiros (financial scams), é caracterizado por esquemas totalmente fraudulentos nos quais os golpistas, muitas vezes utilizando identidades falsas ou inspirando confiança, persuadem as pessoas a interagirem voluntariamente com eles, resultando na entrega de fundos ou informações sensíveis relacionadas às finanças pessoais. Ao contrário do primeiro tipo, não há uma base legítima por trás dos golpes financeiros; eles se sustentam apenas por meio de um jogo de confiança. Esse segundo tipo de golpe é o que esse trabalho desenvolve os conceitos.

4. METODOLOGIA

Neste capítulo são apresentados os procedimentos metodológicos da pesquisa, especificando sua caracterização e os procedimentos adotados para sua execução.

Este trabalho adotará a abordagem de pesquisa qualitativa, uma vez que busca uma compreensão não numérica dos temas estudados. Conforme Alyrio (2009) explica, a pesquisa qualitativa consiste no estudo de um objeto com o objetivo de interpretá-lo em termos de seu significado. Nesse contexto, a análise prioriza a subjetividade do pesquisador, visando considerar a totalidade em vez de dados ou aspectos isolados. Assim, na pesquisa qualitativa, a abordagem aos dados é interpretativa, com uma propensão maior à interferência da subjetividade do pesquisador, caracterizando-se pela reflexividade.

Além disso, a abordagem qualitativa preocupa-se em analisar e interpretar aspectos mais profundos, descrevendo a complexidade do comportamento humano e fornecendo uma análise mais detalhada sobre investigações, hábitos, atitudes, tendências de comportamento, entre outros.

Sampieri, Collado e Lucio (2013) citados por Marconi e Lakatos (2022) destacam que o enfoque quantitativo volta-se para a descrição, previsão e explicação, enquanto o enfoque qualitativo concentra-se na exploração, descrição e entendimento do problema. Alyrio (2009) adiciona que a pesquisa pode ser classificada quanto ao grau de aplicação mais ou menos imediata de seus resultados, sendo classificada como pesquisa pura ou aplicada. Simon (1969) apud Alyrio (2009) define a pesquisa pura como aquela cujos resultados se situam em um futuro remoto, sem aplicação imediata, enquanto a pesquisa aplicada visa resultados rápidos.

Segundo Marconi e Lakatos (2022), a pesquisa básica é voltada para a aquisição e ampliação de novos conhecimentos, sem uma finalidade específica de resolver questões práticas, enquanto a pesquisa aplicada busca resolver um problema específico. Quanto à natureza da pesquisa deste trabalho, ela se enquadrará como pesquisa básica ou pura, não visando aplicação imediata ou solução para um caso específico.

No que diz respeito à classificação quanto aos objetivos, a pesquisa adotará uma abordagem exploratória, com o intuito de elucidar o problema em questão. De acordo com Gil (2002), a pesquisa exploratória visa proporcionar uma maior familiaridade com o problema, tornando-o mais explícito ou gerando hipóteses. Essas pesquisas têm como objetivo principal aprimorar ideias ou fazer descobertas intuitivas.

Na pesquisa exploratória, conforme Gil (2017) citado por Marconi e Lakatos (2022), a coleta de dados pode incluir levantamento bibliográfico, entrevistas com especialistas no assunto e análise de exemplos. Segundo Severino (2013), a pesquisa exploratória busca levantar informações sobre um determinado objeto, delimitando assim um campo de trabalho e mapeando as condições de manifestação desse objeto. O autor indica que a pesquisa exploratória prepara o terreno para a pesquisa explicativa, que procura identificar as causas dos fenômenos estudados, seja por meio de métodos experimentais/matemáticos, seja por meio de métodos qualitativos.

O procedimento adotado será o da pesquisa bibliográfica, que busca e analisa o que a literatura e outras fontes de informação apresentam e explicam sobre as temáticas em estudo.

De acordo com Lakatos (2021), a pesquisa bibliográfica ou de fontes secundárias abrange todo o conteúdo já criado e publicado sobre um determinado tema, incluindo artigos científicos, livros, jornais, revistas e meios de comunicação oral. Nesse sentido, Alyrio (2009) destaca que esse tipo de pesquisa deve abranger o máximo possível da bibliografia de domínio público relacionada ao assunto estudado, considerando livros, publicações avulsas, boletins, jornais, revistas, monografias, dissertações, teses, entre outros. Alyrio enfatiza que a pesquisa bibliográfica é o alicerce que sustenta todo o plano de investigação, permitindo que o pesquisador se atualize sobre o tema indicado e amplie seus conhecimentos teóricos e intelectuais, promovendo uma abordagem reflexiva e crítica sobre o assunto estudado.

5. RESULTADOS E DISCUSSÕES

5.1. A CARACTERIZAÇÃO DO GOLPE PARA A ENGENHARIA SOCIAL

Para Koch (2022), o primeiro passo para categorizar e compreender o mecanismo da engenharia social é descrever seu método de funcionamento. Os diagnósticos dos golpes são descritos na lei 14.155 de 2021. Acrescentados os conceitos científicos, frutos da pesquisa bibliográfica, os tópicos podem ser definidos.

5.1.1. PHISHING

O termo Phishing, ou “pescaria” em livre tradução, se refere a uma forma de cibercrime em que os criminosos tentam enganar as pessoas para que revelem informações pessoais, financeiras ou confidenciais, como senhas, números de cartão de crédito, informações bancárias e outras informações sensíveis. Isso é geralmente feito fazendo-se passar por uma entidade confiável ou legítima, como um banco, uma empresa ou um serviço online. Essa prática tem como objetivo manipular as emoções dos usuários, como o medo, levando-os a realizar ações solicitadas, como, por exemplo, preencher informações em uma página de login falsa de sites populares, como Facebook, Email, plataformas de leilões e serviços de pagamento online.

Segundo Castro (2018), um engenheiro social envia essas mensagens para um usuário comum por meio de e-mails ou páginas na web como ponto de partida para um ataque. Essas mensagens e sites são meticulosamente projetados para se assemelharem aos legítimos, tornando extremamente difícil detectar a tentativa de golpe. Um exemplo típico envolve um e-mail que solicita que o usuário execute determinadas ações, como "Você está prestes a exceder sua capacidade de armazenamento" ou "clique aqui para manter sua conta ativa". Quando o usuário clica ou fornece as informações solicitadas, os dados do usuário são imediatamente capturados e enviados para o engenheiro social.

5.1.2. SMISHING

O smishing é uma forma de ataque cibernético com o mesmo propósito do tópico anterior, o phishing, porém, essa técnica envolve o uso de mensagens de texto, o formato SMS para realizar atividades de phishing, com o objetivo de enganar e manipular as vítimas a fim de obter informações pessoais ou financeiras.

Scheffler (2018), descreve dois principais métodos empregados nos golpes de smishing. No primeiro método, a vítima recebe uma mensagem de texto que aparenta ser proveniente de uma fonte conhecida e confiável, como seu banco ou o administrador de sistemas. No segundo método, a vítima recebe uma mensagem de texto alertando sobre a suposta perda de identidade ou o congelamento de sua conta.

Em seguida, os golpistas direcionam a vítima para um site ou número de telefone, alegando que é necessário verificar as informações da conta. Uma vez que os golpistas obtêm essas informações, eles podem realizar transações não autorizadas na conta da vítima ou até mesmo abrir um novo cartão de crédito em seu nome. Outra tática utilizada pelos criminosos que praticam o smishing é ameaçar a vítima e começar a cobrar tarifas diárias pelo suposto uso de um serviço, caso ela não clique em um link e forneça as informações pessoais solicitadas.

5.1.3. VISHING

O termo Vishing é uma combinação das palavras "voice" (voz) e phishing, e refere-se a uma técnica de fraude que envolve a utilização de chamadas telefônicas de voz para enganar as vítimas e obter informações pessoais, financeiras ou confidenciais. Assim como no phishing tradicional, os criminosos que praticam o vishing tentam se passar por entidades legítimas, como bancos, empresas de cartão de crédito, agências governamentais ou outras organizações confiáveis, para convencer as vítimas a fornecer informações sensíveis. Para Scheffler (2018), a chamada de voz cria uma sensação de urgência para que o usuário tome medidas e faculte informações adicionais.

Os golpistas que praticam o vishing muitas vezes utilizam táticas de persuasão e intimidação para induzir as vítimas a revelar informações pessoais, como números de cartão de crédito, senhas, números de seguro social ou outras informações de identificação. Eles podem alegar que há um problema urgente com a conta da vítima ou uma situação crítica que requer uma resposta imediata.

5.1.4. SPAM

Existem algumas interpretações divergentes quanto ao significado da palavra "SPAM", mas a mais amplamente aceita é que se trata de uma sigla para o termo "Sending and Posting Advertisement in Mass", que, em uma tradução livre, se refere a "Enviar e Publicar Anúncios em Massa", como descreve Alencar (2018). Dessa forma, "spam" é a expressão empregada para descrever mensagens eletrônicas que são encaminhadas sem a sua autorização e, frequentemente, são direcionadas a um grande número de destinatários.

Esse tipo de e-mail indesejado consiste, predominantemente, em propagandas. Nesse contexto, o spam também é chamado de "Mensagem Comercial Não-Solicitada". Entretanto, em situações distintas, essas mensagens podem conter conteúdos mais nocivos, como vírus, e até mesmo obter informações pessoais, como dados bancários, por exemplo.

Conforme destacado por Scheffler (2018), no Brasil, o envio de spam ainda não é considerado um crime, mas esse tema está atualmente em discussão no Senado e pode ser objeto de uma futura legislação. Apesar de ainda não haver uma proibição oficial, a prática do spam é, de fato, regulamentada de maneira indireta, uma vez que aqueles que a praticam são mal vistos, sua empresa ou produto perde credibilidade e seu provedor de serviços, domínio ou endereço IP pode ser incluído em listas de bloqueio mantidas por administradores de redes. É

por isso que, na maioria das vezes, o envio de spam está associado a atividades criminosas ou à falta de conhecimento por parte do empreendedor.

5.1.5. PHARMING

Outra phishing que não depende do envio de e-mails, mensagens ou ligações tem direcionado navegadores da web dos usuários para sites falsos. Essa categoria de crime é conhecida como pharming. Entretanto, em situações distintas, essas mensagens podem conter conteúdos mais nocivos, como vírus, e obter informações pessoais, como dados bancários, por exemplo.

O pharming funciona de maneira semelhante ao phishing, enganando os usuários para que acreditem que estão acessando um site legítimo, quando, na realidade, não estão. No entanto, ao contrário do phishing, que pode ser evitado por usuários mais atentos que não respondem a e-mails fraudulentos, o pharming é praticamente indetectável por um usuário comum da Internet, a menos que possua conhecimentos técnicos mais avançados. Nesse tipo de golpe, os criminosos exploram a disseminação de software malicioso que modifica o funcionamento do navegador da vítima. Quando a vítima tenta acessar um site, como o de um banco, por exemplo, o navegador comprometido a redireciona para um site falso que se parece visualmente com o site legítimo.

No imaginário popular, as ligações de presídios já são ameaças comuns, mas os outros mecanismos de engenharia social nem sempre são conhecidos, o que viabiliza discursos que popularizam a prevenção e detecção de ameaças.

5.2. OS GOLPES BANCÁRIOS NO SISTEMA FINANCEIRO BRASILEIRO

A sociedade brasileira enfrenta frequentemente o desafio da insegurança pública que permeia todo o território nacional. Indivíduos que saem de suas casas carregam o receio de não retornar com os bens conquistados com esforço, juntamente com o temor de serem vítimas de agressões ou até mesmo de perderem suas vidas, o bem mais valioso que um ser humano possui. Essa insegurança se estende à internet e às redes sociais. Para Diniz (2022) o vazamento de dados bancários, golpes com clientes de bancos digitais, e engenharias sociais nas mais diversas instituições financeiras vem se intensificando e se tornando motivo de desconfiança dos usuários com o banco. A pesquisa conduzida por Guerra, Oleto e Peñaloza (2018) evidenciou que a satisfação desempenha um papel crucial na variação da fidelidade do cliente bancário em ambientes de atendimento por múltiplos canais e que a confiança do cliente com a instituição financeira é o item vital para essa fidelidade.

Conforme DINIZ (2021), as medidas de prevenção contra golpes têm se revelado ineficazes, visto que as ocorrências dessas fraudes continuam em ascensão. Em consonância, em 10 de setembro de 2021, o até então ministro da Justiça e Segurança Pública, Anderson Torres, e o ex presidente da Federação Brasileira de Bancos (FEBRABAN), Isaac Sidney, realizaram um encontro para debater a implementação de uma Estratégia Nacional de Combate ao Crime Cibernético (FEBRABAN..., 2021).

Portanto, é observável uma escassez de estudos sobre os golpes financeiros que empregam a Engenharia Social, havendo uma carência de publicações nacionais a respeito, apesar de ser uma questão contemporânea séria que resulta em danos significativos tanto para as vítimas quanto para as instituições bancárias.

Compreender quais são os principais golpes bancários e o perfil das vítimas pode contribuir para uma compreensão deste problema e a identificação de ameaças. Na tabela a seguir, descrevo alguns desses golpes.

Ao discutir os desafios apresentados pelos crimes cibernéticos, é crucial destacar a natureza intrínseca desses delitos, os quais estão intimamente ligados à dependência do suporte proporcionado pelos sistemas informáticos. Nesse contexto, a violação do bem jurídico crucial, que são os dados, revela-se como uma faceta inevitável dessas práticas delituosas.

TABELA 1: Tipos de Golpes Financeiros

GOLPE DA TROCA DE CARTÃO	Um golpista se passa por atendente bancário, por mensagem no WhatsApp ou SMS, informa um erro com o cartão, que pode estar antecedido de falsas cobranças, oferece assistência à vítima e, ao final, substitui o cartão da vítima por outro, ficando com o original.

GOLPE DO CARTÃO NÃO PRESENTE	Ocorre quando os detalhes do cartão são copiados, por exemplo, durante uma transação presencial, e posteriormente são empregados em compras online pelos criminosos.
GOLPE DO FALSO MOTOBOY	Pessoas se fazem passar por funcionários de alguma instituição financeira, alegando ter havido uma fraude em seu cartão de crédito ou débito. Normalmente, possuem informações cadastrais precisas para parecer uma ligação legítima, informações muitas vezes simples encontradas em banco de dados frágeis.
GOLPE DA RETENÇÃO DE CARTÃO	Golpe onde, por vezes, golpistas aplicam uma substância adesiva ou colante no local de inserção dos cartões nos caixas eletrônicos, prendendo o cartão. Ao perceber o problema, o golpista oferece ajuda ao cliente, disponibilizando um telefone celular supostamente conectado diretamente ao banco.

GOLPE DO BILHETE PREMIADO	Este golpe foi mais comum no início da década, onde os criminosos desempenham diferentes papéis e, por meio de uma encenação muito elaborada e convincente, persuadem a vítima de que possuem um bilhete premiado na Loteria de alto valor.
GOLPE DO WHATSAPP	Criminosos identificam o número de celular e o nome da vítima para clonar a conta do WhatsApp do usuário. Eles registram a conta nos próprios celulares, mas precisam inserir um código de segurança enviado via SMS. Então, os criminosos enviam mensagens pelo WhatsApp, fingindo ser do suporte ao cliente de um site de vendas ou empresa em que a vítima está cadastrada, solicitando o código de segurança sob pretexto de atualização, manutenção ou confirmação de cadastro.

GOLPE DO LINK FALSO	Um exemplo de Phishing muito comum, na qual citamos neste trabalho tem como objetivo fisgar vítimas a fim de roubar suas informações, é frequentemente realizado por engenheiros sociais fraudadores. Eles conseguem senhas e dados pessoais ao enviar links por meio de mensagens em e-mails, SMS, WhatsApp e redes sociais.
GOLPE DO FALSO CANCELAMENTO DE EMPRÉSTIMO	Este golpe também é muito comum no Brasil, e se desenrola quando o fraudador, através de contato telefônico ou, principalmente, via WhatsApp, se faz passar por um funcionário do banco.
GOLPE DO FALSO BOLETO	Neste tipo de golpe, o criminoso já possui informações pessoais da vítima e pode encaminhar um boleto falso, simulando ser uma correspondência bancária ou de uma loja física ou online. Esses boletos são enviados por e-mail, SMS ou WhatsApp e se assemelham bastante aos originais, porém o valor indicado é redirecionado para a conta do golpista.

GOLPE DO DELIVERY	Outro golpe bem atual, com alta incidência na pandemia, é o golpe onde o cliente faz um pedido através de um aplicativo e, ao receber a entrega, o golpista usa uma máquina com o visor danificado ou de alguma forma impede que o cliente verifique o valor a ser pago.
GOLPE DA TROCA DE CARTÃO	Um golpista se passa por atendente bancário, por mensagem no WhatsApp ou SMS, informa um erro com o cartão, que pode estar antecedido de falsas cobranças, oferece assistência à vítima e, ao final, substitui o cartão da vítima por outro, ficando com o original.
GOLPE DO CARTÃO NÃO PRESENTE	O clássico Golpe do Cartão Não Presente ocorre quando os detalhes do cartão são copiados, por exemplo, durante uma transação presencial, e posteriormente são empregados em compras online pelos criminosos.

GOLPE DA FALSA CENTRAL DE ATENDIMENTO	O fraudador finge ser um funcionário do banco e, por meio de uma ligação telefônica, manipula o cliente para realizar transações financeiras em benefício de um grupo criminoso.
GOLPE DA FALSA DÍVIDA	Envolve vazamentos de dados como contas bancárias e telefones, esses dados são utilizados em ligações para ameaçar clientes com acusações de dívidas falsas, o que no primeiro momento, assusta e comove as vítimas, seguido de uma promoção ou desconto na suposta dívida com um prazo determinado e muito curto.
GOLPE DA FALSA PORTABILIDADE	Com vítimas na maior parte dos casos, funcionários públicos, é uma estratégia criminosa na qual os golpistas, muitas vezes se passam por funcionários de instituições financeiras, entram em contato com vítimas que geralmente já possuem empréstimos consignados.

GOLPE DO NOVO CONTATO DE WHATSAPP	Eles iniciam conversas com parentes e amigos, fingindo ser o usuário, alegando ter trocado de número e instruindo o contato a apagar e até bloquear o antigo. Em seguida, solicitam dinheiro, apresentando desculpas plausíveis para justificar as transferências.
GOLPE DA TABELA PIX	Os criminosos geralmente prometem, por meio de publicações em feeds ou stories do Instagram, que ao usuário investir uma quantia específica, obterá um lucro que pode chegar a até cinco vezes o valor investido.
GOLPE DO "BENÇA TIA"	Perpetrada por indivíduos que se fazem passar por parentes ou conhecidos das vítimas, tipicamente por meio de contato telefônico. Os golpistas alegam estar em situações de crise, como acidentes, problemas de saúde ou questões financeiras prementes, e solicitam empréstimos de dinheiro às vítimas.

GOLPE DO FALSO LEILÃO	A modalidade fraudulenta envolve a criação de um site que simula ser um leiloeiro, apresentando falsos leilões de veículos, imóveis, maquinários e outros itens, frequentemente com valores abaixo do mercado, visando atrair indivíduos em busca de oportunidades vantajosas.
GOLPE DO DDA	Trata-se do recebimento de um e-mail fraudulento que menciona um suposto desconto, direcionando a vítima a desconsiderar o pagamento por meio do Débito Direto Autorizado (DDA) e realizar a quitação através de um boleto enviado por e-mail, o qual substitui o DDA.
GOLPE DOS VALORES A RECEBER	Os golpistas se aproximam das potenciais vítimas alegando a existência de ‘Valores a receber BCB’. O termo 'BCB' refere-se ao Banco Central do Brasil, e os criminosos utilizam a expressão "valores a receber" para aludir a um sistema de consulta de fundos esquecidos em entidades financeiras que podem ser resgatados.

GOLPE DO DEPÓSITO PARA EMPRÉSTIMOS	Algumas organizações criminosas se aproveitaram desse cenário, passando a oferecer a promessa de conceder empréstimos desprovidos de procedimentos burocráticos, sem verificação junto às entidades reguladoras, de maneira ágil e descomplicada.
GOLPE DO ROBÔ OU GOLPE DO BOT	Esta estratégia fraudulenta envolve a interação com vítimas, geralmente por meio de chamadas telefônicas automatizadas (robôs), mensagens de texto ou aplicativos de mensagens, onde os golpistas persuadem as vítimas a realizarem transferências via Pix.
GOLPE DO DUMP E PUMP	Essa estratégia fraudulenta tem o intuito de manipular o valor de um ativo, geralmente conduzida por meio de comunidades online ou fóruns de investimento, visando gerar lucros para os organizadores à custa de outros investidores.

Fonte: Elaborado pelo Autor

O cartão é um dos produtos bancários que possuem numerosos tipos de golpe, no Golpe da Troca de Cartão, um golpista se faz passar por atendente bancário, informando à vítima sobre um suposto erro no cartão. Após oferecer ajuda, o golpista substitui o cartão original por outro, utilizando artifícios como falsas cobranças ou alegando problemas no caixa eletrônico. Já no Golpe do Cartão Não Presente, envolve a obtenção dos detalhes do cartão durante transações presenciais, seguido pelo uso dessas informações em compras online. Criminosos utilizam sites falsos e atraentes, induzindo vítimas a fornecer dados pessoais. A recomendação é verificar ofertas diretamente em lojas físicas ou ligar para a central de atendimento para confirmar a legitimidade. No Golpe da Retenção de Cartão, os golpistas aplicam uma substância adesiva em caixas eletrônicos, retendo o cartão da vítima. Oferecem ajuda, proporcionando um telefone falso conectado ao banco. Ao revelar informações confidenciais, a vítima permite que o golpista use o cartão para compras ilegais.

No Golpe do Falso Motoboy, os indivíduos se passam por funcionários bancários, alegando fraude no cartão. Após convencer a vítima a cortar o cartão ao meio, mantendo o chip, um falso motoboy retira o suposto cartão destruído. Com senha e chip em mãos, os golpistas realizam transações fraudulentas.

Já no Golpe do Bilhete Premiado, criminosos convencem as vítimas de posse de um bilhete premiado na loteria. Oferecem vender o bilhete a uma fração do valor. A recomendação é registrar um boletim de ocorrência imediatamente.

O Golpe do WhatsApp tem crescido, onde criminosos clonam contas do WhatsApp, solicitando códigos de segurança alegando serem de suporte ao cliente. Com acesso à conta, pedem dinheiro aos contatos da vítima. Recomenda-se nunca responder códigos de segurança enviados por SMS e ativar opções de segurança. O que se difere do Golpe do Novo Contato de WhatsApp, onde criminosos criam perfis falsos, solicitando dinheiro a contatos de amigos e familiares. Recomenda-se verificar a veracidade do contato.

No Golpe do Link Falso, os fraudadores enviam links suspeitos por e-mail, SMS, ou redes sociais, fingindo ser instituições bancárias. A recomendação é evitar clicar em links desconhecidos e usar antivírus legítimos.

Já o Golpe do Falso Cancelamento de Empréstimo, criminosos se passam por funcionários bancários, comunicando um empréstimo consignado. Direcionam o depósito para contas próprias, desviando os fundos. Instituições não realizam consignados por telefone.

O Golpe do Falso Boleto implica em criminosos enviarem boletos falsos por e-mail, SMS ou WhatsApp, desviando o pagamento para contas próprias. Recomenda-se verificar dados antes do pagamento.

No Golpe do Delivery, o cliente paga mais do que deveria ao receber um pedido, sendo convencido por um visor danificado ou simulações de problemas. A recomendação é usar sistemas de compra seguros. Já o famoso Golpe da Falsa Central de Atendimento, os fraudadores se passam por funcionários bancários, manipulando clientes para realizar transações financeiras. A recomendação é não fornecer dados por telefone.

Assim como o Golpe da Falsa Dívida, onde fraudadores ameaçam vítimas com dívidas falsas, obtendo quantias sob a promessa de descontos. Recomenda-se negociar diretamente com a instituição. No Golpe da Falsa Portabilidade, golpistas se passam por funcionários bancários, oferecendo portabilidade de empréstimos. Com informações detalhadas, enganam as vítimas. Recomenda-se verificar propostas diretamente com as instituições.

O Golpe da Tabela PIX, os fraudadores prometem lucros exorbitantes em investimentos falsos, usando o PIX para transferências. Recomenda-se evitar esquemas de investimento duvidosos. O Golpe do "Bença Tia", os fraudadores se passam por parentes em situações de crise, solicitando empréstimos. Recomenda-se validar a autenticidade da situação antes de agir.

Já o fantasioso Golpe do Falso Leilão, criminosos criam sites simulando leilões, recebendo pagamentos sem entregar os produtos. Recomenda-se desconfiar de ofertas muito abaixo do mercado. No Golpe do DDA, os fraudadores enviam e-mails fraudulentos induzindo as vítimas a pagar boletos falsos, substituindo o Débito Direto Autorizado (DDA). Recomenda-se verificar a validade do documento com o beneficiário.

O Golpe dos Valores a Receber, criminosos usam o nome do Banco Central para induzir vítimas a verificar supostos valores pendentes, levando-as a transferir dinheiro. Recomenda-se consultar a instituição financeira antes de transações. O Golpe do Depósito para Empréstimos, por sua vez, golpistas prometem empréstimos fáceis em troca de depósitos antecipados. Recomenda-se evitar transações com entidades sem reconhecimento oficial.

Além dos golpes indicados pela FEBRABAN, um tipo de fraude recorrente no setor financeiro, mencionado por Oliveira (2012), são as "fraudes documentais que tratam, por exemplo, de clonagem de cheques, falsa identidade e abertura de conta corrente com documento falso". As fraudes documentais se caracterizam pela adulteração e/ou falsificação de documentos bancários ou de identidade.

Conforme mencionado por Oliveira (2012) as principais fraudes documentais podem ser categorizadas em seis grandes grupos: Fraude na Abertura de Conta, Cheques

Clonados/Falsificados e Adulterados, Fraude em TEDs, DOCs, Ordens de Pagamento e Boletos de Cobrança, Fraude no Crédito Direto ao Consumidor, Fraude no Crédito Consignado e Fraude no Financiamento de Veículos.

Essas considerações ressaltam a urgência de estratégias abrangentes por parte das instituições financeiras no combate a golpes e fraudes.

CONSIDERAÇÕES FINAIS

Na sociedade contemporânea, as preocupações com segurança tornaram-se extremamente relevantes. No entanto, muitas organizações negligenciam o fato de que seus próprios recursos humanos estão no epicentro da maioria das violações de segurança. Entre as estratégias de ataque, a engenharia social encontrou um terreno fértil para ser explorado.

Este trabalho teve como objetivo fazer um levantamento das variadas modalidades de golpes financeiros que acometem pessoas físicas e jurídicas no Brasil através de pesquisas bibliográficas, assim como o levantamento das problemáticas que acompanham o tema, como a organização do Sistema Financeiro Nacional e a segurança da informação.

O objetivo estabelecido no projeto foi alcançado, e a revisão bibliográfica proposta contribuiu significativamente para a compreensão dos diversos tipos de ataques de engenharia social, além de fornecer uma demonstração prática de como esses ataques são executados. O trabalho possibilitou a apresentação de práticas que podem auxiliar os usuários a evitarem cair em golpes desse formato.

Os dados evidenciam a importância crucial das instituições financeiras na proteção de seus clientes contra essas ameaças. Essas instituições desempenham um papel crítico na manutenção da confiança de seus clientes em seus serviços e na prevenção de fraudes. Os resultados da pesquisa destacaram a necessidade de as instituições financeiras continuarem aprimorando e evoluindo suas medidas de segurança para enfrentar as estratégias em constante mudança dos fraudadores.

A diversidade de golpes financeiros e a forma com que são aplicados denunciam que as brechas por trás da falta de Segurança da Informação são maiores que as já declaradas. Por um lado, há o vazamento de dados na ampla rede da Internet, que vitimiza os usuários e coloca a maior parte da população em perigo, os bancos de dados são compartilháveis e por isso, frágeis. Com a disseminação cada vez maior da utilização de sistemas de informação e sua

interconectividade com outras redes, incluindo a Internet, os sistemas agora estão mais vulneráveis do que nunca a ameaças de segurança.

Os ataques ocorrem com frequência crescente, tornando-se mais eficazes, criativos e complexos de detectar e mitigar. O Open Banking, sistema de compartilhamento de dados interbancários, é um exemplo prático.

A engenharia social é empregada com o propósito de adquirir informações confidenciais ou obter acessos não autorizados a sistemas, utilizando métodos que se fundamentam nas interações humanas. Essa forma de ataque tem crescido em importância, capturando a atenção tanto da comunidade acadêmica quanto da empresarial, e caminha, em passos curtos, da população brasileira em geral.

Descrever as modalidades de golpes e o modus operandi dos seus atuantes passa a ser importante para criar uma unidade de conhecimento, que foi exposta por esse trabalho. As denominações dos golpes ainda são regionalizadas, informais e pouco morfológicas, ou seja, em literaturas acadêmicas, as usadas e referenciadas neste trabalho, não consideram como Fraude, nenhum tipo de ataque que seja exterior à Instituição Financeira mesmo que o destino final delas ainda seja os usuários. Descrevê-los é também uma denúncia aos leitores.

A velocidade das mudanças também é um problema que recai sobre um perfil de pessoas que não acompanham a transição para o mundo digital com tanta facilidade. Neste estudo, também foi discutida uma outra problemática, a falta de educação financeira no Brasil, e esta é uma pauta importante pois enfatiza-se como o conhecimento desses princípios pode auxiliar o investidor a avaliar prontamente suas decisões e evitar cair em golpes. Assim como observado por Lusardi (2015), a alfabetização sobre o risco torna-se crucial, uma vez que muitas decisões financeiras fundamentam-se na compreensão do risco e na diversificação do mesmo. Com pouca alfabetização financeira, maior o risco de golpes e fraudes.

Por fim, ressalta-se a importância de conduzir mais pesquisas sobre a problemática relacionada aos golpes financeiros de Engenharia Social, abordando novas perspectivas, tanto das vítimas quanto das instituições financeiras. Recomenda-se que esses estudos adotem uma abordagem multidisciplinar, envolvendo a colaboração de pesquisadores da área do direito, da psicologia, da tecnologia da informação, administradores, comunicadores, entre outros. Além disso, é crucial buscar abrangência nos registros de golpes de Engenharia Social na instituição e, a partir disso, desenvolver comunicações mais específicas aos usuários potencialmente vulneráveis.

6. REFERÊNCIAS

RAZAK, Lebuhraya Tun. The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM" Mohammed A. Al-Sharaf,“Ruzaini A. Arsha," Emad Abu-Shanab and “Nabil Elayah" Faculty of Computer Systems and Software Engineering, UMP. **Journal of Engineering and Applied Sciences**, v. 100, n. 3, p. 545-552, 2016. Acesso em 30 de julho de 2023.

SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. **Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**, v. 31, p. 16, 2016. Acesso em 30 de julho de 2023.

ZACHARIAS, Maria Luiza Barcellos; FIGUEIREDO, Kleber Fossati; ALMEIDA, Victor Manoel Cunha de. Determinantes da satisfação dos clientes com serviços bancários. **RAE eletrônica**, v. 7, 2008. Acesso em 30 de julho de 2023.

SANTOS, Maria Isabel Sousa Calisto dos. **O sistema financeiro nacional: os efeitos das novas ferramentas online nas instituições financeiras**. 2022. Acesso em 30 de julho de 2023.

DOS REIS, David Carvalho; RECCO, Claudineia Helena; FERNANDES, Marcelo Eloy. Segurança da Informação nas Redes Sociais. **Revista de Sistemas de Informação**, v. 1, n. 01, 2021. Acesso em 30 de julho de 2023.

BRITO, M. S.; JÚNIOR, I. G. Ciberataques em Serviços Essenciais de Telecomunicações: Uma Revisão Sistemática. **FatecLog - Congresso de Segurança da Informação,** acesso em 30 de julho de 2023.

ROMUALDO, Paulo Henrique. S**egurança da informação, engenharia social: principais ataques às organizações e o elo mais fraco da segurança.** 2020. Acesso em 30 de julho de 2023.

FINKLER, F. B.; AMARAL, M. A. ENGENHARIA SOCIAL – A NOVA ARMA CONTRA OS USUÁRIOS DE TECNOLOGIA. **PROJETOS E RELATÓRIOS DE ESTÁGIOS,** v. 4, n. 1. Acesso em 5 agosto de 2023.

SOUZA, Guilherme et al. Segurança da Informação na comunicação de dispositivos médicos: uma revisão quasi-sistemática. **Journal of Health Informatics**, v. 11, n. 2, 2019. Acesso em 5 de agosto de 2023.

GUEDES, Matheus Santos et al. Crimes e golpes virtuais: desafios enfrentados pelos idosos na era tecnológica. **OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA**, v. 21, n. 9, p. 14026-14040, 2023.

ALMEIDA, C. et al. **Utilização de novas tecnologias por idosos institucionalizados**. Revista Motricidade, v. 15, n. 4, p. 31-35, 2019. Acesso em 7 de agosto de 2023.

BARDIN, L. **Análise de conteúdo.** São Paulo: Edições 70, 2011. Acesso em 7 de agosto de 2023.

10 DICAS ANTIGOLPE. FEBRABAN, 2021. Disponível em < https://antifraudes.febraban.org.br/?gclid=Cj0KCQjwiNSLBhCPARIsAKNS4_ea3_CE FURviFrzzvWdVsAdBbONNQSTmMviKozKk7nU-MrNLH0hicQaAtUPEALw_wcB>. Acesso em 17 de agosto de 2023.

CORRÊA, L. et al. **Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020.** Research, Society and Development, v. 11, n. 1, p. e43411125214-e43411125214, 2023.

ALEROUD, Ahmed; ZHOU, Lina. **Phishing environments, techniques, and countermeasures: A survey. Computers & Security 68, 160–196, 2017.** Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404817300810?via3Dihub. Acesso em 30 de agosto de 2023.

Algumas dicas de segurança. BANCO DO BRASIL. Disponível em https://www.bb.com.br/pbb/pagina-inicial/bb-seguranca#/. Acesso em: 03 de dez. 2021.

ARAMUNI, João Paulo; MAIA, Luiz Cláudio. **O impacto da Engenharia Social na Segurança da Informação: uma abordagem orientada à Gestão Corporativa.** AtoZ, v. 7, n.1. 2018. ISSN: 2237-826X. Disponível em: https://revistas.ufpr.br/atoz/article/view/64640/40229. Acesso em 30 de agosto de 2023.

AUGUSTO, Mário António Gomes; FREIRE, Sara Filipa Rodrigues. **Atributos do investidor e tolerância face ao risco: a perspetiva dos pequenos investidores.** REGE, v. 21,

n. 1, p. 103-120, jan./mar. 2014. DOI: 10.5700/rege 521. Disponível em: file:///C:/Users/usuário/Downloads/99921-Article% 20Text-174185-1-10-20150702.pdf. Acesso em 30 de agosto de 2023.

BITAAB, Marzieh et al. Scam Pandemic: H**ow Attackers Exploit Public Fear Through Phishing. ArXiv, v. 1, 2021**. Disponível em: https://arxiv.org/abs/2103.12843. Acesso em: 31 de ago. 2023.

CABRAL, Daniel Barbosa; TORRES, Nancy Maria Correa. **Satisfação e fidelização de clientes do setor bancário brasileiro. Navus,** v. 9, n. 4, p. 195-205, out./dez. 2019. DOI: http://dx.doi.org/10.22279/navus.2019.v9n4.p195-205.929. Disponível em: https://navus.sc.senac.br/index.php/navus/article/view/929/pdf. Acesso em 02 de setembro de 2023.

DORIGON, A.; SOARES, R. V. de O. **Crimes cibernéticos: dificuldades investigativas na obtenção de indícios da autoria e prova da materialidade.** Revista Jus Navigandi, Teresina, ano 23, nº. 5342, 15 fev. 2018. Disponível em: https://jus.com.br/artigos/63549. Acesso em 03 de setembro de 2023.

GIL, A. C. **Como elaborar projetos de pesquisa, 6ª edição**. São Paulo: Atlas, 2017.

GIL, A. C. **Métodos e técnicas de pesquisa social. 7. ed.** São Paulo: Atlas, 2019

Crescem golpes envolvendo manipulação de vítimas para roubo de informações pessoais. FEBRABAN, 2010. Disponível em: https://portal.febraban.org.br/noticia/3704/pt-br. Acesso em: 09 de setembro de 2023.

KRUG, R. de R.; XAVIER, A. J.; D'ORSI, E. **Fatores associados à manutenção do uso da internet, estudo longitudinal**. Revista de Saúde Pública, v. 52, 2018. Acesso em 09 de setembro de 2023.

BRASIL. Policia Federal (PF). PF e Febraban renovam acordo de cooperação técnica. Brasília, fev., 2018. Disponível em: http://www.pf.gov.br/agencia/noticias/2018/02/pf-efebraban-renovam-acordo-de-cooperacao-tecnica. Acesso em 09 de setembro de 2023.

DILEMA, Marguerite et al. **Financial Fraud Among Older Americans: Evidence and Implications. The Journals of Gerontology: Series B**, v. 75, n. 4, p. 861 – 868, 2020.

DOI: https://doi.org/10.1093/geronb/gby151. Disponível em: https://academic.oup.com/psychsocgerontology/article/75/4/861/5250441. Acesso em: 30 de ago. 2023.

PLATT, W. **Produção de informações estratégicas.** Rio de Janeiro: Biblioteca do Exército: Livraria Agir Editora, 1974. Acesso em 27 de setembro de 2023.

SANTOS, Izequias Estevam dos. **Manual de métodos e técnicas de pesquisa científica.** 9. ed. Niterói: Impetus, 2012. Acesso em 27 de setembro de 2023.

SERAPIONI, Mauro. **Métodos qualitativos e quantitativos na pesquisa social em saúde: algumas estratégias para a integração.** Ciênc. Saúde Coletiva, Rio de Janeiro, v. 5, n. 1, p. 187-192, 2000. Acesso em 28 de setembro de 2023.

CABRAL, Daniel Barbosa; TORRES, Nancy Maria Correa. **Satisfação e fidelização de clientes do setor bancário brasileiro.** Navus, v. 9, n. 4, p. 195-205, out./dez. 2019.DOI: http://dx.doi.org/10.22279/navus.2019.v9n4.p195-205.929. Disponível em: https://navus.sc.senac.br/index.php/navus/article/view/929/pdf. Acesso em 02 de novembro de. 2023.

GOLPES ENVOLVENDO CARTÕES/GOLPES ENVOLVENDO SENHAS. Banrisul, 2021. Disponível em: https://www.banrisul.com.br/bob/link/bobw22hn_home.aspx?secao_id=1888. Acesso em 02 de outubro de 2023.

GONÇALVES, Lucca Merhy Arruda. **Responsabilidade civil em casos de fraudes digitais no setor bancário.** Orientador: Dr. Charles Emmanuel Parchen. 2021. 80 f. TCC (Graduação) – Curso de Direito, Centro Universitário Curitiba, Curitiba, 2021. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/17830. Acesso em 06 de outubro de 2023.

PIX. Banco Central, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix. Acesso em 08 de outubro de 2023.