Curso de Tecnologia em Análise e Desenvolvimento de Sistemas

ENGENHARIA SOCIAL E LETRAMENTO DIGITAL: DESENVOLVIMENTO DE UMA FERRAMENTA DE CAPACITAÇÃO INTERATIVA PARA PREVENÇÃO AO GOLPE DO PIX NO WHATSAPP

Carlos Augusto Muniz de Queiroz[1]

RESUMO

Este artigo investiga a acentuada vulnerabilidade da população idosa a golpes de engenharia social no WhatsApp, com foco na fraude do "falso parente" para solicitação de PIX. A problemática central reside na carência de letramento digital direcionado, que gera insegurança e perdas financeiras. O objetivo do estudo é propor e descrever o desenvolvimento de uma ferramenta de capacitação digital interativa, desenhada especificamente para este público. A abordagem metodológica inicia com um diagnóstico qualitativo, utilizando o método de entrevista-persona para definir os requisitos da solução. O artefato resultante evoluiu de um infográfico estático para um protótipo funcional web, que guia o usuário por um processo mandatório de cinco etapas (Alerta, Pressão, Pausa, Verificação, Decisão). Os resultados demonstram que a ferramenta interativa, ao forçar o aprendizado sequencial, atende melhor às necessidades pedagógicas do público-alvo do que os métodos passivos. Conclui-se que a solução proposta oferece um mecanismo eficaz para mitigar o senso de urgência, principal gatilho do golpe, ao instituir um processo de verificação prático e fácil de memorizar.

Palavras-chave: engenharia social. letramento digital. pessoa idosa. metodologia interativa.

[1]Técnico em Eletrônica, Tecnólogo em Análise e Desenvolvimento de Sistemas pelo Centro Universitário Cidade Verde – UNICV; Pós Graduando em Engenharia da Computação pela Faculdade Focus. augusto_queiroz@id.uff.br

INTRODUÇÃO

A digitalização dos serviços financeiros no Brasil representa uma das transformações socioeconômicas mais rápidas e abrangentes das últimas décadas. No epicentro dessa mudança está o PIX, o sistema de pagamentos instantâneos do Banco Central, que, desde seu lançamento em novembro de 2020, redefiniu a maneira como pessoas e empresas transacionam valores. Em 2024, o PIX consolidou sua hegemonia, registrando 63,8 bilhões de transações, um volume que supera a soma de todas as outras modalidades de pagamento, como cartões de crédito, débito e boletos.[1] A conveniência é inegável: atualmente, 82% das transações bancárias no país são realizadas por canais digitais, com o celular respondendo por 75% desse total.[2]

Contudo, essa migração massiva para o ambiente digital, embora tenha promovido a inclusão financeira e a eficiência, também expandiu drasticamente a superfície de ataque para atividades criminosas. A mesma instantaneidade que facilita o comércio e a vida cotidiana tornou-se uma ferramenta poderosa nas mãos de fraudadores. Nesse novo ecossistema, emergiu uma modalidade de crime particularmente insidiosa e prevalente: o "Golpe do Falso Parente", também conhecido como "Golpe do Número Novo". Esta fraude se destaca por não explorar falhas tecnológicas complexas, mas sim as vulnerabilidades mais intrínsecas da natureza humana: a confiança, o afeto e o desejo de ajudar entes queridos.[3] Utilizando a engenharia social como principal arma, os criminosos manipulam suas vítimas através do WhatsApp para obter transferências via PIX, causando prejuízos financeiros e emocionais significativos.

Este artigo tem como objetivo fornecer uma pesquisa aprofundada deste fenômeno, servindo como um documento de base para o projeto de extensão universitária "Capacitação em Segurança Digital no WhatsApp", conduzido por Carlos Augusto Muniz de Queiroz, profissional com formação tecnológica superior em Análise e Desenvolvimento de Sistemas pelo UNICV - Centro Universitário Cidade Verde, de Maringá/PR.

Ao longo dos capítulos seguintes, será dissecada a anatomia do golpe, apresentado o cenário quantitativo da fraude digital no Brasil, analisada a vulnerabilidade específica da população idosa, detalhadas as estratégias de defesa e prevenção, e delineados os mecanismos de ação e recurso disponíveis para as vítimas. A finalidade é construir um panorama completo que possa subsidiar e

validar as ferramentas educacionais desenvolvidas no âmbito do referido projeto, contribuindo para a criação de um ambiente digital mais seguro para todos os cidadãos.

REFERENCIAL TEÓRICO

Capítulo 1: A anatomia do golpe: Engenharia social

O "Golpe do Falso Parente" é um exemplo paradigmático de como a simplicidade pode ser a característica mais perigosa de uma fraude digital. Seu sucesso não reside em complexidade técnica, mas na execução metódica de um roteiro de manipulação psicológica que explora a confiança e a urgência. A compreensão de seu funcionamento, passo a passo, é o primeiro e mais crucial elemento para a construção de defesas eficazes.

A engenharia social utiliza técnicas de persuasão que abusam da confiança ou do medo das vítimas para obter informações confidenciais (MITNICK; SIMON, 2003)[50]. No contexto digital, essa abordagem é adaptada para explorar a vulnerabilidade específica de grupos como o de pessoas idosas. Conforme aponta Morgado (2024)[47], os idosos são frequentemente classificados como "imigrantes digitais", pois necessitaram aprender a usar as tecnologias já na vida adulta, tornando-os mais suscetíveis a ataques que exploram a falta de familiaridade com o ambiente digital.

1.1 O passo a passo da fraude: A simplicidade perigosa

A execução do golpe segue um padrão notavelmente consistente, que pode ser dividido em quatro fases distintas:

Fase 1: Obtenção de dados e criação do perfil falso

O processo inicia-se com uma fase de "inteligência". O criminoso seleciona uma pessoa a ser personificada e coleta informações básicas e essenciais. A principal fonte de dados são as redes sociais com perfis públicos, de onde extraem a foto de perfil e o nome completo da vítima.[4] Em posse desses elementos, o golpista adquire um novo chip de celular e cria uma conta no WhatsApp, configurando-a com a foto e o nome da pessoa que será falsamente representada.

Fase 2: O contato inicial e a justificativa

Com o perfil falso ativo, o criminoso começa a contatar pessoas do círculo próximo da vítima, como familiares e amigos. A abordagem inicial é projetada para

ser casual e não levantar suspeitas. Uma mensagem típica é: "Oi! Troquei de celular, pode salvar o meu número novo na sua agenda. O outro vou deixar só para trabalho".[4] A justificativa para a troca de número é um elemento-chave para a credibilidade do golpe. As narrativas mais comuns incluem histórias como "meu celular foi danificado em uma queda e eu o levei para a assistência técnica" ou "o aparelho molhou e não tem conserto".[3] A simplicidade desse evento no cotidiano moderno é o que permite ao golpista passar pelo primeiro filtro de desconfiança da vítima.

Fase 3: Construção de credibilidade e o pedido urgente

Uma vez estabelecido o contato inicial, o golpista pode trocar algumas mensagens para simular normalidade e reforçar a crença de que o interlocutor é, de fato, o parente ou amigo.[3] Após essa breve interação, o ataque começa. O criminoso inventa uma situação de emergência que requer uma transferência financeira imediata via PIX. A desculpa mais frequente é a suposta incapacidade de acessar o próprio aplicativo bancário no "aparelho novo", solicitando que o alvo faça um pagamento em seu nome com a promessa de reembolso posterior.[3]

Fase 4: A transação e a confirmação

A vítima, agora convencida da identidade do interlocutor e pressionada pela urgência da situação, é instruída a realizar a transferência para uma chave PIX fornecida pelo golpista. Um ponto crítico de verificação que poderia expor a fraude é o fato de que o nome do destinatário do PIX será diferente do nome do parente. No entanto, os criminosos antecipam essa checagem e apresentam justificativas adicionais, como "a conta é de um terceiro a quem devo" ou "estou usando a conta de um amigo porque a minha está bloqueada". Pressionada, a vítima muitas vezes ignora essa inconsistência e completa a transação.[7]

1.2 A psicologia da manipulação que explora vínculos e emoções

O golpe do "falso parente" via WhatsApp explora diretamente o gatilho mental da urgência e o laço afetivo. O criminoso se passa por um familiar próximo, geralmente filho ou sobrinho, alegando uma emergência (como a necessidade de pagar uma conta imediata) para solicitar uma transferência via PIX. O próprio governo federal, através de materiais de orientação, já mapeou essa prática (BRASIL, 2024)[49]. A engenharia social empregada se baseia em três pilares:

Gatilho da urgência e pressão: A narrativa é sempre construída em torno de uma necessidade imediata e inadiável ("preciso pagar uma conta que vence hoje",

"estou no meio de uma compra e meu cartão não passou"). Esse senso de urgência fabricado tem o propósito de induzir um estado de estresse na vítima, o que comprovadamente inibe o pensamento crítico e a análise cuidadosa da situação.[6]

Exploração do vínculo afetivo: Ao se passar por um filho, mãe, irmão ou amigo próximo, o golpista ativa a predisposição natural do ser humano para ajudar seus entes queridos. A resposta da vítima deixa de ser puramente lógica e passa a ser predominantemente emocional. A preocupação e o desejo de resolver o problema do familiar se sobrepõem a quaisquer sinais de alerta.[3]

Normalização da situação: A premissa inicial do golpe, a troca de um número de celular, é um evento tão comum que a abordagem se torna plausível. Essa normalidade cria uma "capa de invisibilidade" para a intenção maliciosa, fazendo com que a vítima baixe a guarda antes mesmo de o pedido financeiro ser feito. A fraude se esconde à vista de todos, disfarçada de um inconveniente cotidiano.

O *modus operandi* deste golpe é quase sempre o mesmo, focando na criação de uma emergência fictícia. Sobre isso, a cartilha de enfrentamento à violência patrimonial orienta:

> *Dessa forma, a estratégia para se livrar desse golpe é manter a calma e tentar descobrir mais informações desse suposto 'sobrinho ou sobrinha': pergunte o nome, pergunte de quem é filho, onde ela se encontra, entre outras características que o ajudem a confirmar se é realmente o seu parente que está te ligando.* (BRASIL, 2024, p. 33) [49].

Esta abordagem, baseada na "pausa" e "verificação", é a mesma utilizada como pilar na ferramenta de capacitação desenvolvida neste trabalho.

1.3 A coleta de informações: O rastro digital como munição para os golpes

Os criminosos não escolhem seus alvos ao acaso. Eles realizam um trabalho prévio de coleta de informações, utilizando fontes diversas para aumentar a autenticidade de seus ataques:

Fontes abertas (OSINT - Open Source Intelligence): As redes sociais são a principal mina de ouro. Perfis abertos ou com configurações de privacidade frouxas podem revelar um "dossiê" completo sobre um indivíduo: fotos de perfil, nomes de parentes (através de marcações e comentários), círculos de amizade, locais frequentados e até detalhes da rotina.[4]

Vazamentos de dados (Data Leaks): Grandes vazamentos de dados de empresas e serviços online disponibilizam ilegalmente informações como nomes completos, CPFs, e-mails e números de telefone na *dark web*. Os criminosos podem comprar esses bancos de dados e cruzar informações para identificar alvos e seus contatos.[6]

Engenharia social direta: Em alguns casos, o próprio golpista pode, durante a conversa inicial, fazer perguntas sutis para extrair nomes de outros familiares ou confirmar graus de parentesco, refinando o ataque em tempo real e tornando a farsa ainda mais convincente.[6]

1.4 Variações e táticas: clonagem e número novo

É fundamental para a compreensão do cenário distinguir entre as duas principais modalidades de fraude no WhatsApp, que muitas vezes são confundidas:

Golpe do número novo (falsificação de perfil): Esta é a tática descrita em detalhe neste capítulo e o foco principal do projeto de extensão. É tecnicamente mais simples, pois o criminoso apenas utiliza a foto e o nome da vítima em um número de telefone completamente novo. Ele não obtém acesso à conta original da vítima, que permanece sob seu controle.[4] Sua simplicidade o torna acessível a um grande número de criminosos.

Clonagem de WhatsApp (roubo de conta): Esta modalidade é tecnicamente mais complexa e invasiva. O golpista busca enganar a vítima para que ela forneça o código de verificação de 6 dígitos enviado por SMS pelo WhatsApp (geralmente sob o pretexto de confirmar um cadastro ou participar de uma promoção). Com esse código, o criminoso consegue ativar a conta da vítima em seu próprio aparelho, efetivamente roubando o acesso e podendo se comunicar com todos os contatos da agenda como se fosse a pessoa real.[9]

A prevalência do golpe do "número novo" pode ser atribuída justamente à sua baixa barreira técnica de entrada. Ele não requer a interação complexa para roubar um código de acesso, dependendo unicamente da habilidade de manipulação do fraudador. O golpe explora uma falha fundamental na forma como a identidade é percebida na comunicação digital. No mundo físico, a identidade é verificada por características únicas como a voz e a aparência. No WhatsApp, a foto de perfil tornou-se um substituto frágil e facilmente falsificável para a identidade autêntica. A narrativa do "celular quebrado" ou "problema no aparelho" é uma manobra genial dos criminosos, pois convenientemente elimina a possibilidade de uma verificação

por chamada de voz ou vídeo, que poderia desmascarar a farsa instantaneamente. Dessa forma, o golpe inverte o ônus da prova: em vez de o solicitante ter que provar sua identidade, a vítima, sob a pressão da urgência fabricada, sente-se na obrigação de ajudar, sem ter as ferramentas ou o tempo para uma verificação adequada.

Capítulo 2: Uma análise quantitativa do cenário da fraude digital no Brasil

A ascensão do "Golpe do Falso Parente" não é um evento isolado, mas sim o sintoma de uma epidemia de estelionato virtual que avança pelo Brasil. A análise de dados estatísticos de fontes autênticas, como o Fórum Brasileiro de Segurança Pública e a Federação Brasileira de Bancos (Febraban), revela a magnitude do problema, o impacto financeiro devastador e o perfil das vítimas, fornecendo um contexto quantitativo crucial para a relevância de iniciativas de capacitação em segurança, como a que está sendo produzida como fruto desta pesquisa.

2.1 Números e impacto da epidemia do estelionato virtual

Os números associados à fraude digital no Brasil são alarmantes e demonstram uma clara migração da atividade criminosa do mundo físico para o virtual, onde os riscos para os golpistas são menores e os retornos financeiros podem ser maiores.

Prevalência e prejuízos massivos: Uma pesquisa do Fórum Brasileiro de Segurança Pública revelou que, no período de um ano (entre julho de 2024 e junho de 2025), aproximadamente 24 milhões de brasileiros foram vítimas de golpes financeiros envolvendo PIX ou boletos bancários. O prejuízo financeiro estimado para a sociedade nesse período atingiu a cifra de quase R$ 29 bilhões.[12] A Febraban confirma essa tendência de crescimento, apontando que o volume de dinheiro perdido em golpes aumentou 17% de 2023 para 2024, saltando de R$ 8,6 bilhões para R$ 10,1 bilhões.[13]

Crescimento exponencial do estelionato: Os registros oficiais de estelionato mostram um crescimento acelerado. Em 2024, o Brasil registrou quase 2,17 milhões de ocorrências, o que equivale a uma média de 4 golpes por minuto. Esse número representa um aumento de 7,8% em relação ao ano anterior e um salto extremo em comparação com os 426,7 mil casos registrados em 2018, antes da popularização massiva do PIX. Especialistas afirmam que há uma relação direta entre a transformação digital da sociedade e o crescimento dos golpes.[14]

Posicionamento do golpe do WhatsApp: A fraude via WhatsApp figura consistentemente entre as mais comuns. A pesquisa Radar Febraban de março de 2025 posicionou o golpe em que "alguém se faz passar por um conhecido solicitando dinheiro por WhatsApp" como o segundo mais citado pelos brasileiros (28%), logo após a clonagem de cartão de crédito (40%).[15] Outros levantamentos da mesma federação, referentes a 2024, chegam a colocar o golpe do WhatsApp em primeiro lugar no ranking de fraudes mais relatadas aos bancos, com um volume estimado de 153 milhões de registros.[17] Embora as metodologias possam variar, o destaque desta modalidade de crime é inquestionável.

Essa escalada revela um paradoxo central da modernidade brasileira: as mesmas ferramentas tecnológicas que impulsionaram a inclusão financeira e a conveniência, como o PIX e o WhatsApp, tornaram-se os principais meios de vitimização e exclusão para os cidadãos digitalmente despreparados. A velocidade da inovação tecnológica superou a capacidade da educação em segurança digital de acompanhar o ritmo, criando um perigoso "déficit de segurança" que os criminosos exploram com eficiência.

2.2 Perfil demográfico das vítimas

Compreender quem são as vítimas é fundamental para direcionar as ações de prevenção. As pesquisas revelam um cenário complexo, onde a vulnerabilidade não está restrita a um único grupo demográfico, mas a natureza da fraude tende a variar de acordo com a idade e o perfil da vítima.

Perspectiva da Febraban: A pesquisa Radar Febraban indica que os grupos mais suscetíveis a golpes financeiros de forma geral são homens (44%), pessoas com 60 anos ou mais (42%) e indivíduos com ensino superior (41%).[15] O dado sobre o ensino superior pode parecer contraintuitivo, mas pode indicar que esse grupo possui maior bancarização, renda e atividade digital, aumentando sua exposição.

Perspectiva do DataSenado: Em contraponto, uma ampla pesquisa realizada pelo Instituto DataSenado com quase 22 mil pessoas revelou que os mais afetados numericamente por golpes virtuais em geral são os jovens na faixa de 16 a 29 anos, que correspondem a 27% das vítimas. A população com mais de 60 anos, embora frequentemente percebida como a mais vulnerável, representou 16% do total de vítimas.[20]

A aparente contradição entre os dados é esclarecida quando se analisa a *natureza* do golpe. Os jovens, por estarem mais tempo online e em busca de

oportunidades, tendem a ser vítimas de fraudes relacionadas a falsas promessas de emprego, ganhos fáceis e golpes em compras online. Por outro lado, a população idosa é o alvo preferencial de golpes de estelionato que exploram a confiança e a manipulação de vínculos afetivos, como a falsa central de atendimento bancário e, de forma proeminente, o golpe do falso parente.[12] Portanto, embora os jovens possam ser vitimados em maior número absoluto, os idosos são desproporcionalmente visados por fraudes que se alinham perfeitamente com o *modus operandi* do golpe do WhatsApp.

A simplicidade técnica do golpe do "número novo" contribui para sua escala massiva. Diferente de ataques cibernéticos que exigem conhecimento em programação ou *hacking*, esta fraude requer apenas habilidades de persuasão, um chip de celular e acesso a informações públicas em redes sociais. Essa baixa barreira de entrada "democratizou" o crime de estelionato, permitindo que um espectro muito mais amplo de criminosos participe da atividade. Essa realidade implica que as soluções não podem ser puramente tecnológicas (como antivírus), mas devem ser fundamentalmente comportamentais e educacionais, focadas em capacitar o indivíduo a reconhecer e resistir à manipulação, validando a abordagem de projetos de capacitação como o proposto.

2.3 Tabela 1: Ranking dos golpes financeiros mais comuns no Brasil

A tabela a seguir consolida dados de diferentes pesquisas da Febraban para oferecer uma visão clara da prevalência dos tipos de fraude financeira no país.

Posição no Ranking	Tipo de Golpe	Percentual / Número de Ocorrências	Fonte / Ano do Dado
1	Golpe da Clonagem de Cartão / Troca de Cartões	40%	Radar Febraban / Março 2025 [15]
2	Golpe do Falso Parente via WhatsApp	28%	Radar Febraban / Março 2025 [15]
3	Golpe da Falsa Central de Atendimento / Falso Funcionário	26%	Radar Febraban / Março 2025 [15]
4	Golpe do PIX (geral, incluindo Bug do PIX, etc.)	16%	Radar Febraban / Março 2025 [15]

1	Golpe do WhatsApp (clonagem ou perfil falso)	153 milhões de registros	Febraban / Dados de 2024 [17, 18]
2	Golpe da Falsa Venda	150 milhões de registros	Febraban / Dados de 2024 [17]
3	Golpe da Falsa Central Telefônica	105 milhões de registros	Febraban / Dados de 2024 [17]

Nota: As diferenças nos rankings e métricas (percentual vs. número de registros) refletem diferentes metodologias de pesquisa e períodos de coleta, mas consistentemente posicionam o golpe do WhatsApp entre os mais impactantes.

2.4 Tabela 2: Análise comparativa do perfil das vítimas de golpes virtuais

Esta tabela contrasta os perfis de vítimas identificados por diferentes pesquisas, destacando a natureza distinta das fraudes que afetam cada grupo demográfico.

Faixa Etária / Perfil	Percentual de Vítimas (DataSenado)	Perfil Suscetível (Radar Febraban)	Tipos de Golpes Prevalentes para o Grupo
Jovens (16-29 anos)	27%	Não destacado como principal	Falsas ofertas de emprego, golpes em compras online, promessas de ganhos fáceis.[20]
Idosos (60+ anos)	16%	42% (grupo mais suscetível)	Estelionato baseado em confiança: Falso parente, Falsa central bancária, Boletos falsos.[12]
Homens	Não especificado	44% (mais suscetíveis que mulheres)	Golpes financeiros em geral.[15]
Com Ensino Superior	Não especificado	41%	Golpes financeiros em geral.[15]

A análise comparativa dos dados fornece uma justificativa quantitativa robusta para focar os esforços de capacitação na população idosa. Embora não sejam as únicas vítimas, eles são desproporcionalmente visados por fraudes que exploram a confiança e a engenharia social, exatamente as características do "Golpe do Falso Parente".

PROCEDIMENTO METODOLÓGICOS

Capítulo 3: A vulnerabilidade da população idosa no ecossistema digital

A população idosa no Brasil encontra-se em uma posição de particular vulnerabilidade quando se refere à segurança digital. Essa fragilidade não decorre de uma incapacidade inerente, mas de uma convergência de fatores de vulnerabilidade social e de falta de capacitação técnica que criam um cenário ideal para a atuação de criminosos. A transição abrupta para um mundo digitalizado, sem o devido acompanhamento educacional, expôs esse grupo a riscos para os quais não estavam preparados.

É evidente que a proteção legal, embora necessária, não é suficiente para impedir a ação dos criminosos. A defesa mais eficaz é a prevenção ativa, que depende diretamente do nível de letramento digital do usuário. Braga, Silva e Gomes (2025)[48] argumentam que a efetividade das leis é limitada, tornando indispensável o fortalecimento de políticas públicas e, principalmente, de programas de educação digital e conscientização social focados neste público.

3.1 Fatores de risco

A análise da legislação brasileira, incluindo o Estatuto do Idoso e o Marco Civil da Internet, demonstra um avanço normativo. Contudo, "a efetividade ainda é limitada, sendo indispensável o fortalecimento de políticas públicas, programas de educação digital e iniciativas de conscientização social" (BRAGA; SILVA; GOMES, 2025, p. 1) [48]. Diversos elementos se combinam para agravar a vulnerabilidade dos idosos a crimes cibernéticos, com destaque para os seguintes:

Analfabetismo e baixo letramento digital: A falta de familiaridade com as ferramentas e a lógica do ambiente digital é o fator de risco mais notável. Muitos idosos não compreendem conceitos básicos de segurança, como a verificação de identidade, os perigos de links desconhecidos ou a facilidade com que informações podem ser falsificadas online.[21] Uma avaliação da Controladoria-Geral da União (CGU) com beneficiários do INSS, por exemplo, concluiu que a pouca familiaridade com aplicativos governamentais e a dificuldade em verificar extratos online os tornavam alvos fáceis para descontos indevidos e outras fraudes.[22]

Isolamento social e confiança como fator de risco: O isolamento social, uma realidade para muitos idosos, pode aumentar a dependência de interações

online e a suscetibilidade à manipulação. Adicionalmente, esse grupo tende a operar com um nível de confiança interpessoal mais elevado, uma característica socialmente valorizada no mundo analógico, mas que se torna uma perigosa vulnerabilidade no ambiente digital anônimo. A "confiança excessiva nas informações recebidas online" é apontada como um dos principais motivos que os tornam alvos fáceis.[21]

O impacto da pandemia de COVID-19: A pandemia de COVID-19 acelerou a adesão da população idosa às plataformas digitais, para manter contato com familiares, realizar compras e acessar serviços bancários, muitos tiveram que adotar tecnologias digitais, mas essa rápida migração não foi acompanhada pelo letramento em segurança. De fato, “Os idosos são considerados imigrantes digitais pois tiveram de aprender a lidar com as tecnologias digitais durante o seu surgimento e por isso são mais vulneráveis frente aos ataques digitais” (MORGADO, 2024, p. 87)[47]. A Febraban relatou um aumento de 60% nas tentativas de golpes financeiros contra idosos durante a pandemia, um dado que ilustra claramente o impacto desse fenômeno.[23]

A vulnerabilidade dos idosos, portanto, não é meramente uma questão de "não saber usar a tecnologia". Trata-se de um profundo choque cultural. Eles foram socializados em um ambiente onde a palavra, o aperto de mão e a confiança mútua eram os pilares das interações. Os criminosos digitais exploram essa "boa-fé pré-digital", que não pressupõe a necessidade de verificação constante que o ceticismo saudável do mundo online exige. Uma capacitação eficaz, portanto, deve ir além de ensinar a clicar em botões; ela precisa inserir um novo conjunto de hábitos comportamentais adaptados à realidade digital.

3.2 O impacto humano: Relatos e consequências

As estatísticas ganham uma dimensão humana quando observadas através dos relatos das vítimas. Esses casos concretos ilustram como as táticas de engenharia social se materializam em perdas reais e profundo abalo emocional.

Estudo de caso 1: A preocupação maternal explorada: O relato de uma idosa de 64 anos que perdeu mais de R$ 5.000 é emblemático. Ela recebeu uma mensagem de um número desconhecido com a foto de seu filho, alegando ter trocado de aparelho. O golpista afirmou ter dificuldades para acessar o aplicativo do banco e pediu ajuda para pagar boletos urgentes. Movida pela preocupação, a mãe realizou duas transferências via PIX. Ela só percebeu o golpe no dia seguinte,

quando o criminoso tentou solicitar mais dinheiro.[6] Este caso demonstra a exploração direta do vínculo afetivo e do instinto de proteção maternal.

Estudo de caso 2: A persistência do criminoso: Em outro caso, uma mulher de 50 anos foi abordada por um suposto parente e, sendo tão convincente a conversa, realizou duas transferências bancárias antes de se dar conta da fraude.[6] Este exemplo ilustra como os golpistas podem ser persistentes, extraindo múltiplos pagamentos de uma mesma vítima ao manter a farsa por mais tempo.

As consequências desses golpes transcendem a perda financeira. As vítimas frequentemente experimentam sentimentos de vergonha, culpa e violação da confiança. O medo de usar a tecnologia, que muitas vezes já era uma barreira, intensifica-se, podendo levar a um maior isolamento digital e social. Este ciclo vicioso do medo é perigoso: o medo gera ansiedade, que por sua vez reduz a capacidade de raciocínio lógico. Quando um golpista aciona um gatilho de pânico (a urgência), uma vítima que já possui um medo latente da tecnologia tem maior probabilidade de agir por impulso para "resolver" a crise, em vez de pausar para verificar. Uma capacitação que oferece um plano de ação claro, como um protocolo passo a passo, é fundamental para quebrar esse ciclo, transformando o medo paralisante em vigilância produtiva e empoderamento.

3.3 Mapeamento de iniciativas de inclusão e educação digital

A crescente conscientização sobre a vulnerabilidade digital dos idosos tem motivado a criação de diversas iniciativas públicas e privadas com o objetivo de promover a inclusão e a segurança digital.

Ações governamentais e legislativas: Em nível municipal, a Prefeitura de Vitória (ES) lançou o projeto "60+ Conectados / Clique Seguro", que oferece oficinas gratuitas de capacitação para idosos, em parceria com o Senai-ES, abordando temas como navegação segura e identificação de riscos.[25] No âmbito legislativo, tramitam projetos de lei, como em Goiás, que visam instituir campanhas permanentes de orientação para a pessoa idosa contra fraudes e golpes na internet e por aplicativos.[24] A própria Anatel também promove campanhas periódicas com dicas de segurança online para este público.[26]

Programas de inclusão e conteúdo educacional: Existem diversos programas focados na inclusão digital, como o "Navegando na Internet na Melhor Idade" no Espírito Santo, que buscam não apenas ensinar o uso das ferramentas, mas também os cuidados necessários para uma navegação segura.[27] Entidades

como a Serasa e empresas de cibersegurança também produzem conteúdo educativo com dicas práticas, como desconfiar de ofertas muito vantajosas, manter softwares atualizados e a importância da educação contínua para se manter a par das novas ameaças.[28]

Essas iniciativas, embora valiosas, ainda são pontuais e demonstram a enorme demanda por projetos de capacitação estruturados e de fácil acesso, como o proposto no âmbito desta extensão universitária. O alinhamento com uma necessidade pública já reconhecida reforça a relevância e o potencial de impacto positivo do projeto.

APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Capítulo 4: Um guia prático de prevenção e estratégias de defesa

A defesa contra o golpe do falso parente e outras fraudes digitais baseadas em engenharia social exige uma abordagem dupla: o fortalecimento das barreiras técnicas e, de forma ainda mais crucial, a adoção de um protocolo comportamental de verificação. A tecnologia pode oferecer uma camada de proteção, mas a decisão final de transferir o dinheiro é humana. Portanto, a capacitação do indivíduo é a linha de defesa mais importante.

4.1 Criando barreiras digitais essenciais

Antes mesmo que uma tentativa de golpe ocorra, os usuários podem tomar medidas técnicas simples, mas eficazes, para proteger suas contas e informações, dificultando a ação dos criminosos.

Ativação da verificação em duas etapas no WhatsApp: Esta é a medida mais importante para se proteger contra a *clonagem* de contas. Ao ativar este recurso (em Configurações > Conta > Verificação em duas etapas), o usuário cria uma senha de 6 dígitos (PIN) que será solicitada periodicamente pelo aplicativo. Isso impede que um criminoso, mesmo que obtenha o código de verificação por SMS, consiga ativar a conta em outro aparelho sem saber o PIN.[6] Embora não impeça o golpe do "número novo", protege a integridade da conta original, que é um ativo digital valioso.

Higiene de senhas: É fundamental utilizar senhas fortes (com letras maiúsculas e minúsculas, números e símbolos) e, principalmente, únicas para cada serviço, especialmente para o aplicativo do banco. A senha de acesso ao banco

nunca deve ser a mesma de outros aplicativos ou redes sociais e jamais deve ser anotada em blocos de notas no celular ou compartilhada com terceiros.[30]

Configurações de privacidade: Para dificultar a fase de coleta de inteligência dos golpistas, é recomendável ajustar as configurações de privacidade tanto no WhatsApp quanto em outras redes sociais. A visibilidade da foto de perfil, do status e do "visto por último" no WhatsApp pode ser restringida para "Apenas meus contatos". Em redes como Facebook e Instagram, limitar a visibilidade de publicações e da lista de amigos para um círculo restrito impede que criminosos mapeiem facilmente os laços familiares e sociais da vítima.[6]

4.2 O protocolo de verificação comportamental e defesa humana

A defesa mais eficaz contra a manipulação é um processo mental estruturado que pode ser acionado no momento da tentativa de golpe. O protocolo de 5 passos: Alerta, Pressão, Pausa, Verificação, Decisão, proposto nesta pesquisa para o projeto de extensão, está perfeitamente alinhado com as melhores práticas de segurança recomendadas por especialistas.

Passo 1: ALERTA (desconfie sempre). O ponto de partida é a desconfiança saudável. Qualquer mensagem recebida de um número desconhecido que se passa por um parente ou amigo, especialmente se o contato subsequente envolver um pedido de dinheiro, deve ser imediatamente tratada como um sinal de alerta máximo. A premissa inicial deve ser: "Isto é um golpe até que se prove o contrário".[6]

Passo 2: PRESSÃO (identifique a manipulação). O segundo passo é reconhecer a tática. O usuário treinado deve ser capaz de identificar os elementos de engenharia social na conversa. O golpista invariavelmente criará uma narrativa de grande urgência e forte apelo emocional.[6] Reconhecer que a "pressão" é uma ferramenta de manipulação é o primeiro passo para neutralizar seu efeito psicológico.

Passo 3: PAUSA (não aja por impulso). Esta é a contramedida direta à pressão. A recomendação mais importante é nunca realizar transferências ou tomar decisões financeiras sob pressão. É preciso resistir ao impulso de "resolver" o problema imediatamente. Ações simples como respirar fundo, deixar o celular de lado por alguns minutos ou dizer ao interlocutor "preciso de um momento para verificar" são cruciais para retomar o controle racional da situação.

Passo 4: VERIFICAÇÃO (confirme por outro canal). Este é o passo infalível que desmascara 100% das tentativas deste golpe. A vítima deve encerrar a

comunicação por mensagem com o número suspeito e tentar confirmar a história por um canal de comunicação diferente e previamente conhecido. A ação mais eficaz é ligar para o número de telefone antigo e original do parente.[6] Se o parente atender e confirmar a história, a situação é legítima. Se ele atender e não souber de nada, o golpe está exposto. Outra tática poderosa é exigir uma chamada de vídeo; o golpista sempre se recusará, inventando desculpas como "a câmera do celular novo não funciona".[6]

Passo 5: DECISÃO (aja com segurança). Com base na verificação, a decisão se torna clara. Se a história foi confirmada por voz no número antigo, a ajuda pode ser prestada com segurança. Se a verificação falhou, a decisão correta é: não transferir o dinheiro, bloquear imediatamente o número do golpista no WhatsApp e, crucialmente, alertar o parente verdadeiro sobre a tentativa de fraude, para que ele possa avisar outros contatos e prevenir que mais pessoas caiam no golpe.[5]

A defesa contra este tipo de golpe é fundamentalmente assimétrica. O criminoso pode tentar o golpe centenas de vezes por dia com baixo custo e esforço, precisando de apenas um sucesso para obter lucro. A vítima em potencial, por outro lado, precisa estar vigilante e acertar em sua única oportunidade de defesa. Essa assimetria torna a educação contínua e a criação de "reflexos de segurança", como o protocolo de 5 passos, mais importantes do que medidas pontuais. O objetivo de uma capacitação eficaz não é apenas informar, mas sim internalizar e automatizar o comportamento de verificação, transformando-o em um hábito.

4.3 Desenvolvimento do artefato visual (Infográfico) e de uma página web educativa

Infográfico: Como parte da materialização da solução proposta por esta pesquisa, foi desenvolvido um infográfico estático. Este artefato visual (Figura 1) foi concebido, criado e editado pelo proponente deste trabalho, Carlos Augusto Muniz de Queiroz, utilizando o software de design gráfico Corel Draw. A imagem sintetiza de forma objetiva e acessível os 5 (cinco) passos centrais do mecanismo de prevenção, sendo: Alerta, Pressão, Pausa, Verificação e Decisão, constituindo a primeira ferramenta de capacitação focada, desenvolvida para o projeto de extensão a qual deverá ser amplamente divulgada nas redes sociais e distribuída ao máximo de pessoas possíveis a fim de receberem a educação preventiva a prática do golpe.

Figura 1 – Infográfico:

Figura 1 *– Infográfico estático dos 5 passos de prevenção ao golpe. Fonte: O autor (2025)* [51]

Página web educativa: A segunda fase da solução, evoluindo do artefato estático, consistiu no desenvolvimento de um protótipo web funcional, cuja interface principal é ilustrada na Figura 2. O proponente deste projeto, Carlos Augusto Muniz de Queiroz, criou a página web interativa utilizando as linguagens de marcação HTML, estilização CSS e programação JavaScript. Esta aplicação consolida algumas informações da pesquisa, apresentando estatísticas atuais sobre o golpe, relatos de vítimas, o infográfico estático e informações relevantes sobre o perfil dos envolvidos. O JavaScript foi empregado especificamente para implementar os recursos centrais da ferramenta: o guia educativo interativo de 5 passos para

prevenção e a integração com a API de inteligência artificial para análise de mensagens suspeitas.

Figura 2 – Página Web:

***Figura 2** – Interface principal do protótipo web interativo (Página de Capacitação). Fonte: O autor (2025).* [51]

A aplicação final está hospedada através de um repositório público na plataforma GitHub e disponível para acesso através do endereço do GitHub Pages:

https://augustoqueiroz13.github.io/SegurancaDigitalnoWhatsApp/.[51] O código-fonte também foi disponibilizado em um repositório no perfil do GitHub do autor, visando fomentar eventuais atualizações e contribuições da comunidade interessada em adicionar melhorias à ferramenta, que pode ser acessado em: https://github.com/AugustoQueiroz13/SegurancaDigitalnoWhatsApp. [51]

4.4 Higiene digital preventiva

Além das medidas específicas, práticas gerais de segurança digital, ou "higiene digital", contribuem para um ambiente online mais seguro e reduzem a exposição geral a riscos.

Cuidado com links e QR codes: Uma regra de ouro é nunca clicar em links suspeitos recebidos por e-mail, SMS ou mensagens de WhatsApp, especialmente de remetentes desconhecidos. Ao realizar pagamentos com PIX via QR Code, é vital conferir com atenção todos os dados do destinatário (nome, CPF/CNPJ, instituição) que aparecem na tela de confirmação antes de digitar a senha.[8]

Uso exclusivo de aplicativos oficiais: Todas as operações bancárias devem ser feitas exclusivamente através dos aplicativos oficiais baixados das lojas de aplicativos (Google Play Store ou Apple App Store). Nunca se deve acessar a conta bancária por meio de links enviados por terceiros.[10]

Gestão da pegada digital: É importante ter consciência das informações compartilhadas publicamente. Ser discreto com dados pessoais em redes sociais, como detalhes sobre rotina, local de trabalho e, principalmente, fotos e nomes de familiares, reduz a quantidade de "munição" disponível para os criminosos montarem seus ataques de engenharia social.[6]

Capítulo 5: Ação e recurso pós-golpe

Apesar de todos os esforços de prevenção, a realidade é que milhares de pessoas se tornam vítimas de golpes diariamente. Nesses casos, saber como agir rapidamente e quais mecanismos acionar pode fazer a diferença entre a perda total do valor e a possibilidade de recuperação. O processo pós-golpe é uma corrida contra o tempo, e a informação correta é a principal ferramenta da vítima.

5.1 Resposta imediata

A instantaneidade do PIX, que é sua maior vantagem, torna-se a maior desvantagem em caso de fraude. O dinheiro é transferido em segundos, e os

criminosos agem com a mesma velocidade para sacar ou pulverizar os valores em outras contas. Portanto, as ações tomadas nos primeiros minutos após a descoberta do golpe são as mais cruciais.

Contatar o banco imediatamente: A primeira e mais urgente medida é entrar em contato com a própria instituição financeira de onde o PIX foi enviado. A vítima deve ligar para a central de atendimento ou usar o chat do aplicativo e relatar a fraude de forma clara e objetiva. O objetivo é solicitar o bloqueio imediato dos recursos na conta de destino.[31]

Acionar o Mecanismo Especial de Devolução (MED): Ao contatar o banco, não basta apenas relatar o golpe. A vítima deve solicitar explicitamente a abertura de um procedimento de contestação via Mecanismo Especial de Devolução (MED). Este é o nome técnico do protocolo oficial do Banco Central para esses casos, e usar o termo correto pode agilizar o processo.[32]

5.2 : Guia detalhado para o Mecanismo Especial de Devolução (MED)

O MED é a principal ferramenta de recurso para vítimas de fraude com PIX. Compreender seu funcionamento, prazos e limitações é essencial para gerenciar as expectativas e seguir os procedimentos corretos.

O que é o MED: Trata-se de um conjunto de regras e procedimentos operacionais criado pelo Banco Central que permite que o banco da vítima comunique o banco do recebedor sobre uma transação fraudulenta, possibilitando o bloqueio e a eventual devolução dos valores. É aplicável exclusivamente em casos de fundada suspeita de fraude, golpe ou falha operacional nos sistemas.[34] É importante ressaltar que o MED não pode ser acionado para resolver disputas comerciais (ex: produto não entregue ou com defeito), arrependimento da compra ou erros de digitação da chave PIX.[34]

Como Funciona o Processo:

1: Solicitação da vítima: A vítima deve registrar o pedido de devolução em seu banco. O prazo máximo para iniciar esse processo é de **80 dias** a contar da data em que o PIX foi realizado.[32]

2: Notificação e bloqueio: O banco da vítima, ao acatar o pedido, utiliza o sistema do Banco Central para notificar a instituição do recebedor (o suposto golpista). Essa notificação gera um bloqueio imediato do valor correspondente na conta de destino, caso ainda haja saldo disponível.[38]

3: Análise do caso: A partir do bloqueio, as duas instituições financeiras (a do pagador e a do recebedor) têm um prazo de até **7 dias corridos** para analisar o caso e concluir se a transação foi de fato fraudulenta.[32]

4: Devolução dos valores: Se a fraude for confirmada e houver saldo (total ou parcial) na conta do recebedor, o dinheiro é devolvido à vítima. O prazo para essa devolução ocorrer, após a conclusão da análise, é de até **96 horas (4 dias)**.[35]

Limitações do mecanismo: É crucial entender que o MED não é uma garantia de estorno. O sucesso da recuperação depende inteiramente da existência de saldo na conta do golpista no momento do bloqueio.[43] Como os criminosos agem rápido para movimentar o dinheiro, muitas vezes a recuperação é apenas parcial ou, em alguns casos, nula. Dados de 2024 indicam que, de todas as solicitações de devolução via MED, apenas 31% resultaram em algum valor retornado à vítima.[44] Este dado alarmante reforça a ideia de que a prevenção é, de longe, a estratégia mais eficaz.

Evolução do MED: Ciente das limitações, o Banco Central anunciou novas regras para o MED, que se tornarão obrigatórias a partir de fevereiro de 2026. A principal mudança permitirá o rastreamento do dinheiro transferido da conta original do golpe para outras contas de destino, possibilitando o bloqueio em múltiplas camadas e aumentando as chances de recuperação dos recursos.[45]

O sistema financeiro instantâneo criou uma assimetria temporal crítica: a fraude ocorre na velocidade da luz, enquanto a recuperação, mesmo otimizada pelo MED, opera na velocidade de um processo analítico e lento. O sucesso da recuperação depende de a vítima perceber o golpe e agir em questão de minutos, antes que o dinheiro seja pulverizado. Essa corrida contra o tempo digital demonstra que a melhor, e talvez a única defesa verdadeiramente eficaz, é a prevenção no ponto de transação, capacitando o usuário a não autorizar a transferência em primeiro lugar.

5.3 Tabela 3: Cronograma do processo de devolução via MED

A tabela a seguir resume os prazos e responsabilidades do processo do MED, servindo como um guia prático para as vítimas.

Etapa do Processo	Responsável pela Ação	Prazo Máximo	Referências
1. Contestação da Transação	Vítima (Pagador)	Até 80 dias após a data	[34, 39]

		do PIX	
2. Notificação e Bloqueio Cautelar	Banco da Vítima / Banco do Recebedor	Imediato após a solicitação	[38, 39]
3. Análise da Fraude	Bancos da Vítima e do Recebedor	Até 7 dias corridos após a solicitação	[32, 39]
4. Devolução do Valor (se fraude confirmada e houver saldo)	Banco do Recebedor	Até 96 horas (4 dias) após a conclusão da análise	[42, 43]
5. Monitoramento de Saldo (em caso de devolução parcial)	Banco do Recebedor	Por até 90 dias após a transação original	[40]

5.4 Ações formais possíveis:

Além das ações junto às instituições financeiras, duas medidas formais são essenciais para o processo de investigação e para a proteção da comunidade.

Registro do Boletim de Ocorrência (B.O.): É fundamental que a vítima registre um Boletim de Ocorrência, o que pode ser feito online na maioria dos estados ou em uma delegacia de polícia. O B.O. é o documento oficial que formaliza o crime de estelionato. Ele é crucial para a investigação policial e também serve como uma prova para fortalecer a solicitação de devolução junto ao banco.[33] Relatos de vítimas indicam que a apresentação do B.O. ao banco foi um passo importante para a devolução bem sucedida dos valores.[46]

Denúncia no WhatsApp: Para ajudar a plataforma a combater a atividade criminosa, a vítima deve denunciar e bloquear o número do golpista diretamente no aplicativo. O procedimento é simples: acessar a conversa com o número fraudulento, clicar nas informações de contato e selecionar as opções "Denunciar contato" e, em seguida, "Denunciar e bloquear".[31] Esta ação impede que o golpista continue a contatar a vítima e sinaliza a conta para remoção pela plataforma.

CONSIDERAÇÕES FINAIS

CONCLUSÃO

A análise aprofundada do "Golpe do Falso Parente" via PIX no WhatsApp revela um desafio complexo e multifacetado, que se situa na intersecção da tecnologia, da psicologia social e da segurança pública. A pesquisa demonstra que esta fraude, embora tecnicamente simples, possui uma eficácia devastadora por explorar a confiança e a falta de literacia digital, com a população idosa emergindo como um dos grupos mais vulneráveis. As estatísticas nacionais apresentam o quadro de uma crise de segurança digital, onde a velocidade da inovação superou a capacidade de adaptação e educação da sociedade. Embora mecanismos de recurso como o MED existam e estejam em evolução, sua eficácia é limitada pela rapidez com que os criminosos agem. A conclusão inequívoca é que a prevenção, focada na capacitação comportamental do usuário, é a estratégia mais eficiente e impactante.

A abordagem adotada pelo projeto de extensão comunitária "Capacitação em Segurança Digital no WhatsApp" é, portanto, integralmente validada por esta pesquisa. A identificação da vulnerabilidade da população idosa como problemática central é validada pelos dados demográficos e qualitativos. A solução proposta, uma capacitação focada em um protocolo comportamental de 5 passos (Alerta, Pressão, Pausa, Verificação, Decisão), ataca diretamente o cerne do problema, que é a engenharia social, e não uma falha tecnológica

Com base em toda pesquisa aqui apresentada e nos resultados que geraram este artigo acadêmico, podem ainda ser propostas algumas melhorias para aprimorar e ampliar o impacto da ferramenta de capacitação desenvolvida até o momento:

Integrar um módulo de ação pós-golpe. A ferramenta interativa é excelente para a prevenção, mas seu valor pode ser ampliado ao oferecer orientação para quem já foi vítima. Pode ser adicionado um sexto passo ou um módulo anexo intitulado "Caí no golpe. E agora?". Este módulo poderá apresentar, de forma simplificada e visual, as informações do Capítulo 5 deste artigo, incluindo um guia de ação imediata (contatar o banco, solicitar o MED) e uma versão gráfica da Tabela 3 com o cronograma do processo. Isso poderá transformar a ferramenta não apenas em um guia de prevenção, mas também em um manual de "primeiros socorros

digitais", oferecendo amparo e direcionamento em um momento de grande estresse para a vítima.

Enfatizar a verificação por voz de forma interativa. A pesquisa destaca que a verificação por um canal alternativo, especialmente a ligação para o número antigo, é o passo mais crítico e infalível para desmascarar a fraude. A página web interativa pode dar ênfase máxima a este ponto. É possível criar uma simulação que, no passo da "Verificação", force o usuário a, por exemplo, "clicar em um botão de telefone" para "ligar" para o número antigo, reforçando este como o comportamento correto e mais seguro. Essa prática interativa pode ajudar a transformar o conhecimento teórico em um reflexo comportamental.

Contextualizar a ameaça com dados de impacto. Para aumentar o engajamento e a percepção da seriedade do tema desde o início, pode-se fazer melhorias para que a ferramenta de capacitação comece com um ou dois dados estatísticos de alto impacto. Uma tela inicial com uma mensagem como: "Você sabia? No último ano, golpes como o que você vai aprender a evitar causaram um prejuízo de quase R$ 29 bilhões aos brasileiros.", isso pode aumentar a atenção e a motivação do usuário, deixando claro que o treinamento não é sobre um risco abstrato, mas sobre uma ameaça real e presente.

A implementação dessas e de outras melhorias, fundamentadas na pesquisa extensiva apresentada, tem o potencial de fortalecer ainda mais uma iniciativa já relevante e bem direcionada, contribuindo de forma significativa para a proteção de um dos segmentos mais vulneráveis da nossa sociedade no novo e desafiador território digital. Toda contribuição e melhorias são bem vindas e podem ser feitas através do repositório GitHub do projeto disponibilizado através do link https://github.com/AugustoQueiroz13/SegurancaDigitalnoWhatsApp.

REFERÊNCIAS

1. FEBRABAN. Pix foi o meio de pagamento mais usado no Brasil em 2024; TED liderou em valores transacionados. **FEBRABAN - Notícias**, 2025. Disponível em: https://portal.febraban.org.br/noticia/4290/pt-br/. Acesso em: 8 out. 2025.
2. FEBRABAN. 82% das transações bancárias dos brasileiros são feitas pelos canais digitais, revela pesquisa. **FEBRABAN - Notícias**, 2025. Disponível em: https://portal.febraban.org.br/noticia/4310/pt-br/. Acesso em: 9 out. 2025.

3. Golpe via WhatsApp usa dados vazados e pede dinheiro a parentes... **Tecnoblog**, 2025. Disponível em: https://tecnoblog.net/noticias/golpe-via-whatsapp-usa-dados-vazados-e-pede-dinheiro-a-parentes-da-vitima/. Acesso em: 10 out. 2025.
4. NUBANK. Golpe do novo número no WhatsApp: entenda como funciona. **blog nubank**, 2025. Disponível em: https://blog.nubank.com.br/golpe-do-novo-numero/. Acesso em: 10 out. 2025.
5. O que Você Precisa Saber Sobre O Golpe Do Parente No WhatsApp? **Magiscred**, 2025. Disponível em: https://magiscred.com.br/educacao-financeira/golpe-do-parente-no-whatsapp/. Acesso em: 10 out. 2025.
6. Como funciona o golpe do falso parente? Saiba como evitar! **Credisis**, 2025. Disponível em: https://credisis.com.br/blog/ciberseguranca/golpe-do-falso-parente/. Acesso em: 10 out. 2025.
7. POLÍCIA CIVIL (Sergipe). Golpes envolvendo Pix acendem alerta para verificação de dados antes da transferência de valores solicitados pelo WhatsApp. **Polícia Civil (SE)**, 2025. Disponível em: https://policiacivil.se.gov.br/golpes-envolvendo-pix-acendem-alerta-para-verificacao-de-dados-antes-da-transferencia-de-valores-solicitados-pelo-whatsapp/. Acesso em: 15 out. 2025.
8. SERASA. Golpe do Pix: conheça os mais comuns e se proteja. **Blog Premium Serasa**, 2025. Disponível em: https://www.serasa.com.br/premium/blog/golpes-do-pix-como-se-proteger/. Acesso em: 15 out. 2025.
9. Criminosos incluem vítimas em grupos de WhatsApp em novo golpe. **Seac ABC**, 2025. Disponível em: https://seac-abc.com.br/criminosos-incluem-vitimas-em-grupos-de-whatsapp-em-novo-golpe/. Acesso em: 15 out. 2025.
10. SEBRAE PR. Golpe do pix e outros: como proteger seu dinheiro e evitar fraudes... **Sebrae PR**, 2025. Disponível em: https://sebraepr.com.br/comunidade/artigo/golpe-do-pix-e-outros-como-proteger-seu-dinheiro-e-evitar-fraudes. Acesso em: 15 out. 2025.
11. Segurança nas Transações via PIX: Como Evitar Golpes? **Be Compliance**, 2025. Disponível em: https://becompliance.com/seguranca-nas-transacoes-via-pix-como-evitar-golpes/. Acesso em: 15 out. 2025.
12. Mais de 24 milhões de pessoas foram vítimas de golpes pelo PIX... **Rádio Senado**, 2025. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2025/08/18/mais-de-24-milhoes-de-pessoas-foram-vitimas-de-golpes-pelo-pix. Acesso em: 16 out. 2025.
13. PODER360. Golpes causaram prejuízo de R$ 10,1 bi em 2024, diz Febraban. **Poder360**, 2025. Disponível em: https://www.poder360.com.br/poder-economia/golpes-causaram-prejuizo-de-r-101-bi-em-2024-diz-febraban/. Acesso em: 16 out. 2025.
14. CONTEC. Brasil tem mais de 2 milhões de golpes, com explosão de fraudes com Pix e redes sociais. **CONTEC**, 2025. Disponível em: https://contec.org.br/brasil-tem-mais-de-2-milhoes-de-golpes-com-explosao-de-fraudes-com-pix-e-redes-sociais/. Acesso em: 16 out. 2025.
15. Tentativas de golpes aumentam no Brasil. **Febraban Tech**, 2025. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/tentativas-de-golpes-aumentam-no-brasil. Acesso em: 16 out. 2025.
16. FEBRABAN. 1 3 4 Método. **Febraban**, 2025. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Relat%C3%B3rio_Radar%20Febraban_Mar%C3%A7o_vf.pdf. Acesso em: 17 out. 2025.

17. ESTADÃO. Febraban lista 10 golpes mais praticados em 2024; saiba quais são e como se proteger. **Estadão**, 2025. Disponível em: https://www.estadao.com.br/economia/golpes-bancarios-mais-praticados-2024-febraban-veja-dicas-para-se-proteger-nprei/. Acesso em: 17 out. 2025.
18. FEBRABAN. Saiba quais foram os 10 golpes mais aplicados contra clientes bancários em 2024. **FEBRABAN - Notícias**, 2025. Disponível em: https://portal.febraban.org.br/noticia/4279/pt-br/. Acesso em: 17 out. 2025.
19. FEEB PR. Conheça os maiores golpes bancários de 2025 e como se proteger deles. **FEEB PR**, 2025. Disponível em: https://www.feebpr.org.br/noticia/k2Xi-conheca-os-maiores-golpes-bancarios-de-2025-e-como-se-proteger-deles. Acesso em: 17 out. 2025.
20. SENADO FEDERAL. Golpes virtuais aumentam e não fazem distinção de idade. **Senado Federal**, 2025. Disponível em: https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade. Acesso em: 17 out. 2025.
21. A preoteção dos idosos contra crimes cibernéticos no brasil: desafios... **Periódico Rease**, 2025. Disponível em: https://periodicorease.pro.br/rease/article/download/18570/10788/47191. Acesso em: 21 out. 2025.
22. AGÊNCIA BRASIL. Dificuldade em acessar serviço digital torna idoso vulnerável a golpes. **Agência Brasil**, 2025. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2025-04/dificuldade-em-acessar-servico-digital-torna-idoso-vulneravel-golpes. Acesso em: 21 out. 2025.
23. GOV.BR. Campanha alerta para aumento de 60% dos golpes financeiros contra idosos na pandemia. **Gov.br**, 2025. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/setembro/campanha-alerta-para-aumento-de-60-dos-golpes-financeiros-contra-idosos-na-pandemia. Acesso em: 21 out. 2025.
24. ALEGO. Campanha para conscientizar idosos contra fraudes na internet avança em primeiro turno. **Portal da Alego**, 2025. Disponível em: https://portal.al.go.leg.br/noticias/146372/campanha-para-conscientizar-idosos-contra-fraudes-na-internet-avanca-em-primeiro-turno. Acesso em: 21 out. 2025.
25. PREFEITURA DE VITÓRIA. Idosos mais seguros: Prefeitura de Vitória lança projeto para... **Prefeitura de Vitória**, 2025. Disponível em: https://www.vitoria.es.gov.br/noticia/idosos-mais-seguros-prefeitura-de-vitoria-lanca-projeto-para-prevenir-golpes-digitais-54712. Acesso em: 22 out. 2025.
26. AGÊNCIA BRASIL. Campanha dá dicas para uso seguro da internet por idosos. **Agência Brasil - EBC**, 2025. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2025-09/campanha-da-dicas-para-uso-seguro-da-internet-por-idosos. Acesso em: 22 out. 2025.
27. PRODEST. Inclusão digital para idosos: benefícios e cuidados com o acesso à internet. **PRODEST**, 2025. Disponível em: https://prodest.es.gov.br/inclusao-digital-para-idosos-beneficios-e-cuidados-com-o-acesso-a-internet. Acesso em: 22 out. 2025.

28. WELIVESECURITY. Cibersegurança para pessoas idosas. **WeLiveSecurity**, 2025. Disponível em: https://www.welivesecurity.com/pt/conscientizacao/ciberseguranca-para-pessoas-idosas/. Acesso em: 22 out. 2025.

29. SERASA. Idosos na internet: dicas de proteção digital. **Blog Premium Serasa**, 2025. Disponível em: https://www.serasa.com.br/premium/blog/idosos-internet/. Acesso em: 30 out. 2025.

30. CNN BRASIL. Golpe do Pix: o que fazer e como se proteger? **CNN Brasil**, 2025. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/caiu-no-golpe-do-pix-saiba-o-que-fazer-e-como-se-proteger/. Acesso em: 22 out. 2025.

31. EXAME. Novo golpe do Pix: criminosos usam redes sociais para esconder esquema de pirâmide financeira. **Exame**, 2025. Disponível em: https://exame.com/economia/novo-golpe-do-pix-criminosos-usam-redes-sociais-para-esconder-esquema-de-piramide-financeira/. Acesso em: 22 out. 2025.

32. ESTADÃO. É possível recuperar o dinheiro após cair em um golpe envolvendo Pix? **Estadão**, 2025. Disponível em: https://www.estadao.com.br/economia/e-possivel-recuperar-dinheiro-cair-golpe-pix-nprei/. Acesso em: 22 out. 2025.

33. ITAÚ. Como cancelar um Pix e recuperar o seu dinheiro. **Blog Itaú**, 2025. Disponível em: https://blog.itau.com.br/artigos/saiba-se-possivel-cancelar-um-pix-e-recuperar-seu-dinheiro. Acesso em: 22 out. 2025.

34. BANCO DO BRASIL. Mecanismo Especial de Devolução (MED). **Banco do Brasil**, 2025. Disponível em: https://www.bb.com.br/site/pra-voce/pix/mecanismo-especial-de-devolucao/. Acesso em: 22 out. 2025.

35. PAGBANK. MED: saiba como funciona o mecanismo de devolução Pix. **Blog PagBank**, 2025. Disponível em: https://blog.pagseguro.uol.com.br/mecanismo-especial-de-devolucao-pix/. Acesso em: 22 out. 2025.

36. CAIXA. Pix CAIXA. **Caixa**, 2025. Disponível em: https://www.caixa.gov.br/pix/Paginas/default.aspx. Acesso em: 23 out. 2025.

37. BANCO BMG. Como contestar um Pix? Confira o passo a passo! **Banco Bmg**, 2025. Disponível em: https://www.bancobmg.com.br/blog/conta-digital/como-contestar-um-pix/. Acesso em: 23 out. 2025.

38. BANCO CENTRAL. Pix terá botão de contestação. **Banco Central**, 2025. Disponível em: https://www.bcb.gov.br/detalhenoticia/20865/noticia. Acesso em: 23 out. 2025.

39. BANCO CENTRAL. Pix - FAQs. **Banco Central**, 2025. Disponível em: https://www.bcb.gov.br/meubc/faqs/s/pix. Acesso em: 23 out. 2025.

40. EFÍ BANK. Como funciona o MED: devolução de Pix em caso de fraude. **Efí Bank**, 2025. Disponível em: https://sejaefi.com.br/blog/mecanismo-especial-de-devolucao-do-pix. Acesso em: 23 out. 2025.

41. TRANSFEERA. MED: como funciona o Mecanismo Especial de Devolução Pix. **Transfeera**, 2025. Disponível em: https://transfeera.com/blog/mecanismo-de-devolucao-pix/. Acesso em: 23 out. 2025.

42. CORA. MED: como funciona o Mecanismo Especial de Devolução do Pix e como acionar. **Cora**, 2025. Disponível em: https://www.cora.com.br/blog/med/. Acesso em: 23 out. 2025.

43. TJAM. Você sabe o que é o MED e a relação dele com a proteção contra fraude no PIX? **TJAM**, 2025. Disponível em: https://www.tjam.jus.br/index.php/juizados/publicacoes/projetos/52931-guia-basico-do-consumidor-3-edicao-tema-mecanismo-especial-de-devolucao-med/file. Acesso em: 30 out. 2025.

44. PAGBANK. Como cancelar um Pix enviado por engano: saiba como agir. **Blog PagBank**, 2025. Disponível em: https://blog.pagseguro.uol.com.br/como-cancelar-um-pix/. Acesso em: 30 out. 2025.

45. CNN BRASIL. Pix terá novas regras para devolução de valores em casos de fraude. **CNN Brasil**, 2025. Disponível em: https://www.cnnbrasil.com.br/economia/pix-tera-novas-regras-para-devolucao-de-valores-em-casos-de-fraude/. Acesso em: 30 out. 2025.

46. ALENCAR ADVOCACIA. Restituição do PIX. Golpe do PIX. MED. Saiba como recuperar seu dinheiro. **YouTube**, 2025. Disponível em: https://www.youtube.com/watch?v=KFxxO_kWq10. Acesso em: 30 out. 2025.

47. MORGADO, Flávio. **Golpes financeiros contra pessoas idosas por meio de engenharia social no ambiente digital**. Revista Longeviver, São Paulo, Ano VI, n. 24, out./nov./dez. 2024.

48. BRAGA, Ana Paula Passos; SILVA, Viviane Neves da; GOMES, Jennifer Alves Rates. **Vulnerabilidade do idoso no mundo digital: desafios e estratégias para a proteção contra golpes e fraudes online**. Revista FT, 2025. DOI: 10.69849/revistaft/fa10202510241445.

49. BRASIL. Ministério dos Direitos Humanos e da Cidadania. **Cartilha de Apoio à Pessoa Idosa:** enfrentamento à violência patrimonial e financeira. Brasília, DF: MDH, 2024. Disponível em: https://www.gov.br/pt-br.

50. MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson Makron Books, 2003.

51. QUEIROZ, Carlos Augusto Muniz de. **Segurança Digital no WhatsApp**: [Repositório de software]. GitHub, 2025. Disponível em: https://github.com/AugustoQueiroz13/SegurancaDigitalnoWhatsApp. Acesso em: 01 nov. 2025