Anatomia da Fraude Digital no Brasil: Um Guia Abrangente de Proteção

Entenda os Golpes, o Modus Operandi e as Estratégias Essenciais de Defesa

CAO/MPMT
DEFESA DE DADOS PESSOAIS
E INTELIGÊNCIA ARTIFICIAL

MPMT
Ministério Público
DO ESTADO DE MATO GROSSO

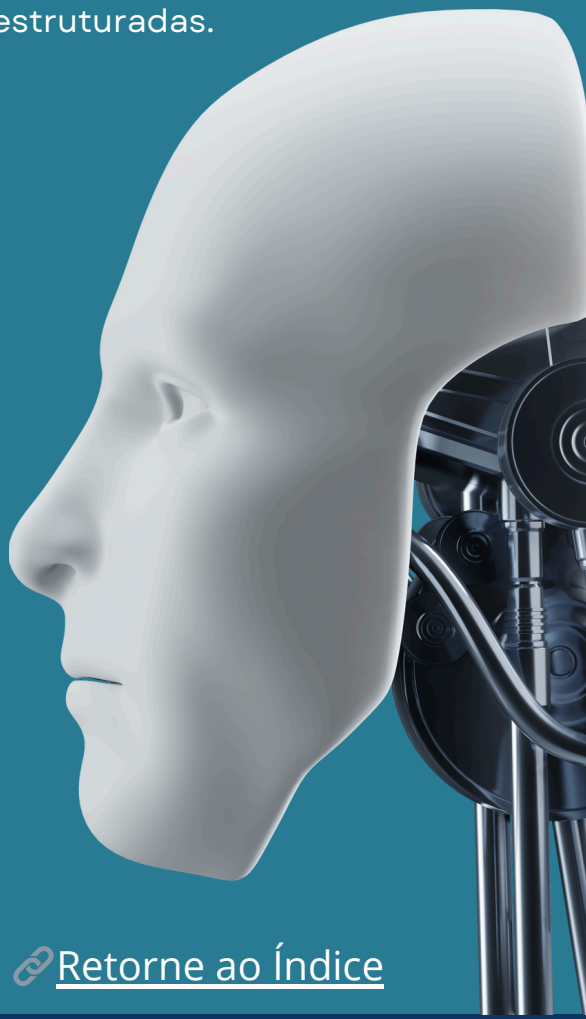
CSI/MPMT
Centro de Segurança
e Inteligência MPMT

O Ecossistema da Fraude Digital no Brasil

O Brasil enfrenta uma epidemia de fraudes digitais, um cenário que transcende incidentes isolados para se configurar como uma ameaça sistêmica à segurança financeira e psicológica da população. Dados recentes revelam uma escala alarmante: mais de 40,85 milhões de brasileiros foram vítimas de golpes online, com um em cada quatro cidadãos sofrendo ao menos uma tentativa de fraude.[1] O impacto financeiro é igualmente massivo, com perdas estimadas em R$ 297,7 bilhões apenas em 2024, segundo a Global Anti-Scam Alliance (GASA).[3]

Uma análise aprofundada indica que a distribuição desses crimes é notavelmente uniforme por todo o território nacional, sem um perfil demográfico ou geográfico claro para as vítimas.[4] Isso demonstra que a infraestrutura criminal digital é disseminada e capilarizada, capaz de alcançar qualquer pessoa, em qualquer lugar. Esta realidade é agravada pela migração do crime organizado para o ambiente digital. Organizações criminosas, em uma análise racional de risco e retorno, percebem que o investimento e o perigo associados a um golpe online são incomparavelmente menores do que os de um assalto a banco, por exemplo, tornando a fraude digital um "negócio" mais seguro e escalável.[2] O resultado é uma "democratização" da fraude, que deixou de ser um ato de hackers isolados para se tornar uma indústria operada por quadrilhas estruturadas.

O pilar que sustenta quase a totalidade dessas fraudes não é uma falha tecnológica complexa, mas sim a Engenharia Social: a arte de manipular psicologicamente as pessoas para que elas realizem ações contra seus próprios interesses.[5] Os criminosos exploram emoções humanas universais como confiança, medo, ganância e um senso de urgência para contornar as defesas lógicas da vítima.[8] A sofisticação desses ataques está em constante evolução, migrando de abordagens massificadas, como e-mails de phishing genéricos, para ataques altamente personalizados (conhecidos como spear phishing) e o uso de tecnologias emergentes, como Inteligência Artificial, para simular com perfeição a voz e até a imagem de pessoas conhecidas (deepfakes), tornando as fraudes cada vez mais críveis e difíceis de detectar.[2]



Retorne ao Índice

Índice com Links

Golpes de Impersonificação e Abuso de Confiança

Os golpes mais eficazes são aqueles que se apropriam de uma identidade confiável para enganar a vítima. Ao se passarem por instituições ou pessoas familiares, os criminosos criam uma fachada de legitimidade que desarma as defesas do alvo. Essa tática, no entanto, gera um efeito colateral perigoso: a erosão da confiança pública. Cada vez que um golpista usa o nome de um banco ou de um órgão governamental, ele não apenas lesa a vítima, mas também desgasta a credibilidade da instituição. Isso pode levar a uma paralisia do usuário, que, de tão cético, passa a ignorar comunicações legítimas, tratando-as como spam e atrasando a resposta a um incidente real.

O Golpe da Falsa Central de Atendimento / Falso Funcionário

Este é um dos golpes mais comuns e perigosos, frequentemente relatado por instituições financeiras.[5] O modus operandi começa com uma ligação ou mensagem na qual o criminoso se identifica como funcionário do banco da vítima. Utilizando um discurso alarmista, ele informa sobre uma suposta transação suspeita, uma tentativa de invasão na conta ou a necessidade de uma atualização cadastral urgente.[11] Para "ajudar" a vítima a resolver o problema, ele solicita informações confidenciais, como senhas, tokens ou o código de segurança do cartão. Em uma abordagem mais agressiva, ele instrui a vítima a realizar uma transferência, geralmente via PIX, para uma suposta "conta segura" que pertenceria ao banco, a fim de proteger os fundos.[10]

Uma variação ainda mais sofisticada envolve o golpista alegar que o gerente da agência da vítima ou a própria agência estão sob investigação policial. Para aumentar a credibilidade, ele pode até enviar um Boletim de Ocorrência falso por mensagem. Em seguida, ele convence a vítima de que, para proteger seu dinheiro durante a "investigação", ela deve transferir todos os seus recursos para contas indicadas por ele.[12]

Prevenção: A principal defesa é a desconfiança. Desligue imediatamente a chamada. Lembre-se que bancos e instituições financeiras legítimas nunca solicitam senhas, códigos de segurança, instalação de aplicativos ou a realização de transferências por telefone.[10] Para verificar a veracidade de qualquer contato, procure o número de telefone oficial do seu banco (geralmente no verso do cartão) e faça você mesmo a ligação a partir de uma linha segura.

Retorne ao Índice

O Golpe do Falso Parente (WhatsApp)

Nesta fraude, o apelo emocional é a principal arma. O golpista obtém a foto de perfil da vítima em redes sociais e, utilizando um número de telefone desconhecido, entra em contato com amigos e familiares se passando pela pessoa.[14] A história é quase sempre a mesma: uma emergência súbita acompanhada da alegação de ter trocado de número. Frases como "Oi, tia! Troquei de número, anota aí. Estou com um problema e preciso pagar uma conta urgente, você pode me fazer um PIX? Te devolvo amanhã" são comuns.[16] A combinação da foto familiar com o senso de urgência e o apelo a um laço afetivo leva muitas pessoas a agirem por impulso, sem realizar a devida verificação.

Prevenção: Desconfie sempre de pedidos de dinheiro recebidos por mensagem, mesmo que o remetente pareça ser alguém de confiança. A melhor forma de confirmar a identidade é fazendo uma ligação de voz ou vídeo para o número antigo da pessoa, ou contatando-a por outro meio de comunicação que você saiba ser legítimo.[14]

O Golpe do Falso Suporte Técnico

Este golpe é frequentemente o precursor de ataques mais devastadores, como o da "**Mão Fantasma**". A vítima se depara com uma mensagem de alerta em seu computador, geralmente um pop-up alarmista, ou recebe um e-mail ou ligação informando que seu dispositivo está infectado com um vírus perigoso ou apresentando falhas críticas de segurança.[17] O falso técnico, com um discurso convincente, oferece uma solução imediata. Para isso, ele instrui a vítima a instalar um software de acesso remoto, sob o pretexto de que precisa se conectar ao dispositivo para "fazer uma limpeza" ou "corrigir o problema". Uma vez instalado, esse software dá ao golpista controle total e irrestrito sobre o computador ou celular da vítima.

Prevenção: Jamais instale softwares ou conceda acesso remoto a pedido de alguém que entrou em contato com você de forma não solicitada. Empresas como Microsoft, Google ou Apple não monitoram proativamente seus dispositivos em busca de vírus para então ligar para você. Se um pop-up travar sua tela, reinicie o computador.

Retorne ao Índice

O Golpe do Falso Advogado

Nesta fraude, o conhecimento jurídico e a falsa autoridade são as principais armas. O golpista se passa por advogado ou funcionário de um escritório, utilizando nomes reais de profissionais, registros da OAB e até dados de processos em andamento para convencer a vítima. O contato geralmente é feito por telefone ou aplicativos de mensagem, com perfis falsos, documentos adulterados (como sentenças, ofícios ou cálculos) e um discurso persuasivo de que há valores a receber em precatórios, RPVs ou indenizações. A história quase sempre inclui a exigência de pagamento imediato de supostas taxas – como "desbloqueio", "emolumentos finais" ou "despesas cartorárias" –, sob a ameaça de que, sem isso, o valor seria perdido ou retornaria ao Estado.[76]

Prevenção: Desconfie sempre de contatos que cobram valores antecipados para liberar créditos judiciais. Antes de qualquer pagamento, confirme a informação diretamente com o advogado constituído, consulte os canais oficiais da OAB e verifique os sistemas processuais. Nunca realize transferências por PIX ou depósito sem confirmar a legitimidade da cobrança. Em caso de dúvida, interrompa o contato e procure orientação oficial.[76]

O Golpe da Falsa Encomenda (Correios, Mercado Livre ou Amazon)

Nesta fraude, a expectativa pela entrega de uma encomenda é a principal arma. O golpista envia mensagens falsas por SMS, e-mail ou aplicativos, informando que o pacote está retido nos Correios ou na alfândega e que é necessário pagar uma taxa para liberação.[77] Essas mensagens usam logotipos oficiais e linguagem semelhante à dos Correios, direcionando a vítima para sites falsos que imitam o oficial. Lá, é solicitado o fornecimento de dados pessoais e financeiros, ou até mesmo o pagamento de um boleto ou Pix. A vítima, ansiosa para liberar sua compra, acaba fornecendo informações sensíveis ou realizando pagamentos que nunca têm retorno.

Um desdobramento comum é o Golpe da Falsa Encomenda em marketplaces, como Mercado Livre ou Amazon. Nesse caso, criminosos se passam por representantes das plataformas e enviam mensagens com supostas cobranças de taxas ou atualizações de entrega. Muitas vezes, eles possuem informações reais das vítimas – como CPF, endereço e até detalhes de pedidos – obtidos por vazamento de dados, o que torna o golpe ainda mais convincente.

Prevenção: Desconfie de mensagens inesperadas que pedem pagamento antecipado ou solicitam dados pessoais. Nunca clique em links recebidos por SMS, e-mail ou aplicativos de mensagens. Acompanhe suas compras apenas pelos aplicativos ou sites oficiais das plataformas (Correios, Mercado Livre, Amazon etc.). Verifique sempre o remetente e desconfie de cobranças urgentes. Em caso de dúvida, entre em contato pelos canais oficiais e jamais realize pagamentos por Pix ou boleto sem confirmação.

Retorne ao Índice

A Falsa Intimação de Órgãos Públicos

Aproveitando-se do respeito e do temor que instituições como a Polícia Federal (PF) e a Receita Federal inspiram, criminosos enviam e-mails e mensagens fraudulentas em nome desses órgãos.[19] As iscas são variadas: uma suposta intimação para depor, um alerta de que a vítima navegou em "sites clandestinos" e que um inquérito policial foi aberto, ou uma notificação sobre irregularidades no CPF ou na declaração do Imposto de Renda.[19] A mensagem sempre contém um link ou anexo para que a vítima possa "regularizar sua situação" ou "visualizar a intimação". Clicar no link leva a páginas de phishing para roubo de dados ou à instalação de malware.

Prevenção: É fundamental saber que órgãos governamentais não comunicam intimações, pendências fiscais graves ou aberturas de inquérito por meio de e-mails genéricos, SMS ou WhatsApp.[19] A comunicação oficial ocorre por canais seguros e estabelecidos, como o portal e-CAC da Receita Federal, ou por correspondência oficial com aviso de recebimento. Em caso de dúvida, nunca clique no link. Acesse o site oficial do órgão digitando o endereço diretamente no seu navegador e verifique sua situação por lá.

Fraudes em Plataformas de Comunicação: A Arma no seu Bolso

As ferramentas que usamos para nos conectar com o mundo – aplicativos de mensagens e e-mail – tornaram-se os principais campos de batalha da segurança digital. A própria natureza dessas plataformas, projetadas para serem rápidas, intuitivas e de baixa fricção, é explorada pelos criminosos. O design de uma boa interface de usuário (UI) visa reduzir a carga cognitiva, tornando ações como clicar e responder quase automáticas.[7] Os golpistas se aproveitam dessa "economia de pensamento", criando mensagens que se encaixam no fluxo normal de interação e exploram a tendência humana de agir rapidamente, sem uma análise crítica aprofundada. A conveniência que torna um aplicativo útil é, paradoxalmente, a vulnerabilidade que o torna um vetor de ataque eficaz.

Retorne ao Índice

Phishing e Smishing: A Pescaria Digital Onipresente

O phishing (fraude por e-mail) e o smishing (fraude por SMS) são as táticas mais difundidas para o roubo de informações pessoais e financeiras.[9] O golpe consiste no envio de uma mensagem que imita a comunicação de uma entidade legítima – um banco, uma loja de varejo, um serviço de streaming, uma empresa de logística. A mensagem geralmente contém um senso de urgência ou uma oferta tentadora, e instrui o destinatário a clicar em um link para "atualizar o cadastro", "rastrear um pedido" ou "aproveitar uma promoção".[10]
Esse link, no entanto, direciona a vítima para uma página da web fraudulenta, que é uma cópia visualmente idêntica do site original. Desavisada, a vítima insere suas credenciais de login (usuário e senha) ou dados de cartão de crédito, que são imediatamente capturados pelos criminosos.

Prevenção: A regra fundamental é nunca clicar em links recebidos em e-mails ou mensagens não solicitadas.[18] Antes de qualquer ação, verifique cuidadosamente o endereço de e-mail do remetente e o endereço do site (URL) para o qual o link aponta, procurando por erros de digitação ou domínios estranhos. A prática mais segura é sempre digitar o endereço do site oficial diretamente na barra do navegador, em vez de usar links.[21] Manter o sistema operacional e o software antivírus atualizados também é crucial para bloquear ameaças conhecidas.[10]

Clonagem e Sequestro de Contas de WhatsApp

Considerado o golpe mais relatado aos bancos em 2024, segundo a FEBRABAN, o sequestro de contas do WhatsApp é devastador por usar a rede de contatos da vítima como alvo secundário.[10] O processo geralmente começa quando o criminoso obtém o número de telefone da vítima, muitas vezes a partir de anúncios em sites de compra e venda onde o número fica exposto.[24]

O golpista então tenta registrar a conta do WhatsApp da vítima em seu próprio dispositivo. O aplicativo, como medida de segurança, envia um código de verificação de 6 dígitos via SMS para o número original. Neste ponto, a engenharia social entra em ação: o criminoso liga ou envia uma mensagem para a vítima, se passando por um funcionário do site de anúncios, de uma empresa ou até mesmo do Ministério da Saúde (com pretextos de pesquisa sobre vacinas), e a engana para que ela forneça o código recebido por SMS, alegando ser um "protocolo de confirmação" ou "código de ativação".[11] Com esse código em mãos, o criminoso assume o controle total da conta, bloqueando o acesso do verdadeiro dono.[15] A partir daí, ele se passa pela vítima e começa a pedir dinheiro emprestado a amigos e familiares, que, acreditando na emergência, realizam transferências para os golpistas.

Retorne ao Índice

Prevenção: A medida de proteção mais eficaz e indispensável é ativar a "verificação em duas etapas" (também conhecida como PIN) nas configurações de segurança do WhatsApp. Isso cria uma senha pessoal de 6 dígitos que será solicitada periodicamente e sempre que a conta for registrada em um novo aparelho.[11] Essa senha é sua segunda linha de defesa. E, claro, nunca, sob nenhuma circunstância, compartilhe o código de verificação recebido por SMS com ninguém.

O Golpe da Tarefa / Renda Extra Fácil

Esta fraude explora o desejo por uma fonte de renda rápida e com pouco esforço. A vítima recebe uma mensagem, geralmente via WhatsApp ou Telegram, de alguém que se apresenta como recrutador ou gerente de marketing de uma grande empresa.[26] A proposta é tentadora: ganhar dinheiro realizando tarefas simples, como curtir vídeos no TikTok, seguir perfis no Instagram, ou escrever avaliações positivas para produtos e hotéis.[25]
Para ganhar a confiança da vítima, os golpistas podem, inicialmente, pagar pequenas quantias (R$ 10, R$ 20) pelas primeiras tarefas. Uma vez que a vítima está engajada e confiante, o golpe avança. Os criminosos então propõem que, para ter acesso a um "pacote de tarefas premium" com remuneração muito maior, a vítima precisa "investir" um valor ou pagar uma "taxa de adesão".[11] Após a vítima realizar o pagamento, os golpistas cortam toda a comunicação e desaparecem com o dinheiro.

Prevenção: Desconfie radicalmente de qualquer oferta de trabalho que prometa dinheiro fácil e rápido com pouco ou nenhum esforço.[26] Empresas sérias não conduzem processos seletivos inteiramente por aplicativos de mensagens e, fundamentalmente, nunca cobram taxas para que alguém possa trabalhar para elas. Antes de se engajar, pesquise a reputação da suposta empresa e do recrutador em canais oficiais.

O Dinheiro como Alvo: Golpes Financeiros e de Pagamento

Os golpes financeiros evoluíram para explorar as vulnerabilidades de cada sistema de pagamento, desde o tradicional boleto até o instantâneo PIX. A inovação tecnológica, quando não acompanhada por uma educação massiva do usuário, cria um vácuo de risco. O PIX é o exemplo perfeito desse paradoxo: suas características revolucionárias – instantaneidade, disponibilidade 24/7 e facilidade de uso – são precisamente as que o tornam a ferramenta ideal para fraudes.[18] A velocidade da transação elimina a janela de tempo para arrependimento ou intervenção que existia em sistemas mais antigos, e sua irreversibilidade torna o erro da vítima financeiramente fatal.[28] Mecanismos como o MED (Mecanismo Especial de Devolução) são reativos, não preventivos, e seu sucesso depende da ação imediata da vítima e da disponibilidade de fundos na conta do golpista.[29]

Retorne ao Índice

O Boleto Bancário Adulterado

Nesta fraude clássica, criminosos criam ou alteram boletos bancários para desviar o pagamento para suas próprias contas.[18] Existem duas formas principais de execução. A primeira é o envio de um boleto falso por e-mail ou WhatsApp, muitas vezes se passando por uma renegociação de dívida ou uma segunda via com desconto de uma conta de consumo (luz, água, condomínio). A segunda, mais sofisticada, envolve a infecção do computador da vítima com um tipo de malware conhecido como "bolware". Esse vírus age silenciosamente, detectando quando o usuário copia a linha digitável de um boleto legítimo e a substituindo, na área de transferência, pela linha digitável do boleto do golpista. O layout do documento parece perfeito, mas os dados do beneficiário são fraudulentos.[24]

Prevenção: O momento do pagamento é a última linha de defesa. Antes de confirmar qualquer transação, confira com máxima atenção os dados do beneficiário (nome, CPF ou CNPJ) que aparecem na tela de confirmação do seu banco ou aplicativo de pagamento. Compare-os com os dados do emissor original da cobrança. Se houver qualquer divergência, não conclua a operação e entre em contato com a empresa credora por seus canais oficiais.[11]

O Ecossistema de Golpes com PIX

A instantaneidade do PIX abriu um leque de novas modalidades de fraude.[18]

- **PIX Reverso / Falso Comprovante:** O golpista envia à vítima um comprovante de transferência PIX forjado e, em seguida, entra em contato alegando ter feito o envio por engano, solicitando a "devolução" do valor.[1] Em uma variação mais complexa, o criminoso pode fazer um depósito real e, imediatamente, acionar o MED junto ao seu banco para reaver o dinheiro. Ao mesmo tempo, ele pressiona a vítima para que ela também "devolva" o valor, tentando assim receber o dinheiro em dobro.[29]
- **Robô do PIX:** Anúncios fraudulentos em redes sociais promovem um suposto "robô" ou "sistema de investimento" que promete multiplicar o dinheiro enviado via PIX. A promessa é simples e absurda: "envie um PIX de R$ 200 e receba R$ 2.000 de volta em minutos".[30] A vítima, atraída pela ganância, faz a transferência e, obviamente, perde o valor integral.[28]

Prevenção: Nunca devolva um PIX supostamente recebido por engano sem antes verificar seu extrato bancário para confirmar se o crédito realmente entrou em sua conta.[29] Se o valor estiver lá, utilize a função "Devolver PIX" do seu aplicativo, que garante que o dinheiro retorne para a conta de origem. Ignore completamente qualquer promessa de multiplicação de dinheiro; isso não existe. Lembre-se que uma transação PIX, uma vez confirmada, não pode ser cancelada.[28]

Retorne ao Índice

O Golpe do Falso Investimento e Pirâmides Financeiras

Criminosos criam sites e perfis em redes sociais de falsas corretoras de investimento, com aparência profissional e sofisticada. Eles prometem retornos altíssimos, rápidos e garantidos, frequentemente usando criptomoedas como isca.[8] Para construir credibilidade, utilizam depoimentos falsos de supostos clientes satisfeitos e pressionam a vítima a investir rapidamente, sob o pretexto de uma "oportunidade única" que está prestes a se encerrar.[10]

Prevenção: Desconfie de qualquer promessa de lucro muito acima da média do mercado e sem riscos.[10] Antes de investir, verifique se a instituição é devidamente autorizada a operar pela Comissão de Valores Mobiliários (CVM) e pesquise sua reputação. Não ceda à pressão para tomar decisões financeiras apressadas.

O Golpe do Falso Empréstimo (Consignado e Pessoal)

Mirando principalmente em pessoas com restrições de crédito, golpistas publicam anúncios em redes sociais ou enviam mensagens de WhatsApp oferecendo crédito fácil, rápido e sem consulta ao SPC/Serasa.[24] Após a vítima demonstrar interesse, os criminosos informam que, para a liberação do valor, é necessário o pagamento de uma "taxa antecipada". As justificativas são variadas: "taxa de cartório", "seguro-fiança", "IOF antecipado". Uma vez que a vítima paga essa taxa, os golpistas desaparecem.[34]

Prevenção: Instituições financeiras sérias e regulamentadas NUNCA cobram valores antecipados para liberar um empréstimo. Todos os custos e taxas da operação são diluídos no valor das parcelas.

O Golpe da Devolução de Empréstimo

Esta é uma fraude particularmente engenhosa. O golpista, já de posse de dados pessoais da vítima (obtidos em vazamentos), contrata um empréstimo legítimo em nome dela em uma instituição financeira. O dinheiro é creditado na conta da própria vítima. Em seguida, o criminoso liga para ela, se passando por um funcionário do banco, e a informa sobre o empréstimo "fraudulento" que foi contratado em seu nome. Para "cancelar a operação", ele instrui a vítima a transferir o valor total recebido para uma chave PIX ou pagar um boleto fornecido por ele. A vítima, acreditando estar resolvendo o problema, transfere o dinheiro para o golpista. No final, ela fica com a dívida do empréstimo e sem o dinheiro.[11]

Prevenção: Se um crédito inesperado aparecer em sua conta, não tome nenhuma atitude precipitada. Entre em contato com seu banco pelos canais oficiais para se informar sobre a origem do valor. Jamais transfira dinheiro para contas de terceiros a pedido de supostos funcionários para "cancelar" uma operação.

🔗Retorne ao Índice

Armadilhas no Comércio e em Serviços Digitais

O ambiente online de compras e serviços cria uma assimetria de informação fundamental: o fraudador constrói uma realidade fabricada – um site perfeito, um anúncio atraente, fotos profissionais – e a vítima precisa despender um esforço significativo para desmenti-la, muitas vezes sem as ferramentas adequadas para verificação à distância.[35] Esses golpes exploram a "intenção positiva" do usuário, que está emocionalmente investido em uma compra, no planejamento de uma viagem ou na busca por um bom negócio. Essa excitação diminui o ceticismo e a vigilância, tornando a própria expectativa da vítima uma arma contra ela.

Lojas Virtuais e Vendas Falsas em Redes Sociais

Criminosos desenvolvem sites de e-commerce falsos que são clones quase perfeitos de lojas famosas e conhecidas, mas hospedados em endereços de internet (URLs) ligeiramente diferentes – por exemplo, trocando uma letra "o" pelo número "0" ou adicionando um termo extra ao domínio.[9] Eles também investem pesado em anúncios patrocinados em redes sociais como Instagram e Facebook, criando perfis de lojas com ofertas irresistíveis e utilizando depoimentos falsos para construir uma reputação artificial.[11] A vítima realiza a compra, efetua o pagamento e o produto nunca é entregue.

Prevenção: Desconfie sempre de preços muito abaixo da média de mercado; ofertas que parecem boas demais para ser verdade geralmente são fraudes.[37] Verifique a reputação da loja em sites de avaliação de consumidores, como o Reclame Aqui. Antes de inserir qualquer dado, confira se o endereço do site começa com https:// e exibe um ícone de cadeado na barra do navegador, o que indica uma conexão segura.[21] Para uma camada extra de segurança, utilize sempre um cartão de crédito virtual para compras online, pois ele pode ser bloqueado ou excluído após a transação.[21]

O Golpe do Falso Leilão Online

Esta fraude visa subtrair grandes quantias de dinheiro de uma só vez. Golpistas criam sites falsos que simulam leilões de veículos, imóveis e outros bens de alto valor, com lances iniciais e preços de arremate muito abaixo do praticado no mercado.[40] Os sites são extremamente convincentes, utilizando layouts profissionais e, em alguns casos, se apropriando indevidamente de logotipos de órgãos oficiais, como Tribunais de Justiça, ou exibindo selos de segurança falsificados para transmitir confiança.[43] A vítima participa, dá o lance, é informada de que "arrematou" o bem e recebe instruções para efetuar o pagamento antecipado, geralmente via PIX ou transferência para a conta de uma pessoa física. Após o pagamento, os criminosos desaparecem e o site é desativado.[42]

Retorne ao Índice

Prevenção: Verifique se o leiloeiro é oficial e devidamente registrado na Junta Comercial do seu estado. Desconfie sempre que o pagamento for solicitado para a conta de uma pessoa física e não para a pessoa jurídica da empresa leiloeira.[41] Se possível, tente visitar o pátio para inspecionar o bem pessoalmente antes de dar qualquer lance. Fique atento ao domínio do site: leilões legítimos no Brasil geralmente usam o final .com.br. Desconfie de domínios que terminam em .org, .net ou que usam artifícios como /br no final.[41]

O Golpe do Delivery

Essa fraude ocorre no momento da entrega do pedido e possui duas variações principais:

- **Maquininha com Visor Quebrado:** O entregador, que é o golpista, chega com uma maquininha de cartão cujo visor está danificado (rachado, arranhado ou com a tela escura), o que impede a visualização clara do valor digitado.[46] Ele digita um valor muito superior ao do pedido (por exemplo, R$ 250,00 em vez de R$ 25,00). A vítima, sem conseguir conferir, insere a senha e aprova a transação fraudulenta.[48]
- **Taxa Extra Falsa:** Após a vítima realizar o pedido pelo aplicativo, ela recebe uma ligação de alguém que se passa por funcionário do restaurante. O golpista alega que houve um erro e que uma "taxa de entrega" não foi incluída, precisando ser paga separadamente. Ele então solicita os dados completos do cartão de crédito por telefone para realizar a cobrança, utilizando as informações para clonar o cartão e fazer compras indevidas.[49]

Prevenção: Jamais aceite pagar por um pedido em uma maquininha com o visor danificado. Exija ver o valor claramente antes de inserir sua senha. Nunca forneça os dados do seu cartão de crédito por telefone. Os pagamentos devem ser feitos diretamente no aplicativo ou na entrega, com você manuseando o seu cartão.

O Golpe do Aluguel de Temporada

Com a popularidade das viagens, essa fraude se tornou comum. Criminosos criam anúncios falsos de imóveis para aluguel de temporada em sites de classificados, grupos de Facebook ou WhatsApp, utilizando fotos e descrições copiadas de anúncios legítimos.[51] Eles oferecem diárias com preços muito atrativos para gerar um senso de urgência e pressionam a vítima a fazer um depósito de "sinal" ou o pagamento integral adiantado para "garantir a reserva". Ao chegar ao destino de férias, a família descobre que o imóvel não existe, não está disponível para locação ou, pior, que pertence a outra pessoa que não faz ideia do golpe.[35]

Prevenção: Dê preferência a plataformas de aluguel seguras e conhecidas (como Airbnb e Booking.com), que intermediam o pagamento e só liberam o dinheiro para o anfitrião após o início da estadia, além de possuírem um sistema de avaliação de outros hóspedes.[38] Desconfie de preços muito abaixo do mercado.[38] Antes de fechar negócio, peça ao suposto proprietário para fazer uma chamada de vídeo e mostrar o imóvel ao vivo.[52] Exija sempre um contrato de locação detalhado e desconfie se o locador pressionar por um pagamento rápido e informal.[53]

Retorne ao Índice

Ataques Híbridos: Combinando Tecnologia e Manipulação

A fronteira entre o mundo digital e o físico está cada vez mais tênue, e os criminosos são mestres em explorar essa fusão. Os ataques híbridos representam a vanguarda da fraude, combinando a obtenção de dados online com interações presenciais, ou vice-versa. Ao introduzir um elemento físico – um entregador na porta, uma "ajuda" no caixa eletrônico – o golpista ancora a fraude na realidade tangível, o que pode diminuir as defesas da vítima, pois a presença humana pode parecer mais legítima que uma mensagem anônima. O roubo de biometria facial é o exemplo mais claro dessa fusão, onde um ato físico (tirar uma foto) é diretamente traduzido em uma ação digital de alto valor (autenticação de identidade).[54] A segurança pessoal, portanto, não pode mais ser compartimentada entre "online" e "offline".

O Golpe da Mão Fantasma (Acesso Remoto)

Este é um dos golpes mais sofisticados e assustadores em circulação. Ele se inicia com uma tática de engenharia social: a vítima recebe uma ligação de um falso funcionário do banco.[55] Com um discurso alarmista, o golpista informa que a conta da vítima foi invadida ou que transações suspeitas foram detectadas. Para "resolver o problema" e "proteger a conta", ele convence a vítima a instalar um aplicativo em seu celular, que supostamente seria um "módulo de segurança" do banco. Na realidade, este aplicativo é um software de acesso remoto legítimo, usado de forma maliciosa.[57]
Uma vez que a vítima instala o app e concede as permissões, o criminoso obtém controle total e irrestrito do aparelho. É como se uma "mão fantasma" estivesse operando o celular à distância.[13] O golpista então acessa os aplicativos bancários, visualiza saldos, e realiza transferências, pagamentos e até a contratação de empréstimos em tempo real, muitas vezes enquanto a vítima assiste impotente, sem conseguir intervir.

Prevenção: A regra de ouro é absoluta: bancos, instituições financeiras ou qualquer empresa legítima NUNCA solicitarão que você instale qualquer tipo de aplicativo ou software de acesso remoto em seu celular ou computador para fins de segurança.[13] Se receber uma ligação com essa solicitação, desligue imediatamente

Retorne ao Índice

O Golpe do Falso Presente

Esta é uma evolução perigosa do golpe do delivery, que explora a surpresa e a emoção positiva. Um falso entregador aparece na residência da vítima, geralmente em uma data especial como seu aniversário (o que indica que os golpistas tiveram acesso a dados pessoais vazados), com um presente inesperado, como flores ou chocolates.[54] A partir daí, o golpe se desdobra em duas variações principais:

- **Cobrança de Frete:** O entregador informa que, embora o presente seja uma cortesia, há uma pequena taxa de frete a ser paga. Ele apresenta uma maquininha de cartão adulterada e, no momento do pagamento, clona os dados do cartão da vítima ou digita um valor exorbitante.[61]
- **Roubo de Biometria Facial:** Esta é a versão mais alarmante. O entregador insiste que, para "confirmar a entrega" e cumprir o "protocolo da empresa", ele precisa tirar uma foto do rosto da vítima segurando o presente. Essa fotografia de alta qualidade é, na verdade, o que os criminosos precisam para realizar a prova de vida (reconhecimento facial) exigida por muitos bancos digitais e fintechs para abrir contas ou contratar empréstimos em nome da vítima.[54]

Prevenção: Desconfie de qualquer presente ou entrega inesperada que exija o pagamento de taxas, por menores que sejam.[63] Jamais permita que um entregador tire uma foto do seu rosto sob qualquer pretexto.[54] É aconselhável instruir porteiros de condomínios a não aceitarem entregas que exijam pagamento ou registro fotográfico do morador.

O Golpe da Troca de Cartão

Este é um golpe físico, mas que frequentemente se apoia em uma transação digital. Acontece em estabelecimentos comerciais, postos de gasolina ou em caixas eletrônicos. O golpista, agindo como um vendedor ou um "bom samaritano", observa a vítima digitar sua senha.[11] Em um momento de distração, ao devolver o cartão ou sob o pretexto de "ajudar" com a maquininha, ele realiza a troca do cartão da vítima por um outro muito similar, mas que pertence a outra pessoa ou é inválido. De posse do cartão verdadeiro e da senha memorizada, o criminoso pode realizar saques e compras até que a vítima perceba a troca.[10]

Prevenção: Nunca perca seu cartão de vista durante uma transação. Ao digitar a senha, proteja o teclado com a outra mão ou com o corpo. E, o mais importante: sempre confira se o cartão que lhe foi devolvido é, de fato, o seu.[10]

Retorne ao Índice

A Exploração das Emoções e Oportunidades

Alguns dos golpes mais devastadores não exploram falhas em softwares ou sistemas, mas sim vulnerabilidades inerentes ao "sistema operacional humano". Eles são projetados para hackear emoções fundamentais: a solidão e o desejo por conexão, a ambição e a necessidade de trabalho, ou o medo e a vergonha. Os golpistas são, em essência, hackers sociais que utilizam roteiros de manipulação em vez de código malicioso. O sucesso dessas fraudes demonstra que a vulnerabilidade mais explorada no ciberespaço não é um sistema operacional, mas a própria psique humana.

O Golpe do Amor (Romance Scam)

Nesta fraude de longo prazo, o golpista cria um perfil falso e atraente em redes sociais ou aplicativos de namoro.[8] Ele inicia um relacionamento online com a vítima, investindo semanas ou até meses para construir um laço emocional profundo e uma relação de confiança absoluta. A comunicação é intensa, com promessas de um futuro juntos. Uma vez que a vítima está completamente envolvida emocionalmente, o golpista inventa uma emergência súbita e dramática: um problema grave de saúde, uma dificuldade financeira que o impede de viajar para encontrar a vítima, uma oportunidade de negócio imperdível que requer um investimento inicial. Movida pelo amor e pela confiança, a vítima é manipulada a enviar dinheiro, muitas vezes em múltiplas transferências, até que suas economias se esgotem.[8]

Prevenção: Seja cético em relação a relacionamentos online que evoluem de forma extremamente rápida e intensa. Desconfie se a pessoa sempre tem uma desculpa para não participar de chamadas de vídeo ou para nunca se encontrar pessoalmente. A regra fundamental é: nunca envie dinheiro ou informações financeiras para alguém que você não conhece pessoalmente, não importa quão convincente seja a história.

O Golpe do Falso Emprego

Anúncios de vagas de emprego que parecem boas demais para ser verdade são a isca principal. Promessas de salários elevados, trabalho 100% remoto, flexibilidade total e poucas exigências de qualificação são publicadas em portais de emprego e redes sociais.[8] Quando a vítima se candidata, o falso recrutador a conduz por um processo seletivo fraudulento. O objetivo é duplo: ou roubar dados pessoais e bancários, solicitando que a vítima preencha um "formulário de cadastro" extenso, ou extorquir dinheiro, exigindo o pagamento de taxas para um "curso de qualificação obrigatório", "exame admissional" ou "compra de uniforme", que nunca existem.[24]

🔗Retorne ao Índice

Prevenção: Empresas sérias e legítimas não cobram nenhuma taxa dos candidatos durante um processo seletivo. Pesquise a reputação da empresa e a veracidade da vaga em seus canais oficiais (como o site da empresa ou o perfil no LinkedIn). Desconfie de processos seletivos conduzidos inteiramente por aplicativos de mensagens como WhatsApp ou Telegram.Sextorsão: A Extorsão por Fotos Íntimas

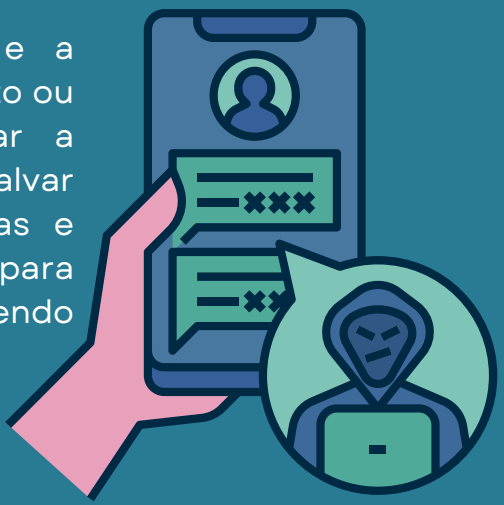
O Golpe da Falsa Facção Criminosa

Nesta modalidade de extorsão, os criminosos exploram o medo e a intimidação para coagir as vítimas a realizarem pagamentos. O golpe se aproveita da reputação de violência de organizações criminosas reais para criar uma ameaça crível e aterrorizante.

O modus operandi geralmente começa com a coleta de informações pessoais da vítima em fontes abertas, como redes sociais. De posse de dados como nome completo e endereço, o golpista entra em contato por ligação ou mensagem de texto. Ele se apresenta como membro de uma facção criminosa atuante na região e, para gerar pânico, acusa a vítima de ser informante da polícia ou de ter "infringido" alguma regra imposta pelo grupo. A ameaça é direta e grave, envolvendo violência contra a vítima e seus familiares. Para evitar as supostas "consequências", é exigido um pagamento imediato, geralmente via PIX.

Uma variação comum tem como alvo comerciantes locais. Nesse caso, os criminosos cobram uma "taxa de proteção" para que o estabelecimento não seja alvo de furtos, roubos ou outros atos de violência, coagindo o proprietário a fazer pagamentos recorrentes.

Prevenção: A principal defesa é a calma e a desconfiança. Jamais realize qualquer pagamento ou transferência. A orientação é não prolongar a conversa, mas, se possível, gravar a ligação ou salvar as mensagens (prints). Não apague as provas e procure imediatamente a autoridade policial para registrar um Boletim de Ocorrência, fornecendo todos os detalhes da tentativa de extorsão.



🔗Retorne ao Índice

Sextorsão: A Extorsão por Fotos Íntimas

A sextorsão é uma forma de chantagem que explora o medo e a vergonha. O golpe geralmente começa com um criminoso usando um perfil falso, na maioria das vezes de uma mulher jovem e atraente, para iniciar uma conversa com a vítima (tipicamente homens) em redes sociais.[24] Após ganhar a confiança, o golpista a convence a trocar fotos ou vídeos de natureza íntima. De posse desse material comprometedor, a fraude muda de fase. Um segundo criminoso entra em cena, se passando por uma figura de autoridade, como o pai furioso da suposta jovem ou até mesmo um falso policial. Ele alega que a garota era menor de idade e que a vítima cometeu um crime grave. Sob ameaça de expor as imagens para a família, amigos e empregador da vítima, ou de dar prosseguimento a um falso inquérito policial, ele exige pagamentos para manter o silêncio.[24]

Prevenção: A medida preventiva mais eficaz é nunca compartilhar conteúdo íntimo com pessoas desconhecidas na internet. Caso se torne uma vítima, é crucial não ceder à extorsão; os pagamentos não farão com que as ameaças parem, pelo contrário, elas tendem a aumentar. O procedimento correto é: não apague as conversas, salve todas as provas (prints das mensagens e dos perfis), bloqueie os contatos dos criminosos e registre imediatamente um Boletim de Ocorrência na delegacia de polícia.

⚠ ALERTA

A sextorsão é um golpe em que criminosos usam perfis falsos para enganar vítimas, obter imagens íntimas e depois chantageá-las com ameaças. Nunca compartilhe conteúdo íntimo com desconhecidos.

🔗Retorne ao Índice

A Mentalidade Defensiva: Estratégias Universais de Proteção

A proteção contra fraudes digitais não depende de uma única ferramenta, mas sim da adoção de uma mentalidade defensiva e de um conjunto de práticas de higiene digital. A seguir, são consolidadas as estratégias de prevenção mais eficazes, que, quando aplicadas em conjunto, criam múltiplas camadas de segurança.

Princípio da Desconfiança Ativa

A base de toda a segurança digital é transformar a cautela em um hábito proativo. A regra de ouro deve ser: na dúvida, não clique, não informe, não transfira. Sempre que receber uma comunicação inesperada ou suspeita, especialmente se ela evocar um senso de urgência, medo ou uma oferta milagrosa, pare e verifique a informação por um canal secundário e confiável.[8] Se o banco ligar, desligue e ligue você mesmo para o número oficial. Se receber um e-mail com uma promoção, digite o endereço da loja no navegador em vez de clicar no link.

Higiene Digital Essencial

- **Gestão de Senhas:** A prática de usar a mesma senha para múltiplos serviços é uma das maiores vulnerabilidades. Crie senhas fortes (longas, com letras maiúsculas e minúsculas, números e símbolos) e, fundamentalmente, únicas para cada conta.[39] Para gerenciar essa complexidade, utilize um gerenciador de senhas confiável, que armazena suas credenciais de forma segura e as preenche automaticamente.[67]
- **Autenticação de Dois Fatores (2FA):** Esta é, possivelmente, a camada de segurança mais importante contra o roubo de contas. Ative a 2FA (ou verificação em duas etapas) em todos os serviços que a oferecem, como WhatsApp, e-mails, redes sociais e aplicativos bancários. Ela exige um segundo código (gerado por um aplicativo ou enviado por SMS) além da sua senha, tornando o acesso por parte de criminosos muito mais difícil, mesmo que eles tenham roubado sua senha.[14]
- **Atualizações e Backups:** Mantenha seus sistemas operacionais (no celular e no computador), aplicativos e programas antivírus sempre atualizados. As atualizações frequentemente contêm correções para falhas de segurança recém-descobertas.[10] Além disso, realize backups periódicos de seus dados importantes (fotos, documentos) em um disco externo ou serviço de nuvem. Isso garante que você não perca tudo em caso de um ataque de ransomware ou falha do dispositivo.[67]

Retorne ao Índice

Proteção de Canais e Dispositivos

● **Blindando o Celular:** Seu smartphone é o centro da sua vida digital e financeira. Proteja-o com uma senha de bloqueio de tela forte (biometria ou PIN/padrão complexo). Ative também um código PIN para o seu chip (cartão SIM), o que impede que criminosos usem seu número em outro aparelho em caso de roubo.[39] Habilite as funções de rastreamento ("Encontre Meu Dispositivo" no Android ou "Buscar iPhone" no iOS) para permitir o bloqueio e a exclusão remota dos dados em caso de perda ou furto.[66]
● **App Celular Seguro:** Utilize o aplicativo 🔗 "Celular Seguro", uma iniciativa do Governo Federal em parceria com a FEBRABAN e a ANATEL. A ferramenta permite que, em caso de perda, furto ou roubo, você possa registrar uma ocorrência que bloqueia rapidamente o aparelho, a linha telefônica e o acesso aos aplicativos bancários, dificultando a ação dos criminosos.[21]

Segurança Transacional

● **Compras Online:** Dê preferência a sites conhecidos e com boa reputação. Sempre verifique a presença do "https" e do ícone de cadeado no endereço do site.[21] Para maximizar a segurança, utilize um cartão de crédito virtual para cada compra. A maioria dos bancos oferece essa funcionalidade, que gera um número de cartão temporário e descartável.[21]
● **Wi-Fi Público:** Evite realizar transações financeiras, acessar seu banco ou inserir informações sensíveis quando estiver conectado a redes Wi-Fi públicas e abertas (de aeroportos, cafés, shoppings), pois elas podem ser inseguras e monitoradas por criminosos. Se precisar usá-las, utilize uma Rede Privada Virtual (VPN) para criptografar sua conexão.[65]

Reduzindo a Pegada Digital

Seja consciente sobre as informações que você compartilha online. Configure seus perfis de redes sociais como privados para limitar quem pode ver suas postagens e dados pessoais. Evite compartilhar informações excessivas que possam ser usadas por golpistas (como data de nascimento completa, nome de parentes, etc.). Considere também utilizar serviços para remover suas informações de sites de busca de pessoas (people search websites), que agregam e vendem dados publicamente disponíveis.[68]

🔗 Retorne ao Índice

Guia de Ação Pós-Incidente: Fui Vítima, e Agora?

Agir com rapidez e método após ser vítima de um golpe é crucial para mitigar os danos e aumentar as chances de recuperação. O período imediatamente após a descoberta da fraude, conhecido como a "hora de ouro", é o mais crítico.

Ações Imediatas (A "Golden Hour" da Fraude)

1.Contato com o Banco: Esta é a primeira e mais urgente providência. Ligue imediatamente para a central de atendimento do seu banco. Utilize o número oficial, que consta no verso do seu cartão ou no site da instituição. Informe o ocorrido e solicite o bloqueio imediato de todos os seus cartões, da sua conta e do acesso ao aplicativo bancário.[6]
2.Acionando o MED do PIX: Se a fraude envolveu uma transferência via PIX, ao contatar seu banco, solicite explicitamente a abertura de um Mecanismo Especial de Devolução (MED). Este protocolo permite que seu banco notifique a instituição que recebeu o dinheiro para que ela bloqueie os fundos na conta do golpista. O tempo é o fator mais crítico para o sucesso do MED, pois ele depende da existência de saldo na conta de destino.[29]

O Registro Formal

1.Boletim de Ocorrência (B.O.): Registre um Boletim de Ocorrência o mais rápido possível. Na maioria dos estados brasileiros, isso pode ser feito de forma online, através do site da Polícia Civil.[34] O B.O. é o documento oficial que formaliza o crime e é essencial para a investigação policial, bem como para contestações de débitos junto às instituições financeiras e de crédito. Ao registrar, forneça o máximo de detalhes possível: números de telefone, chaves PIX, nomes, prints de conversas, e-mails e qualquer outra prova que você tenha coletado.[71]

2.Comunicação à Polícia Civil: Procure a Delegacia Especializada de Repressão a Crimes Cibernéticos (DRCC) do seu estado. No Estado de Mato Grosso, comunique à Delegacia Especializada de Repressão a Crimes Informáticos (DRCI): Rua Santiago, nº 215, Jardim das Américas - Cuiabá/MT, Telefone: (65) 3613-5625 / (65) 98173-0710, Chatbot: (65) 98173-0544 (atendimento virtual whatsapp), E-mail: drci@pjc.mt.gov.br

Retorne ao Índice

Guia de Ação Pós-Incidente: Fui Vítima, e Agora?

Limpeza e Contenção Digital

1.Trocar Todas as Senhas: Altere imediatamente a senha da conta que foi comprometida. Por precaução, troque também as senhas de outras contas importantes (especialmente seu e-mail principal), principalmente se você reutilizava senhas.
2.Notificar Plataformas: Denuncie o perfil ou a conta fraudulenta na rede social (Facebook, Instagram, WhatsApp) ou na plataforma onde o golpe se originou. Isso ajuda a plataforma a remover o conteúdo malicioso e a proteger outros usuários.[8]
3.Verificar Dispositivos: Execute uma varredura completa com um software antivírus atualizado em seu celular e computador. Isso é especialmente importante em casos como o golpe da "Mão Fantasma" ou phishing, para garantir que não há malwares ou aplicativos espiões instalados.[8]

Monitoramento e Próximos Passos

1.Monitorar Extratos e Faturas: Nos dias e semanas seguintes ao golpe, monitore de perto seus extratos bancários e faturas de cartão de crédito para identificar qualquer outra atividade fraudulenta que possa ter passado despercebida.

Recomendações de Prevenção para o Cidadão:

1.Registrato (Banco Central): Consultar mensalmente para verificar todas as contas bancárias abertas em seu nome, incluindo instituições de pagamento. [74]
2.Rede Sim (Receita Federal): Inibir a permissão para participar de CNPJs, evitando que dados sejam usados para abrir empresas fraudulentas em seu nome.[75]
3.Cautela: Tomar cuidado com ligações e mensagens, pois criminosos usam dados vazados para dar roupagem lícita às abordagens.

Retorne ao Índice

Golpes virtuais: como mitigar o impacto social e enfraquecer o crime organizado.

“A crescente onda de aplicação e a sofisticação dos golpes virtuais impõe um desafio estratégico às instituições públicas e privadas, exigindo ações preventivas articuladas e baseadas em inteligência.

Para além de episódios isolados, as fraudes digitais configuram uma ameaça sistêmica, que impacta a segurança financeira, a confiança social e a estabilidade das organizações. Nesse cenário, a prevenção e a ampla divulgação dos diferentes tipos de golpe são instrumentos para reduzir vulnerabilidades, fortalecer a resiliência informacional e mitigar os efeitos da engenharia social, principal vetor dessas práticas ilícitas.

A publicização atua como barreira de contenção, ampliando a conscientização social e dificultando a atuação de criminosos, ao passo que o trabalho de inteligência permite antecipar tendências e estruturar respostas mais eficazes. Assim, unir conhecimento técnico, comunicação clara e cooperação institucional é o caminho mais sólido para enfrentar o avanço dos crimes digitais e proteger a sociedade.

Eventos acadêmicos assumem também papel central nesse processo, pois promovem a difusão de conhecimento e aproximam a comunidade dos mecanismos de prevenção e das peculiaridades de cada modalidade de fraude catalogada e, de outro lado, reforçam que não se trata de um rol fechado de golpes, já que a criatividade e a inovação dos criminosos são constantes, exigindo vigilância contínua, aprendizado permanente e a construção de uma cultura de segurança digital compartilhada.”

Mauro Zaque de Jesus
Coordenador do Centro de Segurança e Inteligência-CSI

Retorne ao Índice

Referências citadas

1.Como o Brasil está enfrentando o aumento de fraudes online em 2024 - Estado de Minas, acessado em agosto 11, 2025, https://www.em.com.br/emfoco/2025/03/19/como-o-brasil-esta-enfrentando-o-aumento-de-fraudes-online-em-2024/

2.Número de golpes digitais aumenta em quase 50% em 2024 | Radar - VEJA, acessado em agosto 11, 2025, https://veja.abril.com.br/coluna/radar/numero-de-golpes-digitais-aumenta-em-quase-50-em-2024/

3.Brasil perdeu mais de R$ 297,7 bilhões com fraudes em 2024 - TI Inside, acessado em agosto 11, 2025, https://tiinside.com.br/19/03/2025/brasil-perdeu-mais-de-r-2977-bilhoes-com-fraudes-em-2024/

4.Golpes digitais atingem 24% da população brasileira, revela DataSenado - Senado Federal, acessado em agosto 11, 2025, https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado

5.Golpes atuais mais comuns – Agência Nacional de ... - Portal Gov.br, acessado em agosto 11, 2025, https://www.gov.br/anatel/pt-br/assuntos/dicas-contra-fraudes/golpes-atuais-mais-comuns

6.Veja os 10 golpes mais comuns aplicados contra idosos e saiba como evitá-los - Febraban, acessado em agosto 11, 2025, https://portal.febraban.org.br/noticia/4177/pt-br

7.Como fortalecer seu WhatsApp para evitar que ele seja usado em golpes financeiros?, acessado em agosto 11, 2025, https://www.estadao.com.br/economia/como-fortalecer-whatsapp-evitar-seja-usado-golpes-financeiros-nprei/

8.Os 9 golpes mais comuns nas redes sociais - McAfee, acessado em agosto 11, 2025, https://www.mcafee.com/blogs/pt-br/seguranca-na-internet/os-9-golpes-mais-comuns-nas-redes-sociais/

9.Os Principais Golpes pela internet em 2024 | [RECOMENDADO], acessado em agosto 11, 2025, https://alexandreberthe.com.br/os-principais-golpes-pela-internet-em-2024/

10.Quais os golpes bancários mais aplicados em 2024? Veja dicas para se proteger - Estadão, acessado em agosto 11, 2025, https://www.estadao.com.br/economia/golpes-bancarios-mais-praticados-2024-febraban-veja-dicas-para-se-proteger-nprei/

11.Saiba quais foram os 10 golpes mais aplicados contra ... - Febraban, acessado em agosto 11, 2025, https://portal.febraban.org.br/noticia/4279/pt-br/

12.Febraban alerta para novo golpe sobre falsa investigação nas agências bancárias, acessado em agosto 11, 2025, https://portal.febraban.org.br/noticia/4194/pt-br/

13.Novo golpe da 'mão fantasma' acende alerta da Polícia Federal - Estado de Minas, acessado em agosto 11, 2025, https://www.em.com.br/app/noticia/nacional/2022/08/24/interna_nacional,1388723/novo-golpe-da-mao-fantasma-acende-alerta-da-policia-federal.shtml

14.Veja como como se proteger de golpes comuns no WhatsApp, acessado em agosto 11, 2025, https://www.estadao.com.br/web-stories/economia/veja-como-como-se-proteger-de-golpes-comuns-no-whatsapp-nprei/

15.Golpe do WhatsApp: entenda e saiba como se proteger - SPC Brasil, acessado em agosto 11, 2025, https://www.spcbrasil.org.br/blog/golpe-do-whatsapp

16.Esses são os principais golpes nas redes sociais que atingem pessoas idosas todos os dias - Estado de Minas - Em foco, acessado em agosto 11, 2025, https://www.em.com.br/emfoco/2025/08/11/esses-sao-os-principais-golpes-nas-redes-sociais-que-atingem-pessoas-idosas-todos-os-dias/

17.Golpes mais comuns na internet em 2025 e como se proteger - Terra, acessado em agosto 11, 2025, https://www.terra.com.br/byte/seguranca-digital/golpes-mais-comuns-na-internet-em-2025-e-como-se-proteger,08f8da78bd94e7f0f628c195dbcf13efnfhw573c.html
18.10 Golpes mais comuns na internet: saiba quais são! - Blog da Algar, acessado em agosto 11, 2025, https://blog.algar.com.br/golpes-mais-comuns-na-internet/
19.Polícia Federal adverte sobre mensagens falsas em seu nome na internet - Agência Brasil, acessado em agosto 11, 2025, https://agenciabrasil.ebc.com.br/geral/noticia/2015-02/policia-federal-adverte-contra-mensagens-falsas-na-internet-em-seu-nome
20.Receita Federal alerta: criminosos simulam endereços de e-mail do órgão para aplicar golpes - Portal Gov.br, acessado em agosto 11, 2025, https://www.gov.br/receitafederal/pt-br/assuntos/noticias/2025/abril/receita-federal-alerta-criminosos-simulam-enderecos-de-e-mail-do-orgao-para-aplicar-golpes
21.Antifraude - Febraban, acessado em agosto 11, 2025, https://portal.febraban.org.br/AntiFraude/
22.Quais são os principais golpes online e como evitá-los? - Kaspersky, acessado em agosto 11, 2025, https://www.kaspersky.com.br/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim
23.Saiba quais foram os 10 golpes mais aplicados contra clientes bancários em 2024, segundo a Febraban | O TEMPO, acessado em agosto 11, 2025, https://www.otempo.com.br/economia/2025/4/14/saiba-quais-foram-os-10-golpes-mais-aplicados-contra-clientes-bancarios-em-2024-segundo-a-febraban
24.Cartilha Golpes na Internet - Atualizada.cdr - Acesso, acessado em agosto 11, 2025, https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf
25.Tipos de golpes pelo WhatsApp: quais os mais comuns? - Neon, acessado em agosto 11, 2025, https://neon.com.br/aprenda/seguranca-digital/tipos-de-golpes-pelo-whatsapp/
26.Conheça os principais golpes aplicados com o uso do celular e saiba como evitá-los - FEBRABAN - Notícias, acessado em agosto 11, 2025, https://portal.febraban.org.br/noticia/4097/pt-br/
27.Quais são os golpes mais comuns na Internet? - Blog da MAG Seguros, acessado em agosto 11, 2025, https://blog.mag.com.br/golpes-de-internet-mais-comuns/
28.Golpe do Pix: veja quais são e saiba como se proteger - SPC Brasil, acessado em agosto 11, 2025, https://www.spcbrasil.org.br/blog/golpe-do-pix
29.Vítima fez um Pix e caiu em um golpe - Banco Central, acessado em agosto 11, 2025, https://www.bcb.gov.br/meubc/faqs/p/vitima-fez-um-pix-e-caiu-em-um-golpe
30.Robô multiplicador de renda e robô Pix funcionam? Veja a verdade!, acessado em agosto 11, 2025, https://blog.genialinvestimentos.com.br/robo-multiplicador-de-renda-e-robo-pix-funcionam-veja-a-verdade/
31.Robô Pix promete dinheiro rápido: é golpe? Como se proteger - meutudo, acessado em agosto 11, 2025, https://meutudo.com.br/blog/robo-de-pix/
32.Golpe do Robô do Pix - Aprenda como evitar - RecargaPay, acessado em agosto 11, 2025, https://recargapay.com.br/pix/robo-do-pix
33.Golpe do Robô do Pix: veja como se prevenir da armadilha - Terra, acessado em agosto 11, 2025, https://www.terra.com.br/economia/golpe-do-robo-do-pix-veja-como-se-prevenir-da-armadilha,256cfe966202def1131db04ada086f71z7vk7n43.html
34.Dia da Mentira: PCPR publica cartilha sobre golpes clássicos e armadilhas digitais - Governo do Paraná, acessado em agosto 11, 2025, https://www.parana.pr.gov.br/aen/Noticia/Dia-da-Mentira-PCPR-publica-cartilha-sobre-golpes-classicos-e-armadilhas-digitais

35.Como não cair em golpes ao alugar casa na praia - DESC Imóveis, acessado em agosto 11, 2025, https://desc.com.br/artigo/485/como-nao-cair-em-golpes-ao-alugar-casa-na-praia
36.Febraban alerta para o golpe da falsa venda no Dia das Mães, acessado em agosto 11, 2025, https://portal.febraban.org.br/noticia/4284/pt-br/
37.Febraban alerta para golpes praticados contra consumidores - Agência Brasil - EBC, acessado em agosto 11, 2025, https://agenciabrasil.ebc.com.br/radioagencia-nacional/economia/audio/2025-05/febraban-alerta-para-golpes-praticados-contra-consumidores
38.Como evitar fraudes em imóveis de temporada | TemporadaLivre, acessado em agosto 11, 2025, https://www.temporadalivre.com/blog/como-evitar-fraudes-em-imoveis-de-temporada
39.Dez dicas de segurança para se prevenir contra golpes e fraudes - Sicredi, acessado em agosto 11, 2025, https://www.sicredi.com.br/coop/altosdaserra/noticias/seguranca/dez-dicas-de-seguranca-para-se-prevenir-contra-golpes-e-fraudes/
40.Golpe do Falso Leilão | Portal - MPMG, acessado em agosto 11, 2025, https://www.mpmg.mp.br/portal/menu/comunicacao/publicacoes/golpe-do-falso-leilao.shtml
41.Golpe do Leilão - Polícia Civil do Paraná, acessado em agosto 11, 2025, https://www.policiacivil.pr.gov.br/NUCIBER/falsoLeilao
42.Golpe do leilão falso: saiba como identificar e se proteger | Blog Premium - Serasa, acessado em agosto 11, 2025, https://www.serasa.com.br/premium/blog/golpe-leilao-falso-como-identificar-para-nao-cair/
43.Golpe do falso leilão resulta na condenação de seis pessoas em Santa Catarina - Imprensa, acessado em agosto 11, 2025, https://www.tjsc.jus.br/web/imprensa/-/-golpe-do-falso-leilao-resulta-na-condenacao-de-seis-pessoas-em-santa-catarina-
44.Golpes de Leilão Online e Selos de Segurança Falsos: Como Criminosos Imitam o TrustLogo para Enganar - Sectigo Brasil, acessado em agosto 11, 2025, https://www.sectigo.com.br/blog/golpes-leilao-online-selos-de-seguranca-falsos
45.Falso leilão: Como identificar e se proteger desse golpe - Migalhas, acessado em agosto 11, 2025, https://www.migalhas.com.br/depeso/424772/falso-leilao-como-identificar-e-se-proteger-desse-golpe
46.Golpe do delivery com maquininhas – veja como funciona - Concil, acessado em agosto 11, 2025, https://www.concil.com.br/blog/golpe-do-delivery-com-maquininhas-veja-como-funciona/
47.Como funciona o Golpe do Delivery? Saiba como se proteger!, acessado em agosto 11, 2025, https://blog.pagseguro.uol.com.br/como-funciona-o-golpe-do-delivery/
48.Golpe do delivery: entenda como funciona - Rosenbaum Advogados, acessado em agosto 11, 2025, https://www.rosenbaum.adv.br/golpe-do-delivery-entenda-como-funciona/
49.Golpe do Delivery: aprenda como se proteger – Blog Santander, acessado em agosto 11, 2025, https://www.santander.com.br/blog/golpe-delivery
50.Golpe do delivery: como funciona e como não cair nessa? - Fala, Nubank, acessado em agosto 11, 2025, https://blog.nubank.com.br/golpe-do-delivery-como-funciona/
51.Golpe do Aluguel de Temporada: como evitar cair nesta armadilha | UNINTER NOTÍCIAS, acessado em agosto 11, 2025, https://www.uninter.com/noticias/golpe-do-aluguel-de-temporada-como-evitar-cair-nesta-armadilha
52.Como se proteger de golpes ao alugar casas de temporada - Viagem e Turismo, acessado em agosto 11, 2025, https://viagemeturismo.abril.com.br/manual-do-viajante/como-se-proteger-do-golpe-de-aluguel-de-casas-de-temporada/
53.Como evitar golpe em aluguel de temporada?, acessado em agosto 11, 2025, https://anfitrioesdealuguel.com.br/blog/como-evitar-golpe-em-aluguel-de-temporada/

54.Foto com presente? Polícia Civil do Paraná alerta população sobre novo golpe, acessado em agosto 11, 2025, https://www.aen.pr.gov.br/Noticia/Foto-com-presente-Policia-Civil-do-Parana-alerta-populacao-sobre-novo-golpe
55.Golpe da mão fantasma: saiba como se proteger e o que fazer se for vítima - Sicredi, acessado em agosto 11, 2025, https://www.sicredi.com.br/site/blog/seguranca/golpe-mao-fantasma/
56.Golpe da mão fantasma: bancos nunca pedem que clientes instalem app para resolver problemas na conta - FEBRABAN - Notícias, acessado em agosto 11, 2025, https://portal.febraban.org.br/noticia/4318/pt-br/
57.Golpe da Mão Fantasma - YouTube, acessado em agosto 11, 2025, https://m.youtube.com/shorts/VL5qmoysee4
58.Conheça os principais golpes - Portal BB, acessado em agosto 11, 2025, https://www.bb.com.br/site/pra-voce/seguranca/conheca-os-principais-golpes/
59.Você sabe o que é o golpe da mão fantasma? - Blog Santander, acessado em agosto 11, 2025, https://www.santander.com.br/blog/golpe-da-mao-fantasma
60.Golpe do falso presente: saiba como identificar e se proteger - Blog Mercantil, acessado em agosto 11, 2025, https://blog.bancomercantil.com.br/seguranca/golpe-do-falso-presente/
61.Novo golpe do 'Presente de Aniversário' pode estar alvejando seu cartão agora! - UAI, acessado em agosto 11, 2025, https://www.uai.com.br/uainoticias/2025/08/09/novo-golpe-do-presente-de-aniversario-pode-estar-alvejando-seu-cartao-agora/
62.Golpe do presente falso: o que é e como acontece? - blog nubank, acessado em agosto 11, 2025, https://blog.nubank.com.br/golpe-do-presente-falso/
63.Golpe do presente de aniversário: descubra como evitar - Banco Bmg, acessado em agosto 11, 2025, https://www.bancobmg.com.br/blog/dicas-de-seguranca/golpe-do-presente-de-aniversario-descubra-como-evitar/
64.Cuidado com os golpes na internet: dicas para se proteger - Infraprev, acessado em agosto 11, 2025, https://www.infraprev.org.br/cuidado-com-os-golpes-na-internet-dicas-para-se-proteger/
65.10 dicas infalíveis para se proteger de golpes virtuais - GZH, acessado em agosto 11, 2025, https://gauchazh.clicrbs.com.br/economia/noticia/2024/09/10-dicas-infaliveis-para-se-proteger-de-golpes-virtuais-cm11klowp00i401e41dgwblz4.html
66.Fique atento aos golpes e saiba como se proteger | Bradesco Segurança, acessado em agosto 11, 2025, https://banco.bradesco/seguranca/index.shtm
67.Fascículos - Cartilha de Segurança para Internet - CERT.br, acessado em agosto 11, 2025, https://cartilha.cert.br/fasciculos/
68.10 dicas de prevenção de fraude - Keeper Security, acessado em agosto 11, 2025, https://www.keepersecurity.com/blog/pt-br/2023/11/14/fraud-prevention-tips/
69.Cartilha contra golpes - Polícia Civil do Paraná, acessado em agosto 11, 2025, https://www.policiacivil.pr.gov.br/Pagina/Cartilha-contra-golpes
70.Não Caia Nessa - Polícia Civil do Paraná, acessado em agosto 11, 2025, https://www.policiacivil.pr.gov.br/sites/default/arquivos_restritos/files/documento/2024-04/cartilha_golpes_pcpr-_2024.pdf
71.Cartilha Prevenção Golpes - Polícia Civil de Santa Catarina, acessado em agosto 11, 2025, https://pc.sc.gov.br/wp-content/uploads/2024/04/Cartilha-Prevencao-Golpes-1.pdf
72.Comunica PF, acessado em agosto 11, 2025, https://apps.pf.gov.br/r/comunicapf/comunicapf/pagina-inicial
73.Comunicação de Crimes – Polícia Federal - Portal Gov.br, acessado em agosto 11, 2025, https://www.gov.br/pf/pt-br/canais_atendimento/comunicacao-de-crimes
74.Consultar mensalmente o banco central para verificar todas as contas bancárias abertas em seu nome, https://www.bcb.gov.br/meubc/registrato
75.Inibir a permissão para participar de CNPJs, evitando que dados sejam usados para abrir empresas fraudulentas em seu nome, https://permissao.negocios.redesim.gov.br/login
76.Golpe do falso advogado, https://www.trf3.jus.br/campanhas/2025/golpe-falso-advogado
77.Golpe da falsa encomenda, https://www.santander.com.br/blog/golpe-dos-correios

Ministério Público do Estado de Mato Grosso
Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial

– GUIA DE BOAS PRÁTICAS –

Equipe do Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial

Membro Coordenador do Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial
Adalberto Ferreira de Souza Junior – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Membro Coordenador Adjunto do Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial
Fabrício Miranda Mereb – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Membro Colaborador do Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial
Adalberto Biazotto Junior – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Membro Colaborador do Centro de Apoio Operacional de Defesa de Dados Pessoais e Inteligência Artificial
Leoni Carvalho Neto – Promotor de Justiça do Ministério Público do Estado de Mato Grosso

Servidora
Maria Cristina Alves Ormond - Auxiliar Ministerial.

Residente Técnico
Pedro Carlos Nogueira Felix

Elaboração do Material :
Adalberto Ferreira de Souza Junior - Promotor de Justiça e Coordenador
Fabrício Miranda Mereb - Promotor de Justiça e Coordenador Adjunto
Adalberto Biazotto Junior - Promotor de Justiça e Colaborador
Leoni Carvalho Neto - Promotor de Justiça e Colaborador
Maria Cristina Alves Ormond - Auxiliar Ministerial
Pedro Carlos Nogueira Felix - Residente Técnico

Apoio na Elaboração do Material :
Centro de Segurança e Inteligência - CSI

CAO/MPMT

DEFESA DE DADOS PESSOAIS E INTELIGÊNCIA ARTIFICIAL

CSI/MPMT

Centro de Segurança e Inteligência MPMT

MPMT

Ministério Público

DO ESTADO DE MATO GROSSO