UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

GUSTAVO DUARTE WALTEREITH KOCH

PERFIL DE VÍTIMAS DE GOLPES EM UMA INSTITUIÇÃO FINANCEIRA

Porto Alegre
2022

GUSTAVO DUARTE WALTEREITH KOCH

PERFIL DE VÍTIMAS DE GOLPES EM UMA INSTITUIÇÃO FINANCEIRA

Trabalho de Conclusão de Curso apresentado como requisito para obtenção de título de Bacharel em Administração pela Universidade Federal do Rio Grande do Sul – UFRGS.

Porto Alegre
2022

CIP - Catalogação na Publicação

Koch, Gustavo Duarte Waltereith
PERFIL DE VÍTIMAS DE GOLPES EM UMA INSTITUIÇÃO FINANCEIRA / Gustavo Duarte Waltereith Koch. -- 2022.
35 f.
Orientador: Pablo Cristini Guedes.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Escola de Administração, Curso de Administração, Porto Alegre, BR-RS, 2022.

1. Golpes financeiros. 2. Engenharia Social. 3. WhatsApp. I. Guedes, Pablo Cristini, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

GUSTAVO DUARTE WALTEREITH KOCH

PERFIL DE VÍTIMAS DE GOLPES EM UMA INSTITUIÇÃO FINANCEIRA

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração. Orientador: Prof. Dr. Pablo Cristini Guedes

Porto Alegre, 2022

BANCA EXAMINADORA:

_____

Prof. Dr. Pablo Cristini Guedes UFRGS

_____

Prof. Dr. Guillermo Fernando Hovermann da Cruz EA/UFRGS

_____

Prof. Dr. Guilherme Brandelli Bucco EA/UFRGS

AGRADECIMENTOS

Ao meu orientador professor Doutor Pablo Cristini Guedes pela disponibilidade e colaboração;

À minha mãe Nilcéa pela ajuda em todas as etapas dessa jornada;

À mãe do meu filho, Raquel, pela ajuda, paciência e força para cuidar do Pedro enquanto o pai estava ocupado;

E ao Pedro por ser a coisa mais linda que já aconteceu na minha vida.

RESUMO

Foi realizada uma pesquisa descritiva sobre o perfil de vítimas de golpes financeiros de Engenharia Social ocorridos com clientes de Instituição Financeira através do aplicativo *WhatsApp*. Engenharia Social pode ser definida como o conjunto de métodos e técnicas para manipular pessoas, predominantemente com o uso de persuasão psicológica, com o objetivo de ganhar acesso a informações pessoais, documentos e sistemas computacionais contendo dados sigilosos. A amostra da pesquisa constou de 32 vítimas e os resultados mostraram que entre as vítimas o sexo feminino predominou com 78,13%; a faixa etária com maior frequência foi de 60 a 79 anos com 59,38%; a predominância quanto à escolaridade foi de curso superior completo com 59,38%, sendo que 12,50% tinham também Pós-Graduação. Novos estudos devem ser realizados para traçar perfis mais específicos dos clientes potencialmente mais vulneráveis.

Palavras-Chave: Golpes financeiros; Engenharia Social; *WhatsApp*

ABSTRACT

A descriptive survey was carried out on the profile of victims of Social Engineering financial scams that occurred with customers of financial institution through the WhatsApp application. Social Engineering can be defined as the set of methods and techniques to manipulate people, predominantly with the use of psychological persuasion, in order to gain access to personal information, documents and computer systems containing sensitive data. The research sample consisted of 32 victims, and the results showed that among the victims, females predominated with 78.13%; the most frequent age group was from 60 to 79 years old, with 59.38%; the predominance in terms of schooling was complete higher education with 59.38%, and 12.50% also had postgraduate degrees. New researches should be carried out to draw more specific profiles of potentially more vulnerable clients.

Key words: Financial scams; Social engineering; Whatsapp

SUMÁRIO

1. DELIMITAÇÃO DO TEMA DE ESTUDO

Engenharia Social pode ser definida como o conjunto de métodos e técnicas para manipular pessoas, predominantemente com o uso de persuasão psicológica, com o objetivo de ganhar acesso a informações pessoais, documentos e sistemas computacionais contendo dados sigilosos (WASHO, 2021; DICAS..., 2021). É uma prática utilizada para aplicar golpes. Um exemplo é o *Phishing,* em que o invasor explora essas técnicas para roubar identidade dos usuários de *internet*. *Phishing* funciona enviando *Short Message Service* (SMS), mensagens instantâneas e *emails* falsos, imitando *sites* de banco, leilão ou pagamento *online*, guiando os usuários a um *site* falso meticulosamente projetado para emular o *site* verdadeiro (ALEROUD; ZHOU, 2017).

Clientes de instituições financeiras foram especialmente atingidos por este fenômeno, fornecendo informações confidenciais, como dados pessoais, senhas e até mesmo entregando seus cartões para os criminosos (VITORIO, 2021). Estes criminosos de posse dos dados passam para a etapa posterior de abordagem que envolve contato por telefone para aprofundar o processo de persuasão até conseguir subtrair algum recurso da vítima (VITORIO, 2021).

Instituições bancárias têm realizado uma série de medidas visando diminuir o número de golpes efetivados em sua base de clientes. O Banco do Brasil, Bradesco, Caixa Econômica Federal (Caixa), Banco do Estado do Rio Grande do Sul (Banrisul), Itaú e Santander em seus *sites* apresentam, como medidas de segurança, material informativo sobre identificação dos golpes financeiros e como preveni-los. Esse material é disponibilizado através de textos, infográficos e vídeos. Em alguns, como no Bradesco e na Caixa as informações estão apresentadas em cartilhas virtuais detalhadas, por vezes longas, que não despertam o interesse e a curiosidade do usuário para consultá-los.

Alguns bancos, como o Banrisul, empregam medidas envolvendo propagandas em estações de rádio FM, envio periódico de *e-mails* contendo recomendações de segurança, envio de SMS alertando sobre os golpes prevalentes e condutas que devem ser evitadas. Ao acessar o aplicativo oficial e o *Home Banking* do Banrisul, estes alertas surgem através de mensagens de *push*, que podem ser definidas como:

> Mensagens de texto *pop-up*, com ou sem uma imagem, que se comunicam de forma proativa com o usuário diretamente de uma variedade de aplicativos ou de um *site* da *web* e que postam uma ampla gama de conteúdo, tanto privado quanto social, enviados por redes sociais, empresas comerciais ou editores de notícias (GAVILAN, *et al.,* 2020)

Segundo Vitorio (2021) as iniciativas para prevenção de golpes têm se mostrado insuficientes, uma vez que os golpes continuam aumentando. Nesse sentido, no dia 10 de setembro de 2021 ocorreu um encontro entre o ministro da Justiça e Segurança Pública, Anderson Torres, e o presidente da Federação Brasileira de Bancos (FEBRABAN), Isaac Sidney, em que discutiram a criação de uma Estratégia Nacional de Combate ao Crime Cibernético (FEBRABAN..., 2021). Um resultado desse esforço conjunto foi a criação de dicas para evitar os golpes através da informação aos clientes bancários (10 DICAS..., 2021).

Constata-se que os golpes financeiros que envolvem Engenharia Social, são pouco estudados, havendo uma carência de publicações nacionais, mesmo sendo uma questão contemporânea grave que tantos danos acarretam às vítimas, bem como às instituições bancárias.

Para o desenvolvimento deste Trabalho de Conclusão de Curso foram selecionados os principais golpes de Engenharia Social, que serão descritos no capítulo 4.

Por ser funcionário de agência bancária, atendo vítimas de golpes financeiros que buscam desesperadamente a reversão das perdas sofridas. Sinto-me impotente, pois além de ouvi-las e fazer o encaminhamento do relato e do boletim de ocorrência policial ao setor responsável da Instituição Financeira, nada mais posso fazer, e em praticamente todos os casos a reversão é impossível.

Frente ao exposto, senti a necessidade de aprofundar o conhecimento sobre o tema. Para tal questiono:

Qual o perfil dos clientes vítimas de golpes financeiros de Engenharia Social e como contribuir com a Instituição Financeira para preveni-los?

2. JUSTIFICATIVA

Os golpes financeiros que envolvem Engenharia Social, como apontados anteriormente, estão aumentando a cada dia, com crescimento de 165% no primeiro semestre de 2021 em relação ao segundo semestre de 2020 (CRESCEM..., 2021), causando às vítimas e suas famílias danos imensos, na maioria das vezes irreparáveis.

Já para as instituições bancárias têm gerado danos à reputação e confiança, requisitos essenciais para a manutenção dos seus negócios. Ainda que diferentes instituições venham estabelecendo medidas para a prevenção desses golpes, para Vitorio (2021), as medidas para evitar esses golpes não têm sido suficientes. Além disso, há carência de publicações nacionais sobre vítimas de golpes financeiros e principalmente sobre as práticas adotadas pelas instituições bancárias para enfrentar este problema. Presume-se que isso decorra de decisões estratégicas dessas instituições em não expor planos de ações sigilosos.

Por outro lado, Kadoya *et al.,* (2021) em estudo sobre vítimas de fraudes financeiras, concluíram que o perfil dessas vítimas difere em cada tipo de golpe e sugerem que uma política de abordagem única não pode combater efetivamente a fraude financeira.

Desta forma, por vivenciar esse complexo problema no local de trabalho, senti a necessidade de obter maior conhecimento sobre o tema. Através deste estudo, conhecendo o perfil de vítimas de golpes financeiros em clientes da Instituição Financeira, espero contribuir com a instituição na ampliação de medidas preventivas direcionadas ao perfil das potenciais vítimas desses golpes.

3. OBJETIVOS

3.1 Objetivo Geral

Conhecer o perfil das vítimas de golpes financeiros de Engenharia Social, ocorridos através do aplicativo *WhatsApp* com clientes de Instituição Financeira, visando fornecer a essa instituição subsídios para a ampliação de medidas de prevenção.

3.2 Objetivos Específicos

a) Conhecer o perfil das vítimas de golpes financeiros de Engenharia Social ocorridos através do aplicativo *WhatsApp* em clientes de Instituição Financeira.

b) Identificar a frequência de golpes financeiros de Engenharia Social ocorridos através do aplicativo *WhatsApp* em clientes de Instituição Financeira

c) Analisar os resultados obtidos com base na revisão teórica.

d) Contribuir com a Instituição Financeira na ampliação de medidas de prevenção aos golpes financeiros.

4. REVISÃO TEÓRICA

Pesquisas no segmento bancário têm sido realizadas para identificar as limitações no uso dos canais digitais, mensurar satisfação e avaliar a fidelidade, lealdade e confiança dos clientes com as instituições bancárias frente à inclusão de novas tecnologias que fazem parte dos multicanais de atendimento. Também procuram classificar a propensão dos clientes para aquisição de produtos dentro do portfólio do banco ou para o desenvolvimento de novos produtos. Em última instância, buscam aumentar a competitividade com consequente incremento na lucratividade dessas empresas.

O estudo de Guerra, Oleto e Peñaloza (2018) mostrou que a satisfação desempenha função importante na variabilidade da lealdade do cliente bancário em um contexto de atendimento através de multicanais. No entanto, a satisfação não teve relação com a confiança.

Em um estudo sobre percepção do usuário no uso das Tecnologias de Informação e Comunicação no autoatendimento bancário, Tomás e Silva (2019) referem que um número reduzido de clientes possuem limitação no uso das ferramentas tecnológicas bancárias. Dentro desse grupo existe uma tendência maior do perfil de indivíduos com mais de 45 anos, com escolaridade até o ensino médio e renda até R$1.874,00 em valores da época.

Já Zacharias, Figueiredo e Almeida (2008) realizaram uma pesquisa com 1001 clientes de bancos no Rio de Janeiro e em São Paulo, e concluíram que o quesito mais importante para a satisfação global do cliente é o modo como o banco soluciona os problemas decorrentes do serviço prestado. Em segundo lugar ficou a satisfação com os gerentes, e esses dois aspectos pertencem ao espectro do relacionamento. No âmbito técnico, a satisfação com produtos e serviços oferecidos e com o caixa eletrônico tiveram grande importância na satisfação geral dos clientes.

Nas últimas décadas o uso de internet para realizar as mais diversas tarefas teve uma expansão muito significativa. O aumento da largura de banda dos provedores de internet e a ampliação dos seus usuários resultaram em fluxos de dados sensíveis cada vez maiores, através de reuniões e aulas virtuais, compartilhamento de arquivos, entre outros. Este processo criou um ambiente propício para crimes virtuais, que cresceram na mesma proporção, tais como:

ransomware[1]*, malware*[2]*,* violação de dados e *phishing*[3] (SUSHRUTH; REDDY; CHANDAVARKAR, 2020). Golpes financeiros também cresceram nos últimos anos. Dois terços dos norte-americanos que usam internet, algo em torno de 116 milhões de pessoas, receberam ao menos uma oferta de golpe *online* em 2013 (RAAIJ, 2016). Estes dados estatísticos são subestimados, uma vez que vítimas de fraudes nem sempre denunciam o que sofreram por temerem o ridículo e a estigmatização de terem sido vítimas de fraude financeira. Doze por cento das vítimas de fraude de investimento conhecidas negaram ter perdido dinheiro em uma aplicação financeira fraudulenta, e apenas metade das vítimas de fraude de loteria conhecidas reconheceram ter sofrido golpe (RAAIJ, 2016).

Os golpes citados fazem parte de um problema social grave chamado eufemisticamente de Engenharia Social, pois deriva de dois termos sem conotação pejorativa:

> a) Engenharia: Arte de aplicar conhecimentos científicos, empíricos e certas habilitações específicas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas;
> b) Social: Da sociedade, ou relativo a ela. Sociável. Que interessa à sociedade (ARAMUNI; MAIA, 2018).

No entanto, o termo no contexto abordado por este trabalho representa a sórdida prática de enganar pessoas para obter informações sigilosas até concretizar a subtração de recursos financeiros das vítimas. Isto pode ocorrer por ingenuidade ou confiança por parte da vítima (ARAMUNI; MAIA, 2018).

Outro conceito de Engenharia Social, segundo Sushruth, Reddy, Chandavarkar (2020) é o *Human Hacking* – equivalente a "*hackear* um humano" em tradução literal. Mesmo que uma empresa invista uma boa fatia do seu faturamento

---

[1]*Ransomware* ou sequestro virtual de dados pessoais para resgate. É uma nova forma de seqüestro, onde o que é mantido em cativeiro não é uma pessoa, mas seus dados pessoais (FERREIRA; KAWAKAMI, 2018).

[2]Qualquer programa que cause dano a um usuário, computador ou rede é chamado de *malware* (HAN *et al*., 2019).

[3]O termo *phishing* que é proveniente do verbo *fishing* em inglês, que quando traduzido na forma literal ao português se iguala ao verbo pescar, é utilizado para definir tipos de condutas fraudulentas cometidas no ambiente digital. Esse tipo de fraude utiliza da engenharia social para enganar a vítima, principalmente através de meios digitais, a fim de obter informações pessoais e confidenciais, como dados de cartões de crédito, contas e senhas bancárias (GONÇALVES, 2021, p. 53).

em tecnologias para prevenir ataques, o elemento mais frágil do sistema de segurança de informação, o ser humano, continua sendo suscetível a antigos métodos de manipulação (ARAMUNI; MAIA, 2018).

Esta vulnerabilidade fica evidente nos golpes de Engenharia Social perpetrados nos clientes bancários, em que pessoas de todos os países recebem *e-mails* falsos de *phishing* de golpistas tentando acessar seus dados financeiros e de cartão de crédito (RAAIJ, 2016). Para iniciar a aplicação desses golpes, o aspecto emocional das potenciais vítimas é explorado, principalmente, com mensagens de *phishing* criadas para diminuir o processamento cognitivo com termos como urgência, cuidado, prazo final e ameaça de fechamento de conta bancária. A intenção dos golpistas é causar emoções nas vítimas e induzi-las a agirem rapidamente (NORRIS; BROOKES, 2020). Um exemplo dessa prática é o golpe do motoboy, onde as vítimas são estressadas a ponto de entregarem rapidamente seus cartões para "impedir uma compra indevida", que, na verdade, nunca existiu.

Os danos desses golpes não são apenas financeiros. Muitos casais se separam, devido à perda substancial de dinheiro; muitas vítimas equiparam o sentimento de terem sido lesadas financeiramente ao trauma oriundo de um estupro e, inclusive, é comum o desenvolvimento de Síndrome do Estresse Pós Traumático após o enfrentamento de um golpe (MALAMED, 2013).

Existe uma tendência de acreditar que os golpistas usualmente têm preferência por vítimas com idade mais avançada, tanto que profissionais da saúde que atendem idosos, rotineiramente encontram pacientes que são vítimas de fraudes (BURNES *et al.,* 2017). No entanto, o que chama atenção é que o perfil das vítimas de golpes traçado por Norris e Brookes (2020) abrange praticamente toda a população, ou seja, qualquer indivíduo pode se tornar uma vítima. Em paralelo, DeLiema *et al., (*2020) afirmam que um elevado grau de instrução e alto poder aquisitivo não são fatores capazes de tornar as pessoas imunes a golpes.

Um estudo japonês (DAIKU *et al.,* 2020) mostrou que, mesmo com aplicação de técnicas de prevenção de fraudes ou informações sobre exemplos de fraudes anteriores, através de órgãos policiais, os golpes não foram evitados de forma eficaz. Ao enfrentar situações reais de golpes, as vítimas não conseguiram lembrar dos alertas que receberam, pois o mecanismo de ação empregado pelos malfeitores baseia-se na manipulação das emoções (DAIKU *et al.,* 2020). Este mecanismo se identifica no Golpe do Bilhete Premiado, um dos tipos de golpes mais antigos do

Brasil e que, mesmo sendo de amplo conhecimento público, continua fazendo vítimas até hoje.

Também no Japão, Kadoya *et al.,* (2021) realizaram pesquisa sobre vítimas de fraudes financeiras com uma amostra de 11218 participantes, e encontraram que 558 pessoas foram vítimas de golpes, o que representa 4,97%. Dependendo do tipo de golpe, determinado perfil foi mais predominante. Embora difícil, os autores apontam a necessidade de identificar grupos em maior risco para estabelecer medidas de prevenção direcionadas, pois uma política genérica não pode combater fraudes financeiras.

Um dos meios utilizados pelos criminosos para movimentar o dinheiro das vítimas em diversos tipos de golpes é o PIX[4]. Desde sua origem, em novembro de 2020, tem sido alvo crescente de uso por malfeitores como forma de concretizar os golpes financeiros. Por ser uma ferramenta recente, existem raras publicações científicas sobre este grave problema.

No mundo, o aplicativo *WhatsApp*[5] é utilizado por 2 bilhões de usuários em 180 países (SOBRE O WHATSAPP, 2022) . No Brasil, é o aplicativo mais usado, estando presente em 54% dos aparelhos celulares (WHATSAPP..., 2022).

4.1 GOLPES DE ENGENHARIA SOCIAL

Bancos tentam minimizar os golpes através de seus endereços eletrônicos, como por exemplo o Banrisul, que em seu *site* (GOLPES..., 2021), detalha como o cliente pode se proteger: evitar abertura de e-mails de remetentes desconhecidos, desconfiar de ligações e mensagens não solicitadas e habilitar verificação em duas etapas no *e-mail*, aplicativos mensageiros e redes sociais, além de destacar condutas jamais praticadas pela instituição, como, por exemplo, solicitação de

[4]Pix é o pagamento instantâneo brasileiro. O meio de pagamento criado pelo Banco Central (BC) em que os recursos são transferidos entre contas em poucos segundos, a qualquer hora ou dia. É prático, rápido e seguro. O Pix pode ser realizado a partir de uma conta corrente, conta poupança ou conta de pagamento pré-paga (PIX, 2021).

[5]*WhatsApp* é um aplicativo multiplataforma que permite trocar mensagens pelo celular gratuitamente, além disso, seus usuários podem criar grupos de até 50 participantes; enviar mensagens ilimitadas com imagens, vídeos e áudio; compartilhar localização; fazer backup do conteúdo postado nos grupos, etc. As mensagens transmitidas quando o dispositivo está fora da área de cobertura ou desligado são automaticamente salvas e recuperadas quando a rede é restaurada ou quando o dispositivo for ligado (PRADO *et al.,* 2020).

senhas. No *site* (GOLPES..., 2021) também são descritos como agem os fraudadores e os golpes mais comuns em andamento, tais como:

- FALSO MOTOBOY: Ligam para você dizendo ser do Banrisul, informam que seu cartão de crédito ou débito foi fraudado. Em geral, eles têm dados cadastrais verdadeiros para convencer que se trata de uma ligação verídica. Assim, afirmam que o cartão foi clonado ou que há compras suspeitas. Dizem que cancelarão o cartão, e que o cliente deverá confirmar alguns dados por telefone, dentre eles a senha do cartão. Após fornecer a senha, para concluir o cancelamento, o cliente deve cortar o cartão ao meio (na vertical, mantendo o chip intacto). Então, um falso motoboy ou falso representante do Banco busca o cartão supostamente destruído na casa do cliente. Com a senha e o *chip* em mãos, os golpistas fazem diversas transações com o seu cartão. Se acontecer, não atenda, pois é golpe.
- TROCA / FURTO DE CARTÃO: Ocorrem em terminais de autoatendimento ou maquininhas de cartão. O golpista aborda um cliente que acabou de realizar uma operação financeira, e o convence de que a operação não foi finalizada, convidando a vítima a reinserir o cartão na máquina e digitar a senha. A vítima aceita a ajuda, entrega seu cartão e digita a senha na presença do golpista, que enxerga a senha. Enquanto distrai, o golpista troca o cartão original por outro, ficando com o original e entregando uma cópia não funcional para o cliente. Quando o cliente percebe a troca, muitas vezes já é tarde e o cartão já foi utilizado pelo golpista.
- RETENÇÃO DE CARTÃO: Às vezes, golpistas aplicam uma substância adesiva no bocal utilizado para a inserção dos cartões. Como o cartão fica preso por causa do adesivo, o golpista aborda o cliente e oferece ajuda, fornecendo um telefone celular em contato direto com o Banco. A vítima aceita ajuda, sem saber que está falando com um comparsa do golpista, e revela todos os seus dados bancários sigilosos e informações cadastrais para o estelionatário que atende a ligação. Quando o cliente vai embora sem o cartão, o golpista recolhe e utiliza o cartão de forma indevida.

Golpe do (a) falso (a) namorado (a) ou Golpe do amor ou Golpe *Don Juan*: neste golpe, criminosos usam perfis falsos em redes sociais e *sites* de relacionamento para atrair, seduzir com declarações de amor e ganhar a confiança das vítimas que procuram um relacionamento amoroso. Após o envolvimento, uma das estratégias usadas é pedir dinheiro para a compra

de passagens aéreas, para que possam se conhecer pessoalmente, ou para pagar tratamentos de saúde que o *Don Juan* supostamente esteja fazendo. Naturalmente, tudo não passa de mentiras para extorquir uma vítima apaixonada (PREVENÇÃO... 2021).

Golpe da ativação do *app* no celular do golpista através do *Home/internet Banking*: neste golpe um falso funcionário liga para o cliente e solicita que o mesmo faça, com urgência, alguns procedimentos para supostamente evitar uma fraude. Sem perceber, o cliente acaba liberando o acesso do *mobile banking* no celular do criminoso, e a partir disso várias operações financeiras são realizadas com prejuízo da vítima.

Golpe do bilhete premiado: nesse golpe, criminosos assumem papéis distintos e através de um elaborado teatro convencem a vítima de que possuem um bilhete premiado na Loteria de alto valor, mas que pode ser entregue para a mesma por uma fração da quantia prometida.

4.2 GOLPES NA PANDEMIA DE COVID-19

A pandemia do COVID-19 acentuou ainda mais o cenário de aumento dos crimes cibernéticos. Os casos de *phishing*, por exemplo, tiveram um incremento de 220% em março e abril de 2020, em comparação com o período pré-pandemia (BITAAB *et al.,* 2021). Para os cibercriminosos, o advento da pandemia pode ser considerado uma oportunidade de negócios, devido ao aumento de usuários na internet que podem ser alvos de suas ações. (SUSHRUTH; REDDY; CHANDAVARKAR, 2020).

Durante esse período, golpistas exploraram o altruísmo e interesse pessoal de vítimas, que acreditando se tratar de doações para órgãos de saúde e aquisição de equipamentos de proteção para COVID-19, enviaram dinheiro para malfeitores (BITAAB *et al.,* 2021).

A pandemia afetou radicalmente a vida das pessoas, ocasionando mudanças em todo o mundo digital, e está produzindo desafios para donos de sites, usuários, governos e pesquisadores de segurança para se adaptarem adequadamente (BITAAB *et al,* 2021). O setor bancário tem sido atingido diretamente, com prejuízo de imagem e deterioração do relacionamento com clientes lesados, mesmo que

juridicamente seja discutível a responsabilidade da instituição (BRASIL TJ/SP, 2021). A consequência dessa insegurança é sensível para muitos clientes que precisam enfrentar ameaças diárias para não cair nas armadilhas relatadas neste trabalho.

No momento, há uma escassez de dados nacionais na literatura que mostrem o perfil das vítimas de golpes financeiros. No entanto, é preciso conhecê-lo para montar estratégias de combate mais assertivas e eficazes.

5. PROCEDIMENTOS METODOLÓGICOS

Este Trabalho de Conclusão de Curso foi realizado através de pesquisa descritiva quantitativa sobre o perfil de vítimas de golpes financeiros ocorridos com clientes de Instituição Financeira. As pesquisas descritivas, de acordo com Gil (2008, p. 28):

> [...] têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. São inúmeros os estudos que podem ser classificados sob este título e uma de suas características mais significativas está na utilização de técnicas padronizadas de coleta de dados. Dentre as pesquisas descritivas salientam-se aquelas que têm por objetivo estudar as características de um grupo: sua distribuição por idade, sexo, procedência, nível de escolaridade, nível de renda, estado de saúde física e mental etc. As pesquisas descritivas são, juntamente com as exploratórias, as que habitualmente realizam os pesquisadores sociais preocupados com a atuação prática. São também as mais solicitadas por organizações como instituições educacionais, empresas comerciais, partidos políticos etc.

As informações coletadas referem-se ao perfil das vítimas de golpes financeiros de Engenharia Social, quanto ao gênero, faixa etária, escolaridade, faixa de renda mensal bruta comprovada e ao valor das perdas de suas economias.

A obtenção dos dados da pesquisa ocorreu após reuniões por telefone, comunicação interna pelo *Skype Business* e *e-mail* corporativo diretamente com o departamento responsável pelo acompanhamento dos golpes ocorridos entre os clientes da Instituição Financeira, e o envio do instrumento (apêndice A) com os dados a serem coletados. O preenchimento foi realizado por funcionário do setor. Todo esse processo, até o recebimento dos dados da amostra demandou em torno de 60 dias.

Os dados coletados foram registrados em uma planilha do software Microsoft Office Excel 2003 ® de acordo com as características de perfil citadas acima e analisados utilizando estatística simples.

O projeto deste estudo previa a coleta retrospectiva nos registros existentes nos arquivos dos sistemas da Instituição, dos golpes de Engenharia Social registrados pelas vítimas durante 15 dias, todavia, somente foi possível identificar como golpes de Engenharia Social os que ocorreram com a utilização do aplicativo

WhatsApp, sendo necessário adequar o projeto. Em decorrência, para aumentar o tamanho da amostra, o período de coleta dos dados, referentes ao registro pelas vítimas na Instituição, foi ampliado para 60 dias, de 1º de novembro a 30 de dezembro de 2021.

A amostra, apesar desse aumento do período de coleta, foi de apenas 32 clientes vítimas de golpes financeiros que ocorreram com a utilização do aplicativo *WhatsApp*. O tamanho da amostra impediu uma análise estatística mais elaborada, com desenvolvimento de correlações, por exemplo.

Os resultados são apresentados em tabelas simples na forma de frequência e percentual.

6. RESULTADOS E DISCUSSÃO

A amostra desde estudo foi de 32 clientes da Instituição Financeira, vítimas de golpes de Engenharia Social ocorridos com a utilização do aplicativo *WhatsApp*. O período de coleta dos dados, referentes ao registro pelas vítimas na Instituição Financeira, foi de à 1º de novembro a 30 de dezembro de 2021.

Apresentamos, a seguir, os resultados quanto a gênero, faixa etária, escolaridade, renda mensal bruta e valores das perdas financeiras.

Gênero

Quanto ao gênero, o predomínio de vítimas de golpes financeiros foi do sexo feminino com 78,13% (TABELA 1). Em conversa com o funcionário do departamento responsável pelo acompanhamento dos golpes da Instituição Financeira, sem maiores detalhes, obtive a informação de que o percentual de mulheres nessa Instituição é bem menor do que o encontrado entre as vítimas dessa pesquisa.

Para Judges *et al.,* (2017) em estudo realizado com idosos de um residencial comunitário no Canadá, a frequência de fraudes financeiras foi semelhante entre o sexo masculino (35,5%) e o feminino (33,33%).

Já Ueno *et al.,* (2021) em estudo realizado no Japão, mostram que a redução cognitiva leve é um fator de risco para vulnerabilidade a golpes em idosos. O sexo masculino apresentou maior vulnerabilidade tanto no grupo dos que possuem redução cognitiva, como no grupo dos que não possuem. Entretanto, reportam dados da Agência Nacional de Polícia do Japão onde 65,30% das vítimas de golpes e fraudes são mulheres.

TABELA 1 – DISTRIBUIÇÃO DA AMOSTRA POR GÊNERO.

SEXO	FREQUÊNCIA	%
FEMININO	25	78,13
MASCULINO	7	21,88
TOTAL	32	100,00

FONTE: ELABORADA PELO AUTOR, 2022

Faixa etária

No estudo da faixa etária, os idosos de 60 a 79 anos, vítimas de golpes financeiros, predominaram com 59,38% e em segundo lugar aparecem os adultos na faixa etária de 50 a 59 anos, com 34,38% (TABELA 2).

Ao traçar o perfil das vítimas de golpes, Norris e Brookes (2020) referiram que a abrangência é praticamente de toda a população, ou seja, qualquer um pode se tornar vítima. Entretanto, Kadoya *et al,.* (2021), em estudo sobre vítimas de golpes financeiros no Japão, entre outros fatores, destacaram uma maior ocorrência desses golpes entre idosos e solitários. Já Ueno *et al.,* (2021) apresentaram dados da Agência Nacional de Polícia do Japão onde 65,30% das vítimas de golpes e fraudes são idosas acima de 65 anos.

TABELA 2 – DISTRIBUIÇÃO DA AMOSTRA POR FAIXA ETÁRIA.

	FAIXA ETÁRIA	FREQUÊNCIA	%
1	até 18 anos	0	0,00
2	19 a 29 anos	1	3,13
3	30 a 39 anos	0	0,00
4	40 a 49 anos	1	3,13
5	50 a 59 anos	11	34,38
6	60 a 69 anos	13	40,63
7	70 a 79 anos	6	18,75
8	80 anos ou mais	0	0,00
	TOTAL	32	100,00

FONTE: ELABORADA PELO AUTOR, 2022.

Escolaridade

Conforme apresentado na TABELA 3, a maior frequência de vítimas de golpes financeiros no quesito escolaridade foi do Curso Superior Completo, com 46,88% (n=15). Com Pós-Graduação (Especialização), aparecem 4 vítimas, equivalente a 12,50%. Considerando estes dois grupos, temos 59,38% (n=19) com Superior Completo. Em segundo lugar o estudo mostrou que 25% (n=8) têm Ensino Médio.

Este resultado vai ao encontro do que DeLiema *et al.,* (2020) encontraram: um elevado grau de instrução e alto poder aquisitivo não são fatores capazes de tornar as pessoas imunes a golpes. Também nessa direção, o estudo de Kadoya *et al.,* (2021) mostra não haver correlação entre a escolaridade e a probabilidade de se tornar vítima de fraude financeira.

Já Judges *et al.,* (2017) encontraram que entre as vítimas de golpes, a maior frequência foi de idosos com curso superior (49%), e com escolaridade até o ensino médio representaram 21,6%.

TABELA 3 - DISTRIBUIÇÃO DA AMOSTRA POR ESCOLARIDADE.

	ESCOLARIDADE	FREQUÊNCIA	%
1	Analfabeto	0	0,00
2	Analfabeto funcional	0	0,00
3	Ensino fundamental incompleto	1	3,13
4	Ensino fundamental	1	3,13
5	Ensino médio incompleto	1	3,13
6	Ensino médio	8	25,00
7	Técnico/ profissionalizante incompleto (nível médio)	0	0,00
8	Técnico/ profissionalizante (nível médio)	0	0,00
9	Superior incompleto	2	6,25
10	Superior completo	15	46,88
11	Pós-Graduação (Especialização)	4	12,50
12	Pós-Graduação (Mestrado)	0	0,00
13	Pós-Graduação (Doutorado)	0	0,00
	Total	32	100,00

FONTE: ELABORADA PELO AUTOR, 2022.

Renda Bruta Mensal

O resultado da amostra quanto à renda mensal bruta das vítimas de golpes financeiros (TABELA 4), não oferece subsídios suficientes para a avaliação do comprometimento pelas perdas, conforme previsto no projeto deste trabalho. Isto porque a renda comprovada pelos clientes na abertura da conta, e constante nos registros do sistema da Instituição Financeira, pode estar desatualizada e não representar o total de ganhos de cada cliente. Além disso, num passado recente, em alguns processos de abertura de conta, a apresentação de comprovante de renda era flexibilizada.

O que é possível observar na TABELA 4, apesar das limitações referidas, é que o predomínio de golpes financeiros ocorreu em vítimas com renda até R$ 3.300,00 (40,63%, n=13) e em segundo lugar, vítimas com renda entre R$ 6.601,00 e R$ 9.900,00 com 25,00% (n=8).

TABELA 4 - DISTRIBUIÇÃO DA AMOSTRA POR RENDA BRUTA COMPROVADA.

	FAIXA DE RENDA MENSAL COMPROVADA	FREQUÊNCIA	%
1	R$ 0,00 R$ 1.100,00	3	9,38
2	R$ 1.101,00 a R$ 3.300,00	10	31,25
3	R$ 3.301,00 a R$ 6.600,00	6	18,75
4	R$ 6.601,00 a R$ 9.900,00	8	25,00
5	R$ 9.901,00 a R$ 13.200,00	1	3,13
6	R$ 13.201,00 a R$ 16.500,00	3	9,38
7	R$ 16.501,00 a R$ 19.800,00	0	0,00
8	R$ 19.801,00 ou mais	1	3,13
	TOTAL	32	100

FONTE: ELABORADA PELO AUTOR, 2022.

Valores das Perdas Financeiras

Na distribuição da amostra quanto às perdas financeiras (TABELA 5), observa-se que a maior parte dos valores ficaram concentrados nas faixas de R$ 1.100,00 a R$ 3.300,00 e de R$ 3.301,00 a R$ 6.600,00, representando 62,50%. Consultando os dados individuais da amostra, constatou-se que a vítima com perda financeira na faixa acima de R$ 19.801,00 ou mais, teve prejuízo de R$ 64.905,70, e, este cliente possui apenas 22 anos de idade.

Esse resultado vai de encontro com o estudo de Payne (2020), sobre o impacto da pandemia em adultos acima de 50 anos quanto aos golpes financeiros. Neste, relata que pessoas mais velhas são alvos de crimes cibernéticos com mais frequência, e que, embora tenha ocorrido aumentos dos golpes em todas as faixas etárias, esse grupo sofreu maior perda financeira.

TABELA 5 - DISTRIBUIÇÃO DA AMOSTRA POR VALORES DAS PERDAS FINANCEIRAS.

	FAIXA DE PERDA	FREQUÊNCIA	%
1	R$ 0,01 R$ 1.100,00	5	15,63
2	R$ 1.101,00 a R$ 3.300,00	10	31,25
3	R$ 3.301,00 a R$ 6.600,00	10	31,25
4	R$ 6.601,00 a R$ 9.900,00	4	12,50
5	R$ 9.901,00 a R$ 13.200,00	2	6,25
6	R$ 13.201,00 a R$ 16.500,00	0	0,00
7	R$ 16.501,00 a R$ 19.800,00	0	0,00
8	R$ 19.801,00 ou mais	1	3,13
	Total	32	100,00

FONTE: ELABORADA PELO AUTOR, 2022.

LIMITAÇÕES DA PESQUISA

Para o desenvolvimento da pesquisa foram encontrados alguns fatores limitantes, tais como:

- a demanda maior de tempo para a obtenção dos dados;
- a necessidade de alterar o enfoque da pesquisa pela dificuldade na obtenção dos dados previstos no projeto, pois a busca desses dados envolveu acesso a sistemas restritos de diferentes departamentos, que teve como consequência uma amostra com n reduzido.
- dificuldade na obtenção de produções científicas, especialmente as relacionadas às medidas adotadas pelas instituições bancárias para enfrentamento dos golpes financeiros.

CONCLUSÃO

Os avanços tecnológicos têm proporcionado muitas facilidades para seus usuários. A comunicação digital, por exemplo, tem evoluído de forma disruptiva, a ponto de chamadas de vídeo que até poucos anos se tratava de ficção científica, esteja acessível com alguns toques no celular utilizando-se o *WhatsApp*. No mesmo caminho, o PIX trouxe uma instantaneidade nas transações financeiras até então inimaginável, inclusive entre bancos. No entanto, trouxeram consigo oportunidades que facilitaram a prática de criminosos, que cada vez mais fazem vítimas entre os clientes bancários.

Com esse trabalho se buscou conhecer o perfil das vítimas nas características de gênero, faixa etária, escolaridade, faixa de renda e faixa de perda financeira. A partir da definição do perfil, pode ser possível traçar planos de prevenção direcionados para cada perfil mais atingido pelos golpes, assumindo que cada grupo pode responder melhor às campanhas de prevenção se utilizado um canal e formato adequados as suas especificidades. Por exemplo, idosos sem familiaridade com dispositivos eletrônicos provavelmente não absorveriam alertas anti-fraude enviados por SMS, mas uma correspondência física ou uma ligação informativa talvez tivessem maior efetividade. Por outro lado, jovens poderiam aproveitar a disponibilidade do WhatsApp para receber informativos atualizados sobre os golpes virtuais e assim diminuir ainda mais a chance de se tornarem vítimas.

Ao término desse trabalho, reforça-se a necessidade de mais estudos sobre a problemática que envolve os golpes financeiros de Engenharia Social, tanto do ponto de vista das vítimas como das instituições financeiras. Considera-se que para tal, os novos estudos devam ter um enfoque multidisciplinar, com a participação de psicólogos, psiquiatras, profissionais de tecnologia da informação e administradores, por exemplo. Além disso, deve ser buscada a totalidade dos registros de golpes de Engenharia Social na Instituição e, a partir disto, traçar perfis mais específicos dos clientes potencialmente mais vulneráveis.

Os resultados encontrados serão apresentados à Instituição Financeira para suscitar o debate e colaborar com a criação de novas políticas de prevenção.

REFERÊNCIAS

10 DICAS ANTIGOLPE. **FEBRABAN**, 2021. Disponível em < https://antifraudes.febraban.org.br/?gclid=Cj0KCQjwiNSLBhCPARIsAKNS4_ea3_CEFURviFrzzvWdVsAdBbONNQSTmMviKozKk7nU-MrNLH0hicQaAtUPEALw_wcB>. Acesso em: 17 de out. 2021.

ALEROUD, Ahmed; ZHOU, Lina. Phishing environments, techniques, and countermeasures: A survey. **Computers & Security 68,** 160–196, 2017. ELSEVIER. DOI: http://dx.doi.org/10.1016/j.cose.2017.04.006. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404817300810?via%3Dihub. Acesso em: 30 de ago. 2021.

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: 20 de out. 2021.

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/rege521. Disponível em: file:///C:/Users/usuario/Downloads/99921-Article%20Text-174185-1-10-20150702.pdf. Acesso em: 03 de dez. 2021.

BITAAB, Marzieh et al. Scam Pandemic: How Attackers Exploit Public Fear through Phishing. **ArXiv,** v. 1, 2021. Disponível em: https://arxiv.org/abs/2103.12843. Acesso em: 30 de ago. 2021.

BRASIL. Tribunal de Justiça de São Paulo. **Apelação**. Processo AC 1006806-26.2019.8.26.0533 SP 1006806-26.2019.8.26.0533. Golpe do motoboy – sentença de improcedência. 37ª Câmara de Direito Privado. Relator Sergio Gomes. Julgamento 29/06/2021. Publicação 15/07/21. Disponível em: < https://tj-sp.jusbrasil.com.br/jurisprudencia/1248634399/apelacao-civel-ac-10068062620198260533-sp-1006806-2620198260533 >. Acesso em: 30 de ago. 2021.

BUENO, Rejane; IKEDA, Ana Akemi. Segmentação de consumidores de produtos e serviços bancários: um estudo exploratório. **Revista Brasileira de Marketing**, v. 12, n. 2, p. 133-157, abr./jun. 2013. DOI: 10.5585/remark.v12i2.2333. Disponível em: https://periodicos.uninove.br/remark/article/view/11995. Acesso em: 02 de dez. 2021.

BURNES, David et al. Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis**. American Journal of Public Health**, Aug;107(8):e13-e21, 2017. DOI:10.2105/AJPH.2017. 303821. Disponível em: https://pubmed.ncbi.nlm.nih.gov/28640686/. Acesso em: 30 de ago. 2021.

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 dez. 2021.

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 mai. 2022.

DAIKU, Yasuhiro, et al. Effective forewarning requires central route processing: Theoretical improvements on the counterargumentation hypothesis and practical implications for scam prevention. **PLoS ONE** 15(3): e0229833. 2020. DOI: https://doi.org/10.1371/journal.pone.0229833. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0229833. Acesso em: 20 de out. 2021.

DELIEMA, 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. 2021.

Dicas de segurança. BRADESCO. Disponível em: https://www.bradescoseguranca.com.br/html/seguranca_corporativa/pf/dicas-de-seguranca/index.shtm. Acesso em: 03 de dez. 2021.

DINISMAN, Tamar; MOROZ, Ania. Understanding victims of crime: The impact of the crime and support needs. **Victim Suport, 2017.** DOI: 10.13140/RG.2.2.17335.73124. Disponível em: https://www.researchgate.net/publication/316787563_Understanding_victims_of_crime_The_impact_of_the_crime_and_support_needs. Acesso em: 6 de nov. 2021.

DO PRADO, Yolanda Cardoso et al. Whatsapp: prevenção à fraude e redução de custos em empresas de cartões de crédito. **Administração de Empresas em Revistas**, v. 2, n. 21, 403-420, 2020. ISSN: 2316-7548. Disponível em: http://revista.unicuritiba.edu.br/index.php/admrevista/article/view/4325/371372602. Acesso em: 02 de abr. 2022

FEBRABAN e Ministério da Justiça discutem criar Estratégia Nacional de Combate ao Crime Cibernético. **FEBRABAN,** São Paulo 2021. Disponível em: < https://portal.febraban.org.br/noticia/3682/pt-br/>. Acesso em: 11 de set. 2021.

FERREIRA, Márcio; KAWAKAMI, Cynthia. Ransomware - Kidnapping personal data for ransom and the information as hostage. Advances in Distributed Computing and Artificial Intelligence Journal, v. 7, n. 3, 5-14, 2018. DOI: http://dx.doi.org/10.14201/ADCAIJ201873514. Acesso em: 08 de mai. 2022.

GAVILAN, Diana et al. Vividness of news push notifications and users' response. **Technological Forecasting and Social Change,** v 161; 2020. DOI: https://doi.org/10.1016/j.techfore.2020.120281. Disponível em: https://www.sciencedirect.com/science/article/pii/S0040162520311070?via%3Dihub. Acesso em: 30 de ago. 2021.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008. cap. 3 p 28. ISBN 978-85-224-5142-5.

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: 18 de out. 2021.

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 mai. 2022.

GUERRA, Diego de Souza; OLETO, Alice de Freitas; PEÑALOZA, Verónica. A relação entre satisfação e lealdade em multicanais: uma reavaliação dos fatores confiança, valor e custo de mudança no setor bancário brasileiro. **Revista de Administração de Roraima-UFRR**, v. 8, n. 2, p. 442-460, jul-dez. 2018. DOI: 10.18227/2237-8057rarr.v8i2.5182. Disponível em: http://revista.ufrr.br/index.php/adminrr/. Acesso em: 02 de dez. 2021.

HAN, Weijie et al. Review: Build a Roadmap for Stepping Into the Field of Anti-Malware Research Smoothly. IEEE Access, v. 7, 143573 – 143596, out, 2019. DOI: 10.1109/ACCESS.2019.2945787. Acesso em: 08 de mai. 2022.

JUDGES, Rebecca A. et al. The role of cognition, personality, and trust in fraud victimization in older adults. **Frontiers in Psychiatry**, v. 8, art. 588, abr, 2017. DOI: 10.3389/fpsyg.2017.00588. Disponível em: https://www.frontiersin.org/articles/10.3389/fpsyg.2017.00588/full. Acesso em: 23 de mar. 2022.

KADOYA, Yoshihiko et al. Who is next? A study on victims of financial fraud in Japan. **Frontiers in Psychiatry**, v. 12, art. 649565, jul, 2021. DOI: 10.3389/fpsyg.2021.649565. Disponível em: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.649565/full. Acesso em: 10 de abr. 2022.

LEVESQUE, Terrence; McDOUGALL, Gordon H.G. Determinants of customer satisfaction in retail banking. **International Journal of Bank Marketing**, v. 14, n. 7, p. 12-20, 1996. ISSN 0265-2323. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/02652329610151340/full/html. Acesso em: 02 de dez. 2021.

MALAMED, David. Victims of fraud: Scams can destroy their prey financially, physically and emotionally. So forensic accountants need to deal with victims on a human level. **CA magazine,** Canadá, p 34-36, jun./jul. 2013.

NORRIS, Gareth; BROOKES, Alexandra. Personality, emotion and individual differences in response to online fraud. **Personality and Individual Differences.** V. 169, 2021. DOI: https://doi.org/10.1016/j.paid.2020.109847. Disponível em: https://www.sciencedirect.com/science/article/pii/S0191886920300374?via%3Dihub. Acesso em: 7 de nov. 2021.

PAYNE, Brian K. Criminals work from home during pandemics too: a public health approach to respond to fraud and crimes against those 50 and above. **American Journal of Criminal Justice**, v. 45, 563–577, jun, 2020. DOI: https://doi.org/10.1007/s12103-020-09532-6. Disponível em: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7274935/. Acesso em: 15 de mar. 2022.

PIX. **Banco Central**, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix. Acesso em: 08 de mar. 2022.

Prevenção a Crimes Cibernéticos. **Polícia Civil do Estado de São Paulo**. 2021. Disponível em: https://www.policiacivil.sp.gov.br/portal/faces/pages_home/noticias/crimesCiberneticos?_afrLoop=265629857488559&_afrWindowMode=0&_afrWindowId=1by85ip6cg_1#!%40%40%3F_afrWindowId%3D1by85ip6cg_1%26_afrLoop%3D265629857488559%26_afrWindowMode%3D0%26_adf.ctrl-state%3D1by85ip6cg_73. Acesso em: 03 de dez. 2021.

QABALIN, Majdi et al. Credit cards theft using social engineering over whatsapp: a survey study. **22nd International Arab Conference on Information Technology (ACIT)**, 78-1-6654-1995-6/21, 2021. DOI: 10.1109/ACIT53391.2021.9677454. Disponível em: file:///C:/Users/usuario/Downloads/Majdi%20Qabalin%20Credit_Cards_Theft_Using_Social_Engineering_over_WhatsApp_A_Survey_Study.pdf. Acesso em: 15 de abr. 2022.

RAAIJ, W. Fred van. **Understanding Consumer Financial Behavior Money Management in an Age of Financial Illiteracy**. 1. ed. Palgrave Macmillan, 2016. cap 9 p 113-114 DOI: DOI: 10.1057/9781137544254. Disponível em: https://link.springer.com/book/10.1057/9781137544254. Acesso em: 15 de out. 2021.

Segurança. **ITAÚ**. Disponível em: https://www.itau.com.br/seguranca/. Acesso em: 03 de dez. 2021.

Segurança caixa. **CAIXA.** Disponível em: https://www.caixa.gov.br/seguranca/Paginas/default.aspx. Acesso em 03 de dez. 2021.

SOBRE O WHASTAPP. **Whatsapp**, 2022. Disponível em: https://www.whatsapp.com/about. Acesso em: 08 de mar. 2022.

SUSHRUTH, Venkatesha et al. Social Engineering Attacks During the COVID19 Pandemic. **SN Computer Science,** 2:78; 2012. DOI: https://doi.org/10.1007/s42979-020-00443-1. Disponível em: https://link.springer.com/article/10.1007/s42979-020-00443-1. Acesso em: 30 de ago. 2021.

TASINAFFO, Flávio. Quem quer ser um milionário? Golpe do bilhete premiado ainda faz vítimas. **Blogosfera – Tudo golpe**, 2019. Disponível em: https://tudogolpe.blogosfera.uol.com.br/2019/10/12/quem-quer-ser-um-milionario-golpe-do-bilhete-premiado-ainda-faz-vitimas/. Acesso em: 18 de nov. 2021.

TOMÁS, Gabriella Ramos; SILVA, Daniel Gustavo da. Limitações no Uso das TICs em Serviços Bancários: estudo exploratório sob a percepção do usuário. **Revista Gest@o.Org**, v. 17, Edição Especial, p. 178-195, 2019. DOI: http://dx.doi.org/10.21714/1679-18272019v17Esp.p178-195. Disponível em: https://periodicos.ufpe.br/revistas/gestaoorg/article/view/243593. Acesso em: 02 de dez. 2021.

UENO, Daisuke et al. Mild cognitive decline is a risk factor for scam vulnerability in older adults. **Frontiers in Psychiatry**, v. 12, art. 685451, dez, 2021. DOI: 10.3389/fpsyt.2021.685451. Disponível em: https://www.frontiersin.org/articles/10.3389/fpsyt.2021.685451/full. Acesso em: 12 de mar. 2022.

VITORIO, Tamires. Golpes financeiros explodem durante pandemia: veja quais são e como se prevenir. **CNN Brasil Business**, São Paulo 2021. Disponível em https://www.cnnbrasil.com.br/business/golpes-financeiros-explodem-durante-pandemia-veja-quais-sao-e-como-se-prevenir/. Acesso em: 20 de ago. 2021.

WASHO, Amy Hetro. An interdisciplinary view of social engineering: A call to action for research. **Computers in Human Behavior Reports,** 2451-9588; 2021. DOI: https://doi.org/10.1016/j.chbr.2021.100126. Disponível em: https://www.sciencedirect.com/science/article/pii/S2451958821000749?via%3Dihub. Acesso em: 30 de ago. 2021.

WHATSAPP É O APLICATIVO MAIS USADO PELOS BRASILEIROS; CONFIRA A LISTA. **G1 Globo**, 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/01/11/whatsapp-e-o-aplicativo-mais-utilizado-por-metade-dos-brasileiros-confira-a-lista.ghtml. Acesso em: 08 de mar. 2022.

ZACHARIAS, Maria Luiza Barcellos; FIGUEIREDO, Kleber Fossati; ALMEIDA, Victor Manoel Cunha de. Determinantes da satisfação dos clientes com serviços bancários. **RAE-eletrônica**, v. 7, n. 2, art. 18, jul./dez, 2008. DOI: https://doi.org/10.1590/S1676-56482008000200002. Disponível em: https://www.scielo.br/j/raeel/a/X8g6F7f7YVdDv3fjwzjzfXK/abstract/?lang=pt. Acesso em: 03 de dez. 2021.

APÊNDICE A - QUESTIONÁRIO PARA COLETA DE DADOS

Perfil de vítimas de golpes financeiros ocorridos com clientes de Instituição Financeira

O questionário a seguir deve ser preenchido com as informações cadastrais de cada cliente vítima de golpe financeiro, dentro do período de 1º de novembro a 30 de dezembro de 2021, a partir dos registros do sistema da Instituição.

01. Qual o gênero do (a) cliente vítima do golpe financeiro?

1. ( ) Feminino
2. ( ) Masculino

02. Qual a idade do (a) cliente que foi vítima do golpe financeiro?

1. ( ) até 18 anos
2. ( ) 19 a 29 anos
3. ( ) 30 a 39 anos
4. ( ) 40 a 49 anos
5. ( ) 50 a 59 anos
6. ( ) 60 a 69 anos
7. ( ) 70 a 79 anos
8. ( ) 80 anos ou mais

03. Qual a escolaridade do (a) cliente vítima do golpe financeiro?

1. ( ) Analfabeto
2. ( ) Analfabeto funcional
3. ( ) Ensino fundamental incompleto
4. ( ) Ensino fundamental
5. ( ) Ensino médio incompleto
6. ( ) Ensino médio
7. ( ) Técnico/ profissionalizante incompleto (nível médio)
8. ( ) Técnico/ profissionalizante (nível médio)
9. ( ) Superior incompleto
10. ( ) Superior completo
11. ( ) Pós-Graduação (Especialização)
12. ( ) Pós-Graduação (Mestrado)
13. ( ) Pós-Graduação (Doutorado)

04. Qual a renda mensal bruta do (a) cliente vítima do golpe financeiro?

1. ( ) menos de R$ 1.100,00
2. ( ) R$ 1.101,00 a R$ 3.300,00
3. ( ) R$ 3.301,00 a R$ 6.600,00
4. ( ) R$ 6.601,00 a R$ 9.900,00
5. ( ) R$ 9.901,00 a R$ 13.200,00
6. ( ) R$ 13.201,00 a R$ 16.500,00
7. ( ) R$ 16.501,00 a R$ 19.800,00
8. ( ) R$ 19.801,00 ou mais

05. Qual o percentual da perda das economias bancárias do (a) cliente vítima de golpe financeiro?

1. ( ) menos de R$ 1.100,00
2. ( ) R$ 1.101,00 a R$ 3.300,00
3. ( ) R$ 3.301,00 a R$ 6.600,00
4. ( ) R$ 6.601,00 a R$ 9.900,00
5. ( ) R$ 9.901,00 a R$ 13.200,00
6. ( ) R$ 13.201,00 a R$ 16.500,00
7. ( ) R$ 16.501,00 a R$ 19.800,00
8. ( ) R$ 19.801,00 ou mais