OAB MATO GROSSO

Comissão de Direito Bancário

CARTILHA

FRAUDES BANCÁRIAS

Comissão Estadual de Direito Bancário da OAB-MT

2ª Edição

Autores:

- Angélica Anai Angulo
- Bruno Felipe Monteiro Coelho (coord.)
- Carolina Lima Ferreira
- Davi Rodrigo Damasceno Ribeiro
- Diogo de Oliveira da Cruz
- João Carlos Disarsz Alves (coord.)
- Santiany Almeida de Siqueira Curvo

SUMÁRIO

SUMÁRIO

Entendendo o Cenário das Fraudes Bancárias

As fraudes bancárias representam um desafio crescente na sociedade contemporânea, impactando não apenas as finanças individuais, mas também a confiança no sistema financeiro como um todo. Compreender a natureza dessas fraudes, suas consequências e os mecanismos de proteção é o primeiro passo para uma navegação mais segura no universo digital e financeiro.

Conceito Jurídico e Impacto Social das Fraudes Bancárias

No âmbito jurídico, a fraude bancária configura-se como um ato ilícito perpetrado com o intuito de enganar indivíduos ou instituições financeiras para obter vantagens indevidas, resultando em prejuízo para a vítima.

Essa conduta pode manifestar-se de diversas formas, desde a utilização de documentos falsos para a abertura de contas ou obtenção de crédito, até esquemas complexos envolvendo engenharia social, em que o criminoso manipula a vítima para que ela própria forneça dados sensíveis ou realize transações fraudulentas.

Frequentemente, tais atos são enquadrados em tipos penais como estelionato (Art. 171 do Código Penal), furto mediante fraude (Art. 155, § 4º, II, do Código Penal), e, mais recentemente, com a tipificação específica de fraudes eletrônicas.

O impacto social dessas fraudes transcende as perdas financeiras diretas. Vítimas frequentemente experimentam significativo abalo emocional, sentimento de violação e insegurança. Além disso, a desconfiança gerada pode levar à subutilização de serviços financeiros digitais, especialmente por parte de populações mais vulneráveis, como idosos ou pessoas com menor familiaridade tecnológica.

Os custos associados à prevenção, investigação e ao ressarcimento de fraudes também podem ser repassados aos consumidores na forma de tarifas mais elevadas, afetando a economia de maneira mais ampla. A complexidade da investigação, muitas vezes dificultada pela atuação transnacional de criminosos

e transnacional de criminosos e pelo uso de identidades falsas, impõe um ônus adicional às autoridades e ao sistema de justiça.

Dados recentes indicam aumento alarmante nas fraudes bancárias. Conforme divulgado por fontes como a Polícia Federal e relatórios de segurança, as perdas no Brasil alcançaram a cifra de R$ 10,1 bilhões em 2024, um aumento de 17% em relação ao ano anterior. Globalmente, as projeções apontam para perdas de aproximadamente US$ 400 bilhões em 2025 devido a fraudes on-line (Fonte: Juniper Research, conforme resumo da pesquisa). Esse cenário reforça a urgência de medidas preventivas eficazes e de uma legislação robusta.

Diferença entre Fraude Bancária e Estelionato Comum

Embora ambos os crimes envolvam o engano para obtenção de vantagem ilícita, existem distinções importantes entre a fraude bancária e o estelionato comum. O estelionato, previsto no Art. 171 do Código Penal, caracteriza-se pelo emprego de artifício, ardil ou qualquer outro meio fraudulento para induzir ou manter alguém em erro, obtendo vantagem ilícita em prejuízo alheio. Geralmente, a vítima é uma pessoa física que é diretamente enganada pelo criminoso, como no caso do golpe do bilhete premiado ou da venda de um produto inexistente.

Já a fraude bancária, embora possa subsumir-se ao tipo penal de estelionato em muitas situações (especialmente com as alterações legislativas que incluíram o estelionato eletrônico), possui particularidades quando direcionada especificamente contra o sistema financeiro ou utilizando seus mecanismos. Um exemplo clássico de fraude que se diferencia do estelionato comum é a obtenção de financiamento mediante o uso de documentos falsos perante uma instituição financeira.

Nesses casos, o crime pode ser enquadrado também na Lei 7.492/1986 (Crimes Contra o Sistema Financeiro Nacional), dependendo da magnitude e do modus operandi. A principal diferença reside no alvo primário da conduta e nos bens jurídicos tutelados, que, no caso da fraude bancária, para além do patrimônio da vítima direta, atinge a credibilidade e a estabilidade do sistema financeiro.

É crucial notar que, com a digitalização, as fronteiras entre essas modalidades podem se tornar tênues. Golpes como o do PIX reverso ou o phishing podem ser vistos tanto como estelionato eletrônico quanto como fraudes bancárias, dependendo do contexto e da forma como a investigação e a denúncia são conduzidas.

Responsabilidade das Instituições Financeiras

A responsabilidade das instituições financeiras em casos de fraude é um tema central e de grande relevância para o consumidor. O Superior Tribunal de Justiça - STJ, por meio da Súmula 479, consolidou o entendimento de que "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". Isso significa que, em regra, o banco é responsável por falhas na segurança de seus sistemas que permitam a ocorrência de fraudes, independentemente da comprovação de culpa.

Essa responsabilidade decorre do chamado "risco da atividade". Ao oferecerem serviços e produtos no mercado, as instituições financeiras assumem os riscos inerentes a essa atividade, incluindo a possibilidade de fraudes. O Código de Defesa do Consumidor - CDC também ampara esse entendimento, ao estabelecer o dever de segurança na prestação de serviços (Art. 14).

Contudo, a jurisprudência vem evoluindo para analisar a conduta do consumidor. Se for comprovada a culpa exclusiva da vítima – por exemplo, se o cliente compartilha voluntariamente sua senha com terceiros, ignora alertas de segurança evidentes ou age com manifesta negligência –, a responsabilidade da instituição financeira pode ser atenuada ou até mesmo afastada. A discussão sobre a culpa concorrente, na qual tanto o banco quanto o cliente falham em seus deveres de cuidado, também está ganhando espaço nos tribunais. Portanto, embora a regra geral seja a responsabilidade objetiva do banco, a análise de cada caso concreto é fundamental.

A Evolução das Fraudes no Ambiente Digital

A transformação digital trouxe inúmeras facilidades, mas também abriu novas avenidas para a criminalidade. As fraudes bancárias evoluíram de golpes físicos e rudimentares para ataques cibernéticos sofisticados e de difícil rastreamento.

Inicialmente, as preocupações concentravam-se em clonagem de cartões e cheques falsificados. Com a popularização da internet e, posteriormente, dos smartphones, os golpes migraram para o ambiente on-line. O phishing (envio de e-mails falsos para capturar dados) e o SMShing (mesma técnica via SMS) tornaram-se comuns.

Criminosos passaram a criar sites falsos, idênticos aos de bancos, para enganar clientes. A introdução de novas tecnologias, como o PIX, embora traga agilidade, também gerou novas modalidades de golpe, como o golpe do PIX reverso ou o golpe do falso investimento via PIX, em que a instantaneidade da transação dificulta a recuperação dos valores.

Mais recentemente, a inteligência artificial (IA) emergiu como ferramenta poderosa nas mãos dos fraudadores. A criação de deepfakes de voz e imagem permite que criminosos passem-se por conhecidos das vítimas ou até mesmo simulem a aprovação de transações por reconhecimento facial ou de voz. O roubo de dispositivos móveis também tornou-se grande preocupação, pois os criminosos buscam acesso direto aos aplicativos bancários instalados.

Essa constante evolução exige que tanto as instituições financeiras quanto os consumidores mantenham-se atualizados sobre as novas táticas e reforcem continuamente suas medidas de segurança. A velocidade com que novas fraudes surgem demanda uma postura proativa e vigilante de todos os envolvidos.

A Importância da Proteção de Dados e da LGPD

A Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.709/2018) representou um marco fundamental na proteção da privacidade e dos dados dos cidadãos brasileiros. No contexto das fraudes bancárias, a LGPD exerce papel crucial, pois muitos golpes iniciam-se a partir do acesso indevido ou do vazamento de informações pessoais, como nome, CPF, endereço, telefone e dados bancários.

A LGPD estabelece princípios e regras para o tratamento de dados pessoais por organizações públicas e privadas, incluindo as instituições financeiras. Isso inclui a implementação de sistemas de segurança robustos, políticas claras de privacidade e a garantia de que os dados sejam utilizados apenas para as finalidades consentidas pelo titular.

Para o consumidor, a LGPD assegura direitos como o acesso aos seus dados, a correção de informações incorretas, a eliminação de dados desnecessários e a portabilidade. Em caso de incidentes de segurança que possam acarretar risco ou dano relevante, as instituições são obrigadas a comunicar o fato à Autoridade Nacional de Proteção de Dados - ANPD e aos titulares dos dados.

A conscientização sobre esses direitos e sobre a importância de proteger os próprios dados é componente essencial na prevenção de fraudes. Nunca compartilhar senhas, códigos de verificação ou dados completos de cartão por telefone ou mensagem, mesmo que o interlocutor pareça ser do banco, é uma regra de ouro.

O Papel do Advogado e da OAB na Orientação ao Consumidor

O advogado desempenha um papel vital não apenas na representação de vítimas de fraudes bancárias em processos judiciais, mas também na orientação preventiva. Um profissional especializado em Direito Bancário e do Consumidor pode esclarecer dúvidas sobre direitos, analisar contratos, identificar cláusulas abusivas e instruir sobre as melhores práticas de segurança e como proceder em caso de golpe.

A Ordem dos Advogados do Brasil-OAB, por meio de suas comissões temáticas, como a Comissão de Direito Bancário e a Comissão de Defesa do Consumidor, também exerce função social importante. A OAB promove eventos, elabora materiais informativos (como essa cartilha) e atua na defesa dos direitos dos cidadãos, buscando aprimorar a legislação e fiscalizar a atuação das instituições. A orientação jurídica qualificada pode fortalecer o consumidor, tornando-o menos suscetível a fraudes e mais preparado para buscar a reparação de seus direitos caso seja lesado.

Golpe do Falso Advogado (Alerta Importante)

Apesar de não ser uma fraude estritamente bancária, o Golpe do Falso Advogado vem tornando-se alarmantemente comum e merece destaque como alerta preventivo, pois frequentemente envolve a solicitação de transferências bancárias urgentes. Nesse golpe, criminosos passam-se por advogados ou funcionários de escritórios de advocacia para ludibriar pessoas que possuem processos judiciais em andamento.

Os golpistas, muitas vezes obtendo informações processuais, que são públicas, entram em contato com a vítima (cliente real de um advogado) alegando a necessidade de um pagamento urgente para a liberação de valores do processo, o pagamento de uma taxa judicial inesperada ou alguma outra despesa processual fictícia. A comunicação pode dar-se por WhatsApp, telefone ou e-mail, utilizando técnicas para simular a identidade do verdadeiro advogado, como o uso da foto do profissional no perfil do WhatsApp ou a criação de endereço de e-mail similar.

Como se proteger desse golpe específico:

- Desconfie de contatos inesperados: se receber solicitação de pagamento urgente de um número ou e-mail desconhecido, mesmo que se identifique como seu advogado, desconfie.

- Confirme por canais oficiais: entre em contato diretamente com seu advogado pelo número de telefone ou e-mail que você já possuía e utilizava para comunicação. Não confie apenas na informação recebida na nova mensagem.

- Chamada de vídeo: se possível, solicite chamada de vídeo para confirmar a identidade.

- Verifique os dados de pagamento: advogados e escritórios geralmente solicitam pagamentos para contas em nome do próprio escritório ou do advogado, ou por meio de guias judiciais oficiais.

- Desconfie de pedidos de depósito em contas de terceiros ou pessoas físicas desconhecidas.

- A Justiça não pede taxas por PIX para contas pessoais: O Poder Judiciário utiliza guias de recolhimento específicas. Qualquer solicitação de pagamento de taxas urgentes via PIX para contas pessoais deve ser tratada com extrema cautela.

Golpes Digitais de Alta Tecnologia

A evolução tecnológica trouxe inúmeros benefícios para o sistema financeiro, mas também abriu espaço para fraudes cada vez mais sofisticadas. Este capítulo apresenta os principais golpes digitais de alta tecnologia que estão afetado os consumidores brasileiros, com explicações detalhadas sobre como funcionam e, principalmente, como se proteger.

PIX Reverso

O que é e como funciona:

O golpe do PIX reverso é uma fraude sofisticada que explora o Mecanismo Especial de Devolução - MED criado pelo Banco Central para facilitar o estorno de transações PIX realizadas por engano. Nesse golpe, o criminoso segue uma sequência bem-planejada:

1.

Primeiro, realiza uma transferência PIX legítima para a conta da vítima (geralmente comerciantes, vendedores on-line ou prestadores de serviço).

2.

Em seguida, entra em contato alegando que transferiu o valor por engano ou em valor superior ao devido, solicitando a devolução.

3.

O ponto crucial do golpe: o fraudador pede que a devolução seja feita para uma chave PIX diferente da utilizada na transferência original, alegando que a primeira conta está com problemas ou bloqueada.

4.

Após receber a devolução na nova chave, o criminoso aciona o MED junto ao banco, contestando a transferência original como fraudulenta.

5.

Se o banco acatar a contestação, o valor da transferência original é estornado automaticamente, e a vítima fica no prejuízo tanto do valor original quanto do valor devolvido.

Exemplo prático:

Mariana vende roupas pelo Instagram. Um cliente faz um PIX de R$ 500,00 para a compra de algumas peças. Minutos depois, entra em contato via WhatsApp alegando haver enviado o valor errado, pois queria comprar apenas uma peça de R$ 150,00. Pede que Mariana devolva R$ 350,00, mas para uma chave PIX diferente, dizendo que a conta original está com limite diário excedido. Após Mariana fazer a devolução, o golpista aciona o MED alegando não reconhecer a transferência original de R$ 500,00. O banco estorna o valor, e Mariana perde R$ 850,00 (os R$ 500,00 estornados mais os R$ 350,00 que devolveu).

Quem são as principais vítimas:

• Pequenos comerciantes e vendedores de plataformas digitais (Instagram, Facebook Marketplace, OLX)

• Prestadores de serviços autônomos

• Pessoas que realizam vendas ocasionais pela internet

Como se proteger
(específico para esse golpe):

• Nunca devolva valores para chaves diferentes da original! Esta é a regra de ouro. Sempre utilize a função “Devolver” no próprio aplicativo do banco, que garante que o dinheiro volte para a mesma chave de origem.

• Estabeleça políticas claras de devolução: se você é comerciante, informe previamente suas políticas de cancelamento e devolução.

• Guarde comprovantes: salve todos os comprovantes de transferências recebidas e realizadas, além de prints das conversas com clientes.

Alerta importante: o Banco Central orienta que, em caso de dúvida sobre uma transferência recebida, o correto é aguardar a solicitação formal de devolução via banco, e não realizar estornos manuais para contas diferentes.

Golpes com uso de Inteligência Artificial (voz e imagem)

O que é e como funciona:

Com o avanço da Inteligência Artificial - IA, surgiu uma nova categoria de fraudes que utiliza tecnologia de deepfake para criar áudios e vídeos falsos, mas extremamente convincentes. Esses golpes exploram duas tecnologias principais:

1.

Clonagem de voz: utilizando apenas alguns segundos de áudio original, algoritmos de IA podem replicar a voz de uma pessoa com impressionante fidelidade, incluindo seu timbre, sotaque e padrões de fala.

2.

Manipulação de imagem e vídeo (deepfake): tecnologias avançadas permitem criar vídeos nos quais o rosto e os movimentos de uma pessoa são sobrepostos em outra, criando a ilusão de que a pessoa está dizendo ou fazendo algo que nunca aconteceu.

A sofisticação desses golpes aumentou drasticamente nos últimos anos. Ferramentas como o “Deep Live Cam” permitem a criação de avatares realistas em tempo real, nos quais o fraudador pode literalmente “vestir” a identidade digital de outra pessoa durante videochamadas. Esses sistemas utilizam redes neurais avançadas para mapear expressões faciais, movimentos labiais e até mesmo padrões de piscadas, criando uma representação virtualmente indistinguível de uma pessoa real.

Esses recursos são utilizados para:

- Ligar para familiares passando-se por parentes em situação de emergência
- Criar vídeos falsos de pessoas “autorizando” transações bancárias
- Simular chamadas de vídeo com executivos ou figuras de autoridade

• Abrir contas bancárias ou solicitar empréstimos usando identidades falsas

• Burlar sistemas de reconhecimento facial ou de voz

• Realizar entrevistas de emprego falsas para coletar dados pessoais

• Criar conteúdo comprometedor para extorsão (sextortion)

Exemplo prático:

Carlos recebe uma videochamada de seu "filho" (aparentemente) pedindo ajuda urgente, dizendo que está em apuros e precisa de dinheiro imediatamente. A imagem é do filho, com movimentos faciais naturais, e a voz é idêntica, com as mesmas expressões e jeito de falar. O "filho" explica que está usando o celular de um amigo porque o dele foi roubado. Carlos, convencido pela videochamada realista, faz uma transferência PIX para a conta indicada. Mais tarde, ao falar com o filho verdadeiro, descobre que foi vítima de um golpe com deepfake gerado por IA.

Como se proteger

(específico para esse golpe):

• Estabeleça senhas ou códigos familiares: combine com familiares próximos palavras-código ou perguntas específicas que só vocês conhecem, para confirmar identidades em situações suspeitas.

• Verifique por múltiplos canais: se receber uma solicitação incomum, mesmo que pareça vir de alguém conhecido em videochamada, confirme por outro meio de comunicação (se recebeu por WhatsApp, ligue diretamente para o número que você já tem registrado).

• Fique atento a pequenas inconsistências: em deepfakes, podem existir falhas sutis como movimentos estranhos dos lábios, iluminação inconsistente, áudio dessincronizado ou comportamento que não condiz com o padrão habitual da pessoa.

• Limite sua exposição digital: seja criterioso com o que publica nas redes sociais. Configure suas contas como privadas, quando possível, e evite compartilhar vídeos falando por longos períodos, que podem ser usados para treinar algoritmos de clonagem de voz.

Alerta importante: a tecnologia de deepfake evolui rapidamente. Se surgir qualquer suspeita, interrompa a comunicação e verifique a identidade da pessoa por outros meios antes de tomar qualquer ação financeira.

Phishing e SMShing bancário (versão moderna)

O que é e como funciona:

Phishing (via e-mail) e SMShing (via SMS) são técnicas de engenharia social nas quais criminosos passam-se por instituições confiáveis para enganar as vítimas e obter dados sensíveis ou induzi-las a realizar ações prejudiciais. Embora existam há anos, essas fraudes evoluíram significativamente, tornando-se mais sofisticadas e difíceis de identificar.

Nas versões modernas, os golpistas:

1. Criam e-mails ou mensagens visualmente idênticos aos enviados por bancos, com logos, formatação e linguagem corporativa precisos.
2. Utilizam domínios de e-mail ou números de telefone que parecem legítimos à primeira vista.
3. Exploram eventos reais ou sazonais (como lançamento de novos serviços bancários, mudanças regulatórias, períodos de declaração de imposto de renda) para dar credibilidade às mensagens.
4. Incluem links que direcionam para sites falsos, praticamente idênticos aos originais, pelos quais capturam dados de login, senhas e informações de cartões.
5. Instalam malwares que podem monitorar atividades, capturar teclas digitadas ou até mesmo assumir o controle do dispositivo.

Exemplo prático:

Ana recebe um SMS aparentemente do seu banco informando sobre uma "tentativa de acesso suspeito" em sua conta digital. A mensagem solicita que ela "confirme sua identidade imediatamente" por meio de um link para evitar o bloqueio da conta. O link direciona para uma página idêntica à do banco, na qual Ana insere seu CPF, senha e o código de verificação recebido por SMS. Minutos depois, percebe transferências não autorizadas em sua conta.

Em uma variação mais recente, João recebe um e-mail informando sobre a nova política de segurança do banco que exige "recadastramento biométrico". O e-mail contém link para um aplicativo falso que, ao ser instalado, captura dados e monitora o celular.

Quem são as principais vítimas:

• Clientes de instituições financeiras

• Pessoas com pouca familiaridade tecnológica

• Usuários de múltiplos serviços on-line (que podem confundir comunicações legítimas e falsas)

• Consumidores em momentos de estresse ou pressa

Como se proteger

(específico para esse golpe):

• Verifique o remetente com atenção: observe o endereço de e-mail completo ou o número de telefone, não apenas o nome exibido. Bancos geralmente usam domínios corporativos oficiais.

• Desconfie de mensagens alarmistas: comunicações que criam senso de urgência ("Sua conta será bloqueada em 24 horas!") são táticas comuns de golpistas.

• Ative notificações oficiais: configure seu aplicativo bancário para receber notificações push, que são mais seguras que SMS.

• Aplicativos oficiais: nunca baixe aplicativos fora da loja oficial de seu celular.

Alerta importante: instituições financeiras NUNCA solicitam dados completos, senhas ou tokens por e-mail, SMS ou telefone. Qualquer comunicação pedindo essas informações deve ser considerada fraudulenta.

Sites, links e perfis falsos de instituições financeiras

O que é e como funciona:

Esta modalidade de fraude envolve a criação de sites, aplicativos, páginas em redes sociais ou perfis que imitam com perfeição a identidade visual e comunicação de instituições financeiras legítimas. O objetivo é enganar consumidores, fazendo-os acreditar que estão interagindo com bancos, financeiras ou corretoras reais.

1.

Domínios de internet similares aos oficiais (como “bancobrasil.com.br” ao invés de “bb.com.br”)

2.

Design profissional, copiando cores, logos e layouts dos sites verdadeiros

3.

Conteúdo convincente, incluindo termos técnicos e informações do mercado financeiro

4.

Certificados SSL falsos (o cadeado no navegador) para simular segurança

5.

Anúncios pagos em redes sociais e mecanismos de busca, aparecendo nos primeiros resultados

Esses sites e perfis falsos geralmente oferecem:

- Empréstimos com condições excepcionalmente vantajosas
- Renegociação de dívidas sem consulta a órgãos de proteção ao crédito
- Investimentos com rentabilidade muito acima do mercado
- Cartões de crédito sem análise de crédito
- Benefícios exclusivos para novos clientes

Exemplo prático:

Pedro, com restrições no nome, busca por “empréstimo sem consulta ao SPC” e encontra um anúncio patrocinado no Google. O link leva a um site idêntico ao de uma financeira conhecida, com depoimentos falsos de clientes satisfeitos.

Após preencher um formulário com dados pessoais, Pedro é informado que seu crédito foi “pré-aprovado”, mas precisa pagar uma taxa de R$ 300,00 para “análise cadastral e liberação”. Após o pagamento via PIX, o suposto atendente desaparece.

Quem são as principais vítimas:

• Pessoas com restrições de crédito buscando empréstimos
• Consumidores atraídos por ofertas muito vantajosas
• Investidores inexperientes buscando alta rentabilidade
• Usuários frequentes de redes sociais

Como se proteger

(específico para esse golpe):

• Verifique a URL com atenção: sites legítimos de bancos geralmente usam domínios oficiais e conexão segura (https://). Fique atento a pequenas alterações como letras trocadas ou adição de caracteres.
• Pesquise o CNPJ e a autorização do Banco Central: instituições financeiras legítimas devem ter registro no Banco Central do Brasil. Verifique no site do BC (www.bcb.gov.br).
• Nunca pague taxas antecipadas: instituições financeiras não cobram valores para “liberar crédito” ou “garantir investimentos”.

Alerta importante: mesmo perfis verificados em redes sociais podem ser falsificados ou hackeados. Sempre confirme ofertas pelos canais oficiais da instituição.

Golpe do investimento via PIX

O que é e como funciona:

O golpe do investimento via PIX explora a promessa de ganhos rápidos e expressivos com pequenos investimentos iniciais. Os criminosos criam esquemas que se apresentam como oportunidades legítimas de investimento, geralmente disfarçados como:

1. Plataformas de “missões remuneradas” ou “tarefas pagas”
2. Grupos exclusivos de investimento em criptomoedas
3. Arbitragem de apostas esportivas
4. Robôs de trading automático
5. Esquemas de cashback ou multiplicação de PIX

O mecanismo do golpe segue geralmente este padrão:

1. A vítima é atraída por anúncios em redes sociais ou é adicionada a grupos de WhatsApp/Telegram por conhecidos que já caíram no golpe.
2. É apresentada a uma oportunidade de “investimento” que promete retornos extraordinários (como multiplicar o dinheiro em horas ou dias).
3. Para começar, é solicitado um depósito inicial pequeno via PIX (R$ 50 a R$ 200).
4. Nos primeiros dias, a vítima realmente recebe alguns “lucros” (pagos com o dinheiro de novos entrantes), criando a falsa sensação de que o sistema funciona.
5. Incentivada pelos resultados iniciais, a vítima investe valores maiores e convida amigos e familiares.
6. Quando tenta sacar valores mais expressivos, encontra dificuldades, taxas adicionais ou o site/contato simplesmente desaparece.

Exemplo prático: Ricardo é adicionado a um grupo de WhatsApp chamado “Investimentos Garantidos 2025”. No grupo, várias pessoas compartilham prints de supostos lucros obtidos. Um “consultor” explica que o sistema funciona por meio de “missões”. Para iniciar, Ricardo precisa fazer PIX de valores específicos (começando com R$ 100) para diferentes chaves, e receberá de volta o valor mais uma comissão de 30%. Nas primeiras missões, Ricardo realmente recebe os valores prometidos. Animado, investe R$ 5.000 em uma “missão premium” que promete retorno de 50%. Após essa transferência, o grupo é fechado e o consultor desaparece.

Quem são as principais vítimas:

- Jovens em busca de renda extra
- Pessoas em dificuldades financeiras
- Indivíduos com pouco conhecimento sobre investimentos
- Usuários ativos de redes sociais e aplicativos de mensagens

Como se proteger
(específico para esse golpe):

- Desconfie de ganhos extraordinários: no mercado financeiro legítimo, altos retornos estão associados a altos riscos. Promessas de ganhos garantidos e expressivos em curto prazo são sinais claros de fraude.

- Verifique a regulamentação: empresas legítimas de investimento devem ser autorizadas pela CVM - Comissão de Valores Mobiliários. Consulte o site da CVM para verificar.

- Cuidado com o efeito manada: o fato de amigos ou familiares estarem participando não significa que o investimento é seguro – eles podem ser vítimas que ainda não perceberam o golpe.

Alerta importante: esquemas de pirâmide financeira inevitavelmente entram em colapso, pois dependem de um fluxo constante de novos participantes. Quando isso acontece, a maioria dos investidores perde todo o dinheiro aplicado.

Golpe do falso suporte técnico por redes sociais

O que é e como funciona:

Nesse golpe, criminosos criam perfis falsos em redes sociais (principalmente Instagram e Facebook) que se passam por canais oficiais de suporte técnico de bancos, empresas de telefonia, serviços de streaming ou outras instituições. Esses perfis são criados com nomes, logos e identidade visual muito semelhantes aos oficiais, como “Suporte Banco X” ou “Atendimento Banco Y”.

O golpe geralmente começa quando a vítima:

1.

Publica uma reclamação ou dúvida na página oficial da empresa marcando-a

2.

Busca por canais de atendimento nas redes sociais

3.

Encontra esses perfis falsos por meio de pesquisas ou anúncios

O falso perfil de suporte então entra em contato oferecendo ajuda imediata. Durante o atendimento, o golpista solicita dados pessoais, senhas, códigos de verificação ou induz a vítima a realizar procedimentos como “confirmar cadastro”, “atualizar aplicativo” ou “validar dispositivo”, que na verdade dão acesso às contas da vítima.

Em alguns casos, o golpista envia links para sites falsos ou solicita a instalação de aplicativos de acesso remoto, alegando que são ferramentas de suporte, quando na verdade são meios para obter controle sobre o dispositivo da vítima.

Exemplo prático:

Fernanda teve problemas para acessar seu aplicativo bancário e fez uma reclamação na página oficial do banco no Facebook. Minutos depois, recebeu uma mensagem privada de um perfil chamado “Suporte Banco X” com a mesma foto de perfil do banco oficial. O atendente apresentou-se como “Carlos da equipe de suporte digital” e informou que poderia resolver o problema remotamente.

Para isso, pediu que Fernanda instalasse um aplicativo de “suporte técnico” (na verdade, um software de acesso remoto) e que fornecesse seu CPF e a senha do aplicativo bancário para “verificação de segurança”. Após fornecer os dados, Fernanda teve sua conta invadida e diversos PIX realizados.

Quem são as principais vítimas:

• Pessoas com problemas técnicos urgentes em serviços bancários
• Usuários com pouca familiaridade com canais oficiais de suporte
• Clientes frustrados com o tempo de espera em canais tradicionais de atendimento
• Usuários frequentes de redes sociais

Como se proteger

(específico para esse golpe):

• Verifique a autenticidade do perfil: perfis oficiais de grandes empresas geralmente possuem o selo de verificação (marca azul). Verifique também há quanto tempo o perfil existe, número de seguidores e qualidade das publicações.

• Use apenas canais oficiais: acesse os canais de suporte por meio do site oficial da empresa ou dos números de telefone que constam no verso do seu cartão ou em documentos oficiais.

• Nunca compartilhe senhas ou códigos: equipes legítimas de suporte técnico nunca solicitam senhas completas, tokens ou códigos de verificação.

• Cuidado com links enviados durante o atendimento: mesmo em atendimentos legítimos, é mais seguro acessar o site oficial digitando o endereço diretamente no navegador. Evite pesquisas por meio de sites de pesquisa, como Google, Yahoo, etc.

Alerta importante: empresas sérias nunca pedem instalação de aplicativos de acesso remoto para
resolver problemas bancários. Se isso for solicitado, é um forte indício de fraude.

Clonagem de anúncios e intermediação falsa

O que é e como funciona:

Esse golpe visa principalmente pessoas que compram ou vendem produtos em plataformas de comércio eletrônico e marketplaces (como OLX, Mercado Livre, Facebook Marketplace). Os criminosos atuam de duas formas principais:

1.

Clonagem de anúncios: copiam anúncios legítimos de produtos (geralmente de alto valor, como eletrônicos, veículos ou imóveis), incluindo fotos e descrições, mas oferecem preços significativamente mais baixos. Quando um interessado contata o falso vendedor, este solicita um depósito ou sinal para "reservar o produto" ou "iniciar o processo de entrega", mas nunca entrega o item.

2.

Falsa intermediação: o golpista passa-se por suposto "intermediário" ou "serviço de garantia" de uma plataforma conhecida. Após o comprador e vendedor legítimos entrarem em acordo, o golpista entra em contato (geralmente por WhatsApp) alegando ser do "departamento de segurança" do marketplace e oferece um processo "seguro" para a transação. O objetivo é convencer uma ou ambas as partes a enviarem dinheiro ou produtos para o golpista, que desaparece em seguida.

Exemplo prático:

João anunciou seu notebook por R$ 3.500 no Marketplace do Facebook. Após negociar com um comprador interessado, recebeu mensagem de número desconhecido, identificando-se como "Serviço de Proteção ao Vendedor do Facebook". O falso atendente explicou que, para garantir a segurança da transação, o comprador já havia depositado o valor em uma "conta garantidora", e que o dinheiro seria liberado assim que João e que o dinheiro seria liberado assim que João enviasse o produto. Enviaram até um link de um site falso no qual João poderia "acompanhar" a transação. Confiando no processo, João enviou o notebook, mas nunca recebeu o pagamento.

Quem são as principais vítimas:

• Compradores atraídos por preços muito abaixo do mercado

• Vendedores inexperientes em plataformas de comércio eletrônico

• Pessoas com pressa para concluir transações

• Usuários que desconhecem os processos oficiais das plataformas

Como se proteger

(específico para esse golpe):

• Utilize apenas os canais oficiais da plataforma: mantenha toda a negociação dentro do ambiente da plataforma até estar certo da legitimidade da outra parte.

• Desconfie de preços muito abaixo do mercado: se um produto está sendo vendido por um valor muito inferior ao praticado, há grande chance de ser fraude.

• Verifique a reputação do vendedor/comprador: analise avaliações, tempo de cadastro na plataforma e comentários de outros usuários.

• Conheça o processo oficial: familiarize-se com os procedimentos legítimos da plataforma que está utilizando. Marketplaces sérios nunca pedem que você envie produtos antes de confirmar o recebimento do pagamento.

• Prefira métodos de pagamento seguros: utilize os sistemas de pagamento integrados às plataformas, que geralmente oferecem proteção ao comprador e ao vendedor.

Alerta importante: plataformas de marketplace legítimas nunca entram em contato por WhatsApp para intermediar transações ou solicitar depósitos em contas de terceiros. Toda comunicação oficial é realizada pelos canais da própria plataforma.

Golpes Tradicionais Ainda Ativos

Apesar da sofisticação crescente das fraudes digitais, muitos golpes tradicionais continuam fazendo vítimas, adaptando-se sutilmente às novas realidades, mas mantendo sua essência enganosa. Conhecer essas táticas mais comuns é fundamental, pois os criminosos frequentemente as combinam com novas tecnologias ou se aproveitam da familiaridade que as pessoas têm com certos procedimentos para aplicar o golpe. Este bloco revisita os golpes tradicionais que ainda representam risco significativo.

Golpe da Falsa Central de Atendimento

O que é e como funciona:

Atualmente, esse é um dos golpes mais comuns praticados pelos fraudadores, que utilizam de uma tática de engenharia social para obter informações pessoais e causar prejuízos financeiros.

O criminoso entra em contato com a vítima passando-se por funcionário do banco ou empresa com a qual mantém um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema e, a partir daí, solicita os dados pessoais e financeiros da vítima. Em alguns casos, pede para que ela ligue na central do banco, no número que aparece atrás do seu cartão, mas o fraudador continua na linha para simular o atendimento da central e pedir os dados da sua conta, dos seus cartões e, principalmente, sua senha quando você a digitar.

Esse golpe também pode ser aplicado por meio de redes sociais, e-mail, SMS e WhatsApp, sempre em tom alarmante, informando possível invasão à sua conta junto a uma instituição financeira, ou uma compra recusada com seu cartão, informando um número de contato para bloquear a transação. Diante da urgência e iminência de invasão, comumente a vítima entra em piloto automático e não desconfia das informações que são passadas ao falso funcionário.

Exemplo prático:

Maria recebe ligação de um número que parece ser do seu banco. O suposto atendente informa que detectaram uma compra suspeita de alto valor em seu cartão e que, para cancelar, ela precisa confirmar alguns dados e digitar sua senha no teclado do telefone. Em outra variação, pedem que ela instale um "módulo de segurança" no celular, que na verdade dá acesso total ao aparelho para o golpista.

Quem são as principais vítimas:

• Clientes de bancos em geral, especialmente idosos ou pessoas com menor familiaridade com questões de segurança digital

• Pessoas que recentemente enfrentaram problemas reais com o banco e estão mais suscetíveis a acreditar no contato

Como se proteger
(específico para esse golpe):

• Desligue a chamada imediatamente: se receber uma ligação suspeita, mesmo que o número pareça oficial, desligue.

• Você entra em contato com o banco: utilize os números de telefone oficiais que constam no verso do seu cartão, no site oficial do banco (digitando o endereço no navegador) ou no aplicativo oficial. Nunca use números fornecidos na ligação suspeita.

• Bancos não pedem sua senha: nenhuma instituição financeira legítima solicita sua senha completa, token ou CVV por telefone, SMS ou e-mail.

• Não instale aplicativos sob orientação de terceiros por telefone.

Alerta importante: o golpe da falsa central é frequentemente o primeiro passo para outros golpes, como o da "mão fantasma" ou o do "motoboy". A informação é sua melhor defesa.

Golpe do Motoboy

O que é e como funciona:

Esse golpe é uma modalidade antiga na qual uma pessoa recebe uma ligação de um fraudador passando-se por funcionário de seu banco, dizendo que seu cartão foi clonado e que irão encaminhar um motoboy para recolher o cartão para efetivação do bloqueio.

A sofisticação é tamanha que criminosos usam até mesmo softwares para simular músicas de espera de bancos e som ambiente de call center, além de conseguirem reter a linha telefônica das vítimas. Assim, com a entrega do cartão ao motoboy, juntamente com os dados pessoais e senha solicitadas durante a ligação, os criminosos conseguem utilizar o cartão para realizar saques, empréstimos, compras e pagamentos de boletos.

Exemplo prático:

Seu João recebe ligação informando que seu cartão foi usado em uma compra suspeita. O falso atendente o convence de que o cartão precisa ser bloqueado e recolhido. Pede que Seu João corte o cartão, mas preserve o chip, e anote a senha em um papel.

Um motoboy uniformizado chega à sua casa pouco tempo depois para "recolher o cartão para perícia".

Quem são as principais vítimas:

• Principalmente idosos, que podem ser mais facilmente convencidos pela urgência e pela suposta "ajuda" oferecida.

• Pessoas que confiam na autoridade de quem se apresenta como funcionário do banco.

Como se proteger

(específico para esse golpe):

• Bancos NUNCA recolhem cartões na residência do cliente: nenhuma instituição financeira envia motoboys ou funcionários para buscar cartões, mesmo que cancelados ou com suspeita de fraude.

• Não entregue seu cartão a ninguém.

• Se receber ligação desse tipo, desligue e contate seu banco pelos canais oficiais.

• Destrua completamente cartões inutilizados: ao descartar um cartão, certifique-se de destruir o chip e a tarja magnética de forma que não possam ser recuperados.

Alerta importante:
A sofisticação dos golpistas pode incluir o uso de uniformes falsos e crachás.
A regra é clara: nunca entregue seu cartão.

Golpe da Mão Fantasma

O que é e como funciona:
O golpe da mão fantasma possui um trato de engenharia social mais avançado, além de ser necessária a participação da própria vítima para a concretização do golpe. Inicialmente, a vítima recebe uma ligação na qual a gravação aparenta ser aquelas provenientes de centrais telefônicas de bancos e instituições financeiras.

Ao ser transferido para um atendente, que neste caso é o próprio criminoso, o consumidor é informado que há movimentações estranhas, como uma compra suspeita e até mesmo possível invasão na conta. A intenção é deixar a pessoa preocupada e insegura com a informação, facilitando a aplicação do golpe.

A partir desse momento, os criminosos, passando-se por funcionários dos bancos, induzem a vítima a acessar algum link para a instalação de um aplicativo que irá solucionar o problema. Ao instalar, no entanto, o criminoso passa a ter acesso a todos os dados que estão no smartphone ou no computador, a depender do local em que foi realizada a operação, inclusive os bancários.

Com acesso ao aparelho, os fraudadores realizam buscas minuciosas, pesquisam por senhas armazenadas pelos próprios usuários em aplicativos e sites e, dessa forma, realizam transações fraudulentas, como transferências, pagamento de contas e boletos e solicitação de empréstimos.

Exemplo prático:
Clara recebe ligação de um suposto técnico do banco informando que seu aplicativo está desatualizado e vulnerável. Ele a instrui a baixar um "novo módulo de segurança" por meio de um link enviado por SMS.

Após a instalação, o "técnico" pede que ela abra o aplicativo 23 do banco para "verificar". Enquanto Clara navega, o golpista, com acesso remoto, realiza um PIX de alto valor.

Quem são as principais vítimas:

• Pessoas com menor conhecimento técnico sobre segurança de dispositivos.

• Usuários que confiam em supostos atendentes e seguem instruções por telefone.

Como se proteger
(específico para esse golpe):

• Não instale aplicativos ou softwares por orientação recebida em ligações ou mensagens suspeitas.

Baixe aplicativos apenas das lojas oficiais (Google Play Store, Apple App Store).

• Desconfie de qualquer solicitação para acesso remoto ao seu dispositivo. Bancos não pedem isso para resolver problemas comuns.

• Mantenha seu sistema operacional e antivírus atualizados.

• Monitore as permissões dos aplicativos instalados.

Alerta importante: se você suspeitar que seu dispositivo foi comprometido, desconecte-o da internet imediatamente e procure assistência técnica de confiança. Contate seu banco por outro dispositivo.

Golpe no WhatsApp (Perfil Falso ou Clonado)

O que é e como funciona:

Outro meio pelo qual os fraudadores aplicam o golpe relaciona-se à clonagem do WhatsApp. Nessa fraude, o criminoso consegue criar uma conta nova por intermédio de informações e fotos encontradas em redes sociais da vítima.

Depois de conseguir os contatos, o golpista utiliza um número desconhecido alegando que algo emergencial aconteceu, como um assalto, ou utilização do novo número apenas para utilização pessoal e o antigo para o trabalho, para justificar o número novo e assim poder pedir dinheiro aos contatos via transferência Pix.

Exemplo prático: Ana recebe mensagem no WhatsApp de um número desconhecido, mas com a foto de sua amiga Beatriz. A mensagem diz: “Oi, Ana, troquei de número, anota aí! Estou com um problema, preciso pagar um boleto urgente e meu app do banco não está funcionando, pode fazer um PIX pra mim? Te devolvo amanhã sem falta.” Ana, acreditando ser Beatriz, faz a transferência, concretizando o golpe.

Quem são as principais vítimas:

• Amigos e familiares da pessoa que teve o WhatsApp clonado ou o perfil falsificado.

• Pessoas que não desconfiam de pedidos de dinheiro vindos de conhecidos.

Como se proteger (específico para esse golpe):

• Ative a verificação em duas etapas no seu WhatsApp: isso dificulta a clonagem da sua conta.

• Desconfie de pedidos de dinheiro inesperados: mesmo que venham de conhecidos, especialmente se for de um número novo ou com uma história urgente e mirabolante.

• Confirme a identidade por outro meio: ligue para a pessoa (no número antigo que você já tinha) ou faça uma pergunta que só ela saberia responder antes de fazer qualquer transferência.

• Avise seus contatos: se seu WhatsApp for clonado ou tiverem criado um perfil falso seu, avise seus amigos e familiares o mais rapidamente possível por outros meios.

Alerta importante: nunca compartilhe códigos de verificação do WhatsApp com ninguém.

Golpe da Troca de Cartão

O que é e como funciona:

O golpe inicia-se quando o cliente dirige-se a um caixa eletrônico, seja ele dentro de um banco, ou shopping centers ou até caixas 24 horas. Diante de alguma eventual dificuldade do cliente em utilizar o caixa eletrônico, a pessoa apresenta-se, como funcionário do banco, ou até um terceiro solícito em ajudar alguém em dificuldade.

Em seguida, o fraudador auxilia a realização do serviço que o cliente estava com dificuldade, acompanhando toda a transação, a fim de "auxiliar". Ao final, retira o cartão do caixa eletrônico, efetivando a troca desse e entregando outro cartão à vítima.

Diante do acompanhamento de todas as transações, o fraudador costuma observar senhas e acessos, a fim de poder reproduzi-las, posteriormente, mediante a posse do cartão fraudado.

Exemplo prático:

Maria está usando um caixa eletrônico e aparenta ter dificuldades. Um homem bem-vestido aproxima-se e oferece ajuda. Ele a instrui a inserir o cartão e digitar a senha. Após algumas tentativas "frustradas", ele devolve o cartão a Maria, que vai embora. Mais tarde, Maria percebe que o cartão devolvido não é o seu, mas um similar. O golpista ficou com o cartão original e a senha que observou, efetivando diversas compras com esse.

Quem são as principais vítimas:

• Idosos ou pessoas com dificuldades em usar caixas eletrônicos.

• Pessoas distraídas durante pagamentos em estabelecimentos.

Como se proteger (específico para esse golpe):

• Não aceite ajuda de estranhos em caixas eletrônicos. Procure um funcionário do banco, se necessário. • Proteja sua senha: ao digitar a senha, cubra o teclado com o corpo e a mão. • Confira seu cartão: sempre verifique se o cartão devolvido após uma transação é realmente o seu.

• Cuidado com maquininhas adulteradas ou comportamentos suspeitos de vendedores.

Alerta importante: muitos cartões hoje possuem tecnologia de pagamento por aproximação (NFC). Se seu cartão for trocado e tiver essa função ativa, o golpista pode realizar compras de baixo valor sem precisar da senha.

Golpe do Boleto Falso

O que é e como funciona:

Os boletos fazem parte do dia a dia do brasileiro. Assim, é evidente que pelo costume e pela rotina os brasileiros efetivam o pagamento de inúmeros boletos diariamente e por muitas vezes não se atentam aos detalhes, abrindo caminho aos fraudadores.

Mais comumente, o golpe do boleto falso utiliza dados pessoais disponíveis na internet para enviar uma cobrança fingindo ser uma empresa que você utiliza. Costumeiramente, as pessoas recebem um e-mail com a informação de que se encontram em débito com alguma fatura de alguma empresa de telefonia, ou banco, ou cartão de crédito, e que com o referido boleto podem quitar a referida obrigação, muitas vezes com desconto, incitando a vítima a efetivar o pagamento como se estivesse quitando seu débito.

Há também a aplicação do golpe do boleto falso para compras via internet. Geralmente os criminosos se utilizam de lojas virtuais falsas, assemelhadas com as verdadeiras, com estruturas, cores e até logotipos semelhantes, ofertando produtos com descontos para pagamento por boleto, assim induzindo a vítima a efetivar o pagamento desse boleto para um terceiro.

Exemplo prático:

Carlos recebe por e-mail um boleto que parece ser da sua operadora de internet, com um pequeno desconto para pagamento antecipado. Ele paga o boleto sem conferir os dados detalhadamente. No mês seguinte, recebe uma cobrança da operadora informando que a fatura anterior está em aberto.

Quem são as principais vítimas:

• Qualquer pessoa que pague contas por boleto.

• Empresas que realizam muitos pagamentos via boleto.

Como se proteger

(específico para esse golpe):

• Confira os dados do beneficiário: antes de pagar qualquer boleto, verifique se os dados do vendedor e do beneficiário estão corretos, se o valor cobrado está alinhado com o valor que deve ser pago.

• Verifique a fonte: confirme se o e-mail, WhatsApp ou site que enviou o boleto é uma fonte segura.

• Atenção a erros de digitação: verifique se há erros de digitação no boleto, que podem indicar fraude.

• Use o DDA - Débito Direto Autorizado: se disponível, cadastre suas contas em DDA. Os boletos são registrados eletronicamente em seu CPF/CNPJ, reduzindo o risco de fraudes.

Alerta importante: ao pagar um boleto on-line, a tela de confirmação do seu banco sempre mostrará os dados do beneficiário final. Se estiverem diferentes do esperado, NÃO conclua o pagamento.

Golpe do Falso Leilão

O que é e como funciona:

Esse tipo de golpe trata-se da criação, pelos fraudadores, de um site de leilão de carros, motos, ônibus, caminhões e demais bens móveis, com a intenção de leiloar, expondo que erados por instituições financeiras. Aproveitando o interesse do consumidor, os criminosos criam um site falso com propostas tentadoras para aplicar o golpe nas vítimas. Visando passar a imagem de legalidade, os estelionatários fazem o atendimento do consumidor, respondem a dúvidas, fazem o cadastro junto ao site. Porém, após o arremate do bem em leilão e o pagamento, o suposto leiloeiro passa endereço onde buscar o bem, porém o endereço é inexistente, e com isso não mais atendem o consumidor.

Exemplo prático: Fernanda busca por carros usados e encontra um site de leilão com veículos recuperados de financeira a preços muito atrativos. Ela cadastra-se, arremata um carro por um valor 30% abaixo da tabela Fipe e recebe

instruções para depositar 50% do valor em uma conta para garantir a compra. Após a transferência, não consegue mais contato com o suposto leiloeiro.

Quem são as principais vítimas:

• Pessoas em busca de bens com preços muito baixos.
• Consumidores com pouca experiência em leilões.

Como se proteger (específico para esse golpe):

• Verifique se o leiloeiro é oficial: consulte o site da Junta Comercial do seu estado ou de associações de leiloeiros para verificar se o leiloeiro é matriculado e está ativo.

• Desconfie de preços excessivamente baixos: bens em leilão podem ter preços vantajosos, mas valores absurdamente baixos são um grande sinal de alerta.

• Visite o pátio (se possível): leilões costumam permitir a visitação dos bens antes do arremate. Desconfie se não houver essa possibilidade ou se o endereço fornecido for vago ou suspeito.

• Pesquise a reputação do site/leiloeiro: busque por reclamações on-line, notícias ou processos judiciais.

Alerta importante:

Muitos sites falsos de leilão utilizam indevidamente nomes e logotipos de instituições financeiras conhecidas para dar aparência de legitimidade.

Golpe do Empréstimo com Depósito Antecipado

O que é e como funciona:

Os falsários encaminham mensagens, e-mail e até telefones oferecendo empréstimos com juros relativamente acessíveis, e sem a necessidade de estar com nome limpo. Aproveitando-se da necessidade da vítima em ter o dinheiro de forma rápida, muitas vezes para ser utilizado em questões de emergência, é solicitado pelos estelionatários um depósito prévio a título de pagamento de cadastro ou seguro, impondo esse depósito como condição de liberação do empréstimo. Quando é depositado o valor, o empréstimo não cai, e os atendentes/ falsários nãomais atendem a pessoa, que fica com o dano financeiro.

Exemplo prático:

Roberto está precisando de dinheiro e encontra um anúncio on-line de uma financeira que oferece “empréstimo para negativados, liberação em 24 horas”. Ele entra em contato e é informado que seu crédito de R$ 5.000,00 foi aprovado, mas, para liberar o valor, ele precisa depositar R$ 350,00 referente a uma “taxa de seguro obrigatório”.

Após fazer o PIX, não recebe o empréstimo e não consegue mais contato.

Quem são as principais vítimas:

• Pessoas com nome negativado ou com dificuldades de obter crédito.

• Indivíduos em situação de vulnerabilidade financeira e com urgência em conseguir dinheiro.

Como se proteger

(específico para esse golpe):

• instituições financeiras NÃO cobram taxas antecipadas: nenhum banco ou financeira regulamentada pelo Banco Central exige depósito prévio para liberar empréstimos. As taxas e impostos são geralmente diluídos nas parcelas do empréstimo.

• Desconfie de ofertas muito facilitadas: promessas de empréstimo sem consulta cadastral ou com aprovação garantida são fortes indícios de golpe.

• Verifique se a instituição é autorizada pelo Banco Central: consulte o site do Bacen para confirmar se a empresa possui autorização para operar.

• Não faça depósitos em contas de pessoas físicas para “liberar empréstimo”.

Golpe do Falso Protesto

O que é e como funciona:

Os criminosos obtêm a informação de dívida de um consumidor, dívidas muitas vezes já prescritas, e encaminham mensagens, e-mails e até telefonemas informando que aquele consumidor está com o nome protestado por essa dívida. Para passar a imagem de legalidade, encaminham o título do protesto, com o brasão das entidades públicas e do suposto cartório, oferecendo vantagens aos devedores na quitação dos débitos existentes.

Assim, quando o consumidor tenta regularizar a situação, os falsários encaminham um boleto para pagamento, no qual os valores cairão na conta dos falsários. Nesse caso, se o pagamento for feito, o envio do título de quitação não se concretiza. O prejuízo nesses casos é em dobro, já que depois a vítima precisa quitar a dívida com a pessoa ou a empresa que realmente está devendo.

Exemplo prático:

Uma pequena empresa recebe um e-mail com um arquivo PDF que simula uma intimação de protesto de um cartório de outra cidade, referente a uma duplicata não paga. O e-mail informa que, para regularizar a situação e evitar o protesto efetivo, a empresa deve pagar um boleto anexo no valor de R$ 1.800,00 em até 48 horas. Preocupado, o administrador paga o boleto, descobrindo depois que era falso.

Quem são as principais vítimas:

- Empresas de todos os portes.
- Pessoas físicas que podem se assustar com a ameaça de protesto.

Como se proteger

(específico para esse golpe):

- Consulte a veracidade do protesto: antes de realizar qualquer pagamento, verifique diretamente com o cartório de protesto indicado na suposta intimação (procure o contato oficial do cartório, não o fornecido na comunicação suspeita) ou consulte plataformas oficiais de consulta de protestos, como o site da Cenprot-Central Nacional de Protesto.

• Desconfie de cobranças inesperadas ou de dívidas desconhecidas.
• Analise a comunicação com cuidado: verifique erros de português,informações inconsistentes ou um senso de urgência exagerado.
• Não pague boletos ou faça PIX sem confirmar a origem da dívida
e a legitimidade da cobrança.

Alerta importante: intimações de protesto oficiais seguem um rito formal. Desconfie de comunicações que fogem muito desse padrão ou que pressionam excessivamente para um pagamento rápido via canais informais.

Golpe do Consignado/RMC-Reserva de Margem Consignável

O que é e como funciona:

O golpe do empréstimo consignado e, mais especificamente, o relacionado ao Cartão de Crédito Consignado com Reserva de Margem Consignável-RMC, afeta principalmente aposentados, pensionistas do INSS e servidores públicos. A RMC é uma parcela da renda (geralmente 5%) que pode ser utilizada para o pagamento mínimo de uma fatura de cartão de crédito consignado.

O golpe ocorre de diversas formas:

1.

Contratação sem consentimento: o consumidor descobre um desconto em seu benefício referente a um cartão RMC que nunca solicitou ou utilizou.

2.

Oferta enganosa de empréstimo: o consumidor acredita estar contratando um empréstimo consignado comum, mas na verdade está aderindo a um cartão de crédito consignado.

3.

Venda casada: o cartão RMC é empurrado junto com a contratação de um empréstimo consignado tradicional, sem o devido esclarecimento.

O principal problema é que, ao pagar apenas o valor mínimo descontado em folha, o saldo devedor do cartão de crédito consignado continua crescendo devido aos juros, transformando-se em uma “dívida infinita”.

Exemplo prático:

Dona Maria, aposentada, foi a um correspondente bancário para solicitar um empréstimo consignado de R$ 2.000,00. O atendente informou que ela tinha uma “margem extra” disponível e ofereceu um valor adicional, que ela aceitou. Meses depois, ao verificar seu extrato do INSS, percebeu um desconto mensal referente a “RMC” e descobriu que, na verdade, havia contratado um cartão de crédito consignado.

Como se proteger

(específico para esse golpe):

- Leia atentamente todos os contratos: antes de assinar qualquer documento, especialmente propostas de empréstimo ou cartão, leia todas as cláusulas.
- Questione a natureza do produto: pergunte explicitamente se o que está sendo oferecido é um empréstimo consignado tradicional ou um cartão de crédito consignado com RMC.
- Monitore seu extrato de benefício/ contracheque: verifique regularmente se há descontos não autorizados ou desconhecidos.

Alerta importante: se houver efetivamente contratado o cartão de crédito consignado, é importante efetivar o pagamento integral da fatura, podendo o consumidor pedir meios para pagamento do valor em aberto, ou de parte dele, a fim de que diminua a incidência de juros, possibilitando assim a quitação do financiamento realizado.

Falsa Portabilidade de Empréstimo com “Devolução de Juros”

O que é e como funciona:

Esse golpe explora o desconhecimento sobre a portabilidade de crédito e a promessa de vantagens financeiras inexistentes. Os criminosos contatam a vítima, geralmente aposentados ou pensionistas com empréstimos consignados, oferecendo uma “oportunidade” de reduzir parcelas ou receber de volta “juros abusivos”.

O golpista passa-se por representante de uma financeira, afirma que a vítima tem direito a uma portabilidade com devolução de juros ou “troco”. Para isso, a vítima é induzida a contratar um novo empréstimo. O valor desse novo empréstimo é creditado na conta da vítima, mas o golpista a instrui a transferir parte ou todo esse valor para uma conta de terceiros, alegando ser pagamento de taxas ou a devolução do valor que “excedeu” a quitação.

Exemplo prático:

Seu Antenor, aposentado, recebe uma ligação de uma suposta “Consultoria Financeira” informando que ele paga juros abusivos e tem direito a receber R$ 5.000,00 de volta. Para isso, precisaria fazer uma “nova operação de portabilidade” e pegar um novo empréstimo de R$ 15.000,00. Assim que o valor cai na conta, o falso consultor diz que R$ 10.000,00 quitarão o empréstimo antigo e os R$ 5.000,00 são o “troco”, mas ele precisa transferir R$ 2.000,00 para a consultoria como “taxa de serviço”. Seu Antenor transfere, mas descobre depois que o empréstimo antigo não foi quitado e agora ele tem duas dívidas.

Como se proteger

(específico para esse golpe):

- Não contrate empréstimos para transferir a terceiros: nenhuma instituição financeira solicita que você pegue um empréstimo para depois transferir o valor para eles como taxa.
- Procure diretamente seu banco ou financeiras conhecidas: se deseja fazer a portabilidade de um empréstimo, procure instituições de confiança.

Fraudes com Dispositivos e Portabilidade

A segurança dos nossos dispositivos móveis e a atenção aos processos de portabilidade são cruciais para evitar golpes financeiros. Este bloco detalha fraudes comuns relacionadas a celulares, tablets e à portabilidade de serviços, oferecendo orientações específicas para proteger suas informações e seu dinheiro.

Golpes após Furto ou Roubo de Celular

O que é e como funciona:

O furto ou roubo de um celular deixou de ser apenas a perda do aparelho físico; transformou-se em uma porta de entrada para o acesso indevido a informações pessoais e, principalmente, a aplicativos bancários. Os criminosos, muitas vezes especializados, buscam desbloquear o aparelho para realizar transações financeiras, solicitar empréstimos, fazer compras ou vender dados pessoais da vítima.

As táticas para obter acesso incluem:

1. Engenharia social reversa: observar a vítima digitando a senha de desbloqueio antes do roubo.
2. Aproveitamento de senhas fracas: tentativas de senhas comuns (datas de nascimento, sequências numéricas) ou senhas anotadas junto ao aparelho.
3. Remoção do chip (SIM Card): para tentar receber códigos de recuperação de senha de aplicativos em outro aparelho, caso a vítima não bloqueie a linha rapidamente.
4. Acesso a e-mails e aplicativos de mensagens: se não estiverem protegidos por senhas adicionais, podem ser usados para redefinir senhas de outros serviços, incluindo bancos.

5.

Exploração de falhas de segurança: em alguns casos, utilizam técnicas para burlar o bloqueio de tela ou acessam informações salvas de forma insegura.

Exemplo prático:

Joana teve seu celular furtado em um evento. O aparelho não possuía senha de bloqueio no chip e a senha de desbloqueio da tela era uma sequência simples. Os criminosos acessaram seu aplicativo de e-mail, que estava logado, e solicitaram a recuperação de senha do seu aplicativo bancário. Com o novo acesso, realizaram diversas transferências via PIX e solicitaram um empréstimo pessoal, causando um prejuízo de milhares de reais antes que Joana conseguisse bloquear tudo.

Como se proteger

(específico para esse golpe):

• Bloqueio do SIM Card (PIN do Chip): ative a senha do PIN do seu chip. Isso impede que ele seja usado em outro aparelho sem essa senha.

• Anote o Imei do aparelho: esse número é essencial para solicitar o bloqueio do dispositivo junto à operadora em caso de perda ou roubo. Para saber o Imei, disque *#06# no seu celular.

• Cuidado ao usar o celular em público: esteja atento ao seu redor, especialmente em locais movimentados.

O que fazer em caso de furto ou roubo (ações imediatas específicas):

1.

Bloqueie a linha telefônica e o Imei: entre em contato imediatamente com sua operadora para solicitar o bloqueio do chip (linha) e do aparelho (Imei).

2.

Comunique seus bancos: informe todas as instituições financeiras sobre o ocorrido e solicite o bloqueio de contas, cartões e acessos a aplicativos.

3.

Altere senhas prioritárias: mude imediatamente as senhas de e-mails, redes sociais e outros serviços importantes que estavam acessíveis pelo celular.

4.

Utilize recursos de localização e bloqueio remoto: Se tiver configurado (como “Localizador” do Android ou “Buscar iPhone” da Apple), tente localizar, bloquear ou apagar os dados do aparelho remotamente.

Golpes por Falta de Segurança em Dispositivos Móveis

O que é e como funciona:

Além do risco de furto ou roubo, a falta de cuidados básicos com a segurança dos dispositivos móveis (smartphones e tablets) pode expor os usuários a diversos tipos de golpes, mesmo com o aparelho em mãos. Isso inclui:

1.

Instalação de malwares e spywares: aplicativos maliciosos baixados de fontes não confiáveis ou por meio de links suspeitos podem roubar dados, monitorar atividades (keyloggers), exibir anúncios invasivos ou até mesmo controlar o dispositivo remotamente.

2.

Phishing via aplicativos: notificações falsas ou mensagens dentro de aplicativos podem direcionar para páginas de login falsas, capturando credenciais.

3.

Ataques via wi-fi público: redes wi-fi abertas e não seguras podem ser usadas por criminosos para interceptar dados transmitidos, incluindo senhas e informações bancárias (ataques “Man-in-the-Middle”).

4.

Vulnerabilidades de softwares: sistemas operacionais e aplicativos desatualizados podem conter falhas de segurança conhecidas que são exploradas por hackers.

5.

Engenharia social: golpistas podem ligar ou enviar mensagens se passando por suporte técnico, solicitando acesso remoto ao dispositivo ou a instalação de softwares específicos sob falsos pretextos.

Exemplo prático:

Carlos baixou um aplicativo de "limpeza de memória" de um site não oficial. O aplicativo, na verdade, era um malware que começou a exibir anúncios em tela cheia e, secretamente, capturava os dados digitados em outros aplicativos, incluindo suas senhas bancárias.

Semanas depois, Carlos notou transações desconhecidas em sua conta.

Como se proteger

(específico para esse golpe):

• Baixe aplicativos apenas de lojas oficiais: utilize a Google Play Store (Android) ou a App Store (iOS) e verifique as avaliações e permissões solicitadas pelo app antes de instalar.

• Revise as permissões dos aplicativos: verifique quais permissões cada aplicativo tem (acesso a contatos, localização, microfone, câmera) e revogue as que não forem essenciais para o funcionamento do app.

• Não faça "root" (Android) ou "jailbreak" (iOS) no seu dispositivo: esses procedimentos removem camadas de segurança importantes, tornando o aparelho mais vulnerável.

Fraude na Portabilidade de Salário

O que é e como funciona:

A portabilidade de salário é um direito do trabalhador. O golpe ocorre quando criminosos, de posse dos dados pessoais e bancários da vítima, solicitam a portabilidade do salário para uma conta fraudulenta, sem seu conhecimento.

Os golpistas obtêm os dados por meio de vazamentos, phishing, compra de dados ilegais ou engenharia social. Com os dados, abrem uma conta digital e solicitam a portabilidade.

Exemplo prático:

Roberto, servidor público, teve seus dados vazados. Criminosos abriram uma conta digital em seu e nome solicitaram a portabilidade do seu salário. No dia do pagamento, Roberto percebeu que o dinheiro não caiu em sua conta habitual.

Como se proteger

(específico para esse golpe):

• Monitore seus dados e CPF: utilize serviços como o Registrato, do Banco Central, para verificar contas abertas em seu nome, e o Serasa Premium para monitorar consultas ao seu CPF.

• Desconfie de contatos solicitando dados para “atualização cadastral” ou “confirmação de portabilidade” não solicitada por você.

Como Proteger-se: Prevenção Geral Contra Fraudes

As fraudes bancárias estão em constante evolução, tornando-se cada vez mais sofisticadas. No entanto, com atenção, conhecimento e adoção de hábitos seguros, é possível reduzir significativamente os riscos. Este bloco consolida as principais orientações de prevenção, aplicáveis a diversos tipos de golpes, para que você possa proteger suas informações financeiras e pessoais de forma eficaz.

Desconfiança é a Primeira Linha de Defesa

• Ofertas com retornos financeiros elevados e imediatos: se a oferta promete lucros muito superiores aos praticados por investimentos tradicionais e regulamentados, ou ganhos garantidos sem risco, desconfie profundamente. Não existe dinheiro fácil. Esquemas como pirâmides financeiras, falsos investimentos em criptomoedas ou propostas de “multiplicação de PIX” são clássicos.

• Pressão para agir rapidamente: golpistas costumam criar um senso de urgência, alegando que a “oportunidade é única” ou “por tempo limitado”, para impedir que a vítima pesquise ou reflita. Não ceda à pressão.

• Solicitações inesperadas de dinheiro: mesmo que venham de números ou perfis que pareçam de conhecidos, sempre confirme por um segundo canal de comunicação antes de realizar qualquer transferência.

Cuidado com Links, Arquivos e Comunicações Suspeitas

• Não clique em links desconhecidos: evite clicar em links recebidos por e-mail, SMS, WhatsApp, Telegram ou mensagens em redes sociais, especialmente se o remetente for desconhecido, a mensagem tiver um tom alarmista, erros de português ou ofertas boas demais para serem verdade.

• Acesse sites oficiais diretamente: se a mensagem parecer ser do seu banco ou de uma loja conhecida, digite o endereço do site diretamente no seu navegador ou use o aplicativo oficial, em vez de clicar no link recebido.

• Verifique o remetente: analise o endereço de e-mail completo ou o número de telefone. Golpistas podem usar nomes parecidos com os de instituições legítimas, mas com pequenas alterações.

• Cuidado com anexos: não baixe ou abra arquivos de e-mails ou mensagens de fontes não confiáveis, pois podem conter malware.

Proteja Seus Dados Pessoais e Bancários

• Senhas fortes e únicas: utilize senhas complexas (com letras maiúsculas, minúsculas, números e símbolos) e diferentes para cada serviço, especialmente os financeiros. Evite senhas óbvias como datas de nascimento ou sequências numéricas.

• Autenticação de dois fatores (MFA): habilite a MFA (ou verificação em duas etapas) em todos os aplicativos e serviços on-line que oferecem essa camada extra de segurança, principalmente e-mails, redes sociais e apps financeiros.

• Não compartilhe dados sensíveis: bancos e instituições financeiras sérias NUNCA solicitam senhas completas, códigos de token, número do cartão de crédito com CVV ou dados de acesso por telefone, e-mail, SMS ou redes sociais. Se alguém pedir, é golpe.

• Cuidado ao compartilhar informações on-line: seja criterioso com as informações pessoais que você divulga em redes sociais ou outros sites. Dados como nome completo, CPF, endereço e telefone podem ser usados por fraudadores.

• Destrua documentos antigos: rasgue ou triture extratos bancários, faturas de cartão e outros documentos com informações pessoais antes de descartá-los.

Segurança de Dispositivos (Celular, Computador, Tablet)

• Mantenha sistemas operacionais e aplicativos atualizados: as atualizações frequentemente corrigem falhas de segurança que podem ser exploradas por criminosos.

• Utilize antivírus e firewall confiáveis: instale e mantenha atualizado um bom software antivírus em todos os seus dispositivos. Um firewall também ajuda a bloquear acessos não autorizados.

• Baixe aplicativos apenas de lojas oficiais: utilize a Google Play Store (Android) ou a App Store (iOS) e verifique as avaliações e permissões solicitadas pelo app antes de instalar.

• Cuidado com redes wi-fi públicas: evite realizar transações financeiras ou inserir dados sensíveis em redes wi-fi abertas e não seguras. Se precisar, utilize uma VPN (Rede Privada Virtual).

• Bloqueio de tela e PIN do chip: configure o bloqueio automático de tela com senha forte ou biometria. Ative também o PIN do seu chip (SIM Card) para impedir seu uso em outro aparelho.

• Não faça root ou jailbreak: esses procedimentos removem camadas de segurança importantes, tornando o dispositivo mais vulnerável.

Verifique a Autenticidade de Sites, Perfis e Empresas

• Confirme o endereço oficial (URL): antes de inserir dados em um site, verifique se a URL é a correta e se a conexão é segura (HTTPS, com o ícone de cadeado). Atenção a pequenas alterações no nome do domínio.

• Pesquise a reputação: antes de fazer negócios com uma empresa desconhecida ou realizar um investimento, pesquise sua reputação em sites como Reclame Aqui, Procon, e verifique se há notícias sobre fraudes envolvendo o nome da empresa.

• Verifique o CNPJ e autorizações: instituições financeiras e empresas de investimento legítimas devem ser registradas e autorizadas por órgãos como o Banco Central e a CVM. Consulte os sites desses órgãos.

• Desconfie de perfis em redes sociais: perfis falsos podem imitar empresas conhecidas. Verifique a data de criação do perfil, número de seguidores, qualidade das postagens e se há selo de verificação (embora este também possa ser falsificado).

Em Caso de Dúvida, Contate a Instituição por Canais Oficiais

• Regra de ouro: se você receber uma ligação, mensagem ou e-mail que pareça suspeito, mesmo que alegue ser do seu banco, não forneça informações e não siga as instruções imediatamente.

• Interrompa o contato suspeito: desligue a ligação, feche a mensagem ou o site.

• Procure os canais oficiais: localize o número de telefone do SAC, da central de atendimento ou do gerente da sua conta em um local seguro (verso do seu cartão, site oficial do banco acessado diretamente pelo navegador, aplicativo oficial).

• Relate o ocorrido: entre em contato com a instituição e pergunte se a comunicação que você recebeu é legítima.

• Nunca utilize contatos fornecidos na mensagem suspeita: não use os números de telefone ou links da comunicação suspeita para verificar sua autenticidade.

Lembre-se: manter a calma, desconfiar de promessas mirabolantes e verificar informações são suas melhores atitudes para evitar cair em golpes. A informação e a prevenção são suas maiores aliadas.

O Que Fazer em Caso de Fraude: Guia Prático

Ser vítima de fraude bancária é uma experiência que vai além do prejuízo financeiro, gerando estresse, insegurança e, muitas vezes, um sentimento de impotência. Saber como agir rapidamente após a descoberta de um golpe é crucial para minimizar os danos, aumentar as chances de recuperação dos valores e buscar a devida responsabilização.

Ações Imediatas ao Perceber a Fraude

A agilidade é sua maior aliada. Assim que identificar uma transação suspeita ou perceber que foi vítima de golpe, siga estes passos imediatamente:

1º Passo: Contate Imediatamente Sua Instituição Financeira (Banco de Origem da Transação)

• Canais de atendimento urgente: utilize os canais de emergência do seu banco (geralmente disponíveis 24h por dia, como SAC, central de fraudes ou chat no aplicativo). Informe o ocorrido de forma clara e objetiva.

• Solicite o bloqueio: peça o bloqueio imediato de cartões, senhas, acessos a aplicativos e, se for o caso, da conta.

• Conteste as transações: formalize a contestação de todas as transações não reconhecidas. Forneça o máximo de detalhes (data, hora, valor, para quem foi a transação, se souber).

• Acione o MED - Mecanismo Especial de Devolução para PIX: se a fraude envolveu transações PIX, solicite expressamente ao seu banco a abertura de um MED. Esse mecanismo, criado pelo Banco Central, permite que o banco de destino dos recursos bloqueie preventivamente os valores na conta do recebedor para análise, aumentando a chance de devolução. O MED deve ser solicitado em até 80 dias da data da transação PIX.

• Anote tudo: guarde números de protocolo, nomes dos atendentes, datas e horários das ligações. Se o contato for por chat ou e-mail, salve todas as conversas.

2º Passo: Contate a Instituição Financeira de Destino dos Valores (se souber e aplicável)

• Se você tiver informações sobre o banco e a conta para onde o dinheiro foi enviado (especialmente em golpes que não envolvem PIX ou quando o MED não é aplicável da mesma forma), entre em contato também com essa instituição.

• Informe que a conta deles recebeu valores de origem fraudulenta e solicite o bloqueio preventivo da conta e dos valores. Forneça o Boletim de Ocorrência (veja próximo passo) e os protocolos do seu banco.

3º Passo: Registre um Boletim de Ocorrência - BO

Imediatamente: dirija-se à delegacia de polícia mais próxima ou registre o BO on-line, se disponível em seu estado (em Mato Grosso, por exemplo, pelo site da Delegacia Virtual: www.delegaciavirtual.mt.gov.br).

• Detalhe os fatos: relate com o máximo de detalhes como o golpe ocorreu: datas, horários, valores, nomes (se houver), números de telefone, chaves PIX, sites falsos, prints de conversas, etc.

• Peça uma cópia: o BO é um documento fundamental para comprovar a fraude perante os bancos, órgãos de defesa do consumidor e, se necessário, na Justiça.

4º Passo: Reúna e Preserve Todas as Evidências

• Extratos bancários: salve ou imprima os extratos que mostram as transações fraudulentas.

• Comprovantes: guarde comprovantes de PIX, TEDs, pagamentos de boletos falsos etc.

• Comunicações com o golpista: salve prints de conversas no WhatsApp, e-mails, SMS, áudios, links de sites falsos, perfis de redes sociais etc. Não apague nada!

• Protocolos de atendimento: mantenha um registro de todos os contatos feitos com os bancos e outras instituições.

• Documentos falsos: se recebeu contratos ou documentos do golpista, guarde-os.

5º Passo: Notifique Órgãos de Proteção e Regulação

• Consumidor.gov.br: registre uma reclamação formal nesta plataforma oficial do Governo Federal. É um canal direto de comunicação com as empresas, incluindo bancos, e muitas vezes agiliza a resolução.

• Banco Central do Brasil - Bacen: registre uma reclamação contra as instituições financeiras envolvidas no canal do cidadão do Bacen (www.bcb.gov.br). O Bacen fiscaliza os bancos e pode aplicar sanções.

• Procon: procure o Procon do seu município ou estado para registrar a reclamação e buscar orientação.

Ferramentas Úteis do Banco Central: Registrato e MED

O Banco Central do Brasil - Bacen oferece ferramentas importantes para o cidadão proteger-se e buscar seus direitos:

• Registrato (Sistema de Informações Banco Central):

– O que é: plataforma gratuita pela qual você pode consultar diversas informações sobre sua vida financeira, como contas bancárias abertas em seu nome, empréstimos e financiamentos, chaves PIX cadastradas, e operações de câmbio.

– Como acessar: o acesso é feito com a conta Gov.br (nível prata ou ouro) ou diretamente pelo site do Bacen com certificado digital.

– Utilidade em fraudes: verificar se foram abertas contas desconhecidas em seu nome (usadas para fraudes), identificar chaves PIX que você não cadastrou, ou empréstimos não solicitados. Essa consulta regular é uma ótima medida preventiva.

– Site: www.bcb.gov.br/meubc/registrato

• MED - Mecanismo Especial de Devolução do PIX:
– O que é: conjunto de regras e procedimentos que permite a devolução de um PIX em casos de fundada suspeita de fraude ou falha operacional nos sistemas das instituições envolvidas. O MED possibilita o bloqueio dos recursos na conta do recebedor para análise.

– Como acionar: a vítima deve registrar Boletim de Ocorrência e contatar imediatamente seu banco (o banco de onde o PIX saiu), informando a fraude e solicitando a abertura do MED. É crucial agir rápido, preferencialmente nas primeiras horas após a transação.

– Prazo: a solicitação do MED pode ser feita em até 80 dias da data da transação PIX.

– Funcionamento: o banco da vítima comunica o banco do recebedor, que pode bloquear os valores na conta de destino. Após análise (que pode levar alguns dias), se a fraude for confirmada e houver saldo na conta do recebedor, o dinheiro pode ser devolvido total ou parcialmente.

– Importante: o MED não garante a devolução, pois depende da existência de saldo na conta do recebedor e da análise da fraude. Contudo, é o principal instrumento para tentar reaver valores de PIX fraudulentos.

Canais Oficiais de Denúncia e Auxílio Adicionais

Além dos canais já mencionados, existem outros locais onde você pode buscar ajuda e registrar denúncias:
• Polícia Civil: para registro do Boletim de Ocorrência e investigação criminal. Muitas delegacias possuem núcleos especializados em crimes cibernéticos.

• Ministério Público: em casos mais complexos ou que afetem um grande número de pessoas, o Ministério Público pode ser acionado.

• Defensoria Pública: se você não tem condições de pagar um advogado, a Defensoria Pública do seu estado pode oferecer assistência jurídica gratuita.

• OAB-Ordem dos Advogados do Brasil: muitas seccionais da OAB possuem comissões de Direito do Consumidor ou de Direito Bancário que podem oferecer orientação ou indicar advogados especializados.

• Plataformas de reputação: sites como o Reclame Aqui, embora não sejam canais oficiais de denúncia, servem para expor o problema e pressionar as empresas por uma solução, além de alertar outros consumidores, devendo, por outra via, o consumidor ter cautela com as informações ali apresentadas uma vez que são públicas, motivo pelo qual dados sensíveis não devem ser disponibilizados na reclamação.

Buscando o Ressarcimento

A coleta adequada de provas é fundamental para aumentar suas chances de ser ressarcido.

1. Via administrativa (bancos): após contestar a fraude e, se for o caso, acionar o MED, aguarde a análise do banco. Muitas vezes, se a falha na segurança do banco for evidente (conforme Súmula 479 do STJ), o ressarcimento é realizado administrativamente.

2. Consumidor.gov.br e Procon: se o banco negar o ressarcimento ou não responder, registre reclamações nessas plataformas. Elas podem mediar um acordo.

3. Via judicial: se as tentativas administrativas falharem, o próximo passo é buscar a Justiça. Um advogado de sua confiança poderá analisar seu caso e verificar a viabilidade de uma ação judicial pleiteando a devolução dos valores, indenização por danos morais e, eventualmente, danos materiais adicionais.

– Juizados especiais cíveis (pequenas causas): para causas de menor valor (geralmente até 40 salários mínimos), o processo é mais rápido e, para causas de até 20 salários mínimos, não é obrigatória a presença de advogado, embora seja sempre recomendável.

– Justiça comum: para causas de valor mais elevado ou mais complexas.

Lembre-se da Súmula 479 do STJ, que estabelece a responsabilidade objetiva das instituições financeiras por fraudes praticadas por terceiros no âmbito interno de operações bancárias. Todavia faz-se necessária a devida comprovação da existência de responsabilidade da instituição financeira e inexistência de responsabilidade/contribuição do consumidor, para o fato.

Quando procurar um advogado e como ele pode ajudar

Embora algumas etapas possam ser realizadas diretamente pelo consumidor, a assistência de um advogado especializado em Direito Bancário e do Consumidor pode ser crucial em diversas situações:

Quando procurar um advogado:

• Imediatamente após o golpe: para orientação sobre os primeiros passos, coleta de provas e comunicação com os bancos.
• Se o banco negar o ressarcimento ou a resposta for insatisfatória.
• Em casos de valores elevados ou contratação de empréstimos fraudulentos.
• Se houver negativação indevida do nome.
• Para entender a complexidade do caso e antes de assinar qualquer acordo com o banco.

Como um advogado pode ajudar:

- Análise do caso e orientação jurídica.
- Notificações extrajudiciais e negociação.
- Ação judicial e pedido de tutela de urgência.
- Cálculo de danos materiais e morais.

Procurar um advogado não é sinal de conflito, mas uma busca por orientação qualificada para defender seus direitos de forma eficaz.

Comissão de
Direito Bancário
MATO GROSSO