

COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 04

Golpes digitais e fraudes eletrônicas

Prevenção, identificação e investigação



HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO
GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Golpes digitais e fraudes eletrônicas

Prevenção, identificação e investigação

Como reconhecer abordagens fraudulentas, reduzir danos e compreender os caminhos da investigação.

Coleção Investigação e Proteção na Era Digital
Volume 04

1ª edição
Santa Fé do Sul, SP
CodexNauta
2026

© 2026 Higor Vinicius Nogueira Jorge

Material educativo de distribuição gratuita.

Coleção Investigação e Proteção na Era Digital, volume 04.

www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.

Golpes digitais e fraudes eletrônicas : prevenção, identificação e investigação [recurso eletrônico] / Higor Vinicius Nogueira Jorge. -- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.

1 recurso online (52 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 4)

Formato: PDF.

Modo de acesso: World Wide Web: <www.higorjorge.com.br>.

Inclui referências e apêndices.

Publicação de distribuição gratuita.

1. Fraudes eletrônicas. 2. Golpes digitais. 3. Engenharia social. 4. Segurança digital. 5. Prevenção criminal. 6. Investigação criminal. I. Título. II. Série.

Sumário

Apresentação.....	5
Objetivos e público-alvo.....	6
1 Panorama das fraudes digitais.....	7
2 Engenharia social e exploração da confiança.....	10
3 Bancos e falsas centrais de atendimento.....	13
4 Fraudes com Pix e transferências eletrônicas.....	16
5 Falso advogado e outras identidades profissionais.....	20
6 Comércio eletrônico e plataformas fraudulentas.....	23
7 Prevenção e identificação de sinais suspeitos.....	26
8 Providências iniciais diante da fraude.....	29
9 Investigação e atribuição de autoria.....	33
10 Estudos de caso e revisão prática.....	37
Considerações finais.....	41
Apêndice A. Protocolo das primeiras horas.....	42
Apêndice B. Sinais de alerta e respostas seguras.....	44
Apêndice C. Registro inicial do incidente.....	45
Referências.....	46
Minicurrículo do autor.....	49
Para aprofundar o estudo.....	51
A coleção.....	52

Apresentação

Uma mensagem pode conhecer o nome da vítima, mencionar um processo verdadeiro ou reproduzir a voz de um familiar. Esses elementos tornam a abordagem convincente, mas precisam ser avaliados antes de qualquer pagamento. A prevenção começa quando a pessoa conserva meios de verificar o pedido fora da conversa em que ele surgiu.

No capítulo sobre fraudes eletrônicas do meu livro *Investigação criminal tecnológica*, examino a exploração da confiança, a urgência fabricada e a necessidade de reconstruir a abordagem anterior ao prejuízo. Esta cartilha desenvolve esses conceitos para o cidadão e para quem investiga, conectando prevenção, resposta inicial e apuração fundamentada (Jorge, 2027).

O leitor encontrará falsas centrais bancárias, transferências induzidas por engano, falsas identidades profissionais e comércio eletrônico fraudulento. Os capítulos explicam como agir diante de cada situação e quais vestígios podem ajudar a esclarecer o ocorrido. O capítulo investigativo distingue a conta que recebeu o dinheiro da pessoa que efetivamente participou do crime.

Ser vítima não autoriza culpa ou humilhação. O atendimento precisa facilitar a comunicação rápida e registrar o que aconteceu com precisão. A publicação oferece ferramentas para esse trabalho e estimula uma prática simples: confirmar a solicitação por um canal independente, antes de assumir seus riscos.

Higor Vinicius Nogueira Jorge
www.higorjorge.com.br

Objetivos e público-alvo

Este volume se dirige a cidadãos, estudantes e profissionais da investigação. O objetivo comum é compreender como uma fraude se organiza, reconhecer sinais de alerta e preservar informações úteis. O capítulo 9 aprofunda o trabalho das autoridades, com linguagem acessível a quem deseja entender a apuração.

Após terminar a leitura, espera-se que o cidadão saiba verificar pedidos suspeitos, interromper uma interação perigosa e comunicar o incidente sem aguardar uma solução prometida pelo próprio fraudador. Espera-se que o profissional consiga reconstruir a abordagem, delimitar as fontes de dados e testar hipóteses de participação individual.

Percursos de leitura

Os capítulos 1 e 2 apresentam conceitos. Os capítulos 3 a 6 examinam situações recorrentes. Os capítulos 7 e 8 organizam prevenção e resposta. Os capítulos 9 e 10 desenvolvem investigação e casos hipotéticos. Os apêndices podem ser impressos e utilizados no atendimento ou na orientação de familiares.

Se o golpe está acontecendo agora. Interrompa os pagamentos e a conversa. Se houve operação financeira, comunique imediatamente seu banco por canal oficial. Se houver controle indevido do aparelho, use outro dispositivo confiável. Consulte o protocolo do Apêndice A; a preservação de informações não deve atrasar sua proteção.

As orientações não exigem que a vítima identifique o responsável ou realize testes em links e arquivos. Esses exames podem exigir ambiente especializado e atuação legalmente autorizada.

CAPÍTULO 1

Panorama das fraudes digitais

1.1 O que precisa ser compreendido

Golpe digital é uma expressão cotidiana para situações em que recursos digitais ajudam a enganar, obter acesso ou causar prejuízo. Ela descreve o modo de atuação, sem substituir a classificação jurídica. A mesma história contada por mensagem pode envolver crimes diferentes conforme o que foi feito, por quem e com qual intenção.

Uma análise inicial deve separar a abordagem, a ação solicitada, o acesso eventualmente obtido e o resultado. Um telefonema pode levar a um pagamento realizado pela vítima. Em outra situação, alguém acessa indevidamente uma conta e movimenta valores sem sua participação. A aparência de pagamento eletrônico não resolve essa diferença.

No livro de referência, a apuração das fraudes acompanha tanto a comunicação quanto o movimento do dinheiro. Esse olhar evita reduzir o caso ao último comprovante e permite descobrir quais informações levaram a vítima a confiar na solicitação (Jorge, 2027).

Exemplo hipotético. Uma pessoa recebe aviso de compra suspeita e realiza uma transferência acreditando cancelá-la. O comprovante mostra o destino do pagamento; a conversa ajuda a explicar o engano. Examinar os dois registros produz uma descrição mais completa do que analisar apenas o saldo perdido.

A cartilha trabalha com mecanismos e critérios de verificação. Os nomes populares dos golpes podem mudar; reconhecer quem pede a ação, de onde surgiu a confiança e como confirmar a solicitação continua útil.

1.2 Da primeira abordagem ao prejuízo

Uma fraude pode começar por anúncio, telefonema, mensagem ou contato presencial. O fraudador apresenta uma justificativa, obtém uma resposta e adapta o pedido. Às vezes, diferentes pessoas aparentam cumprir funções separadas, como atendente, supervisor ou advogado. Essa encenação precisa

ser reconstruída sem presumir que cada personagem corresponde a um participante real distinto.

A história pode produzir perdas financeiras e outros danos. A vítima entrega documento, código ou acesso ao aparelho; depois aparecem contas, empréstimos ou mensagens enviadas em seu nome. Por isso, descobrir se houve transferência é apenas parte do atendimento. Também é preciso perguntar quais informações foram compartilhadas e quais permissões foram concedidas.

Etapa observada	Pergunta para compreender o fato
Contato inicial	Como a pessoa chegou à vítima?
Aparência de legitimidade	Que informação, imagem ou vínculo inspirou confiança?
Pedido	Que ação foi solicitada e com qual justificativa?
Execução	O que a vítima ou outra pessoa efetivamente fez?
Consequência	Que prejuízo, acesso ou exposição foi identificado?

Esse mapa é um instrumento de descrição, sem funcionar como teste automático de crime. A resposta depende dos documentos, das versões e das verificações possíveis. A ausência de uma transferência não torna inofensiva uma tentativa de obter senhas ou documentos.

Aprendizado. Registrar a sequência ajuda a explicar o mecanismo e a escolher providências. Expressões vagas, como “invadiram tudo”, precisam ser esclarecidas com perguntas sobre acontecimentos concretos.

1.3 O enquadramento depende da conduta

O Código Penal distingue o estelionato, no art. 171, da subtração mediante fraude eletrônica, no art. 155, § 4º-B. O art. 171, § 2º-A, trata da fraude eletrônica nas condições descritas no dispositivo. O art. 154-A disciplina a invasão de dispositivo informático. A escolha do enquadramento exige reconstruir a atuação e o elemento subjetivo, sem partir apenas do nome popular do golpe (Brasil, 1940).

A entrega de valores pela vítima, induzida em erro, e a subtração sem esse ato de disposição são distinções úteis ao raciocínio. Situações combinadas, acesso remoto e diferentes momentos de atuação exigem exame individual. O livro de referência utiliza essa diferença para orientar perguntas e diligências (Jorge, 2027).

O art. 171, § 2º, VII, prevê a cessão de conta laranja. A presença de um nome no comprovante não demonstra, por si, a conduta prevista. É necessário apurar como a conta foi aberta, disponibilizada e controlada. O § 5º do art. 171 foi revogado pela Lei nº 15.397/2026. A análise de fatos anteriores demanda cuidado com a sucessão normativa; a vítima deve comunicar o ocorrido prontamente, sem tentar resolver essa questão sozinha (Brasil, 1940).

Para as hipóteses de estelionato descritas no art. 70, § 4º, do CPP, a competência considera o domicílio da vítima, com regra própria para pluralidade de vítimas. Isso não autoriza generalizar a solução a qualquer delito digital (Brasil, 1941).

CAPÍTULO 2

Engenharia social e exploração da confiança

2.1 Como o pedido ganha credibilidade

Engenharia social é a manipulação de pessoas para obter informações ou induzir ações. No contexto das fraudes, o pedido procura parecer compatível com uma relação conhecida: cliente e banco, familiar e parente, advogado e cliente. A pessoa é levada a aceitar uma explicação antes de examinar a consequência do que fará.

O fraudador pode usar informações verdadeiras em uma narrativa falsa. Saber o nome de um gerente, o endereço de uma empresa ou a existência de um processo não comprova que o contato foi autorizado. Esses dados podem ter origens diferentes, que precisam ser investigadas. A abordagem não permite concluir automaticamente que determinada organização sofreu vazamento.

No livro de referência, a urgência fabricada ajuda a explicar por que a conferência independente é abandonada. A contribuição prática é identificar o momento em que a vítima foi pressionada a decidir e quais obstáculos foram criados à verificação (Jorge, 2027).

Exemplo hipotético. Uma mensagem menciona uma entrega esperada e exige taxa imediata. A coincidência com uma compra recente aumenta a plausibilidade. O comprador pode consultar o pedido no aplicativo legítimo da loja ou transportadora, sem abrir o endereço recebido.

O CERT.br (2026c) relaciona a engenharia social à exploração de sentimentos e à indução de respostas impulsivas. A proteção deve permitir uma pausa para conferir o pedido, inclusive quando o assunto desperta medo ou vontade de ajudar.

2.2 Por que a pressa dificulta a conferência

A pressão pode assumir formas diferentes. Uma perda é anunciada como iminente; uma oportunidade parece prestes a acabar; o interlocutor exige segredo para supostamente proteger uma investigação. Em todos esses

cenários, a vítima é desencorajada a consultar outra pessoa ou usar um canal próprio.

Uma providência segura é transformar a regra de decisão antes do incidente: pagamentos novos e mudanças de destinatário precisam de confirmação independente. Essa regra deve valer também para pedidos emocionalmente convincentes. Se a pessoa conhecida está em perigo real, a verificação pode ocorrer por contatos familiares já estabelecidos e por serviços oficiais adequados à situação.

Exemplo hipotético. Alguém escreve que trocou de número e precisa pagar uma conta. A foto é de um familiar. O destinatário tenta o número anterior e conversa com outra pessoa da família por contato conhecido. A conferência recai sobre a identidade e a necessidade, sem exigir que o remetente suspeito forneça mais dados.

Em famílias e organizações, a ajuda deve ser acessível. Um funcionário que teme punição por perguntar tende a decidir sozinho. Um familiar que recebe críticas pode esconder o primeiro pagamento. Combinar uma pessoa de apoio e aceitar perguntas reduz esse isolamento.

Erro frequente. Confundir prevenção com julgamento moral. Ter atendido a uma solicitação manipuladora não torna a vítima responsável pela fraude. O relato detalhado é mais útil que uma discussão sobre o que ela deveria ter percebido.

2.3 Imagem e voz precisam de contexto

Fotografia, áudio e vídeo podem ser reutilizados ou alterados. Sistemas de inteligência artificial também permitem produzir conteúdo sintético. A aparência familiar, isoladamente, não resolve a identidade de quem pede dinheiro. Tampouco um detalhe visual estranho comprova falsificação.

No livro de referência, o tratamento das manipulações sintéticas reforça a investigação da origem e do contexto. Para o cidadão, a consequência é prática: uma confirmação deve usar um caminho que o próprio solicitante suspeito não controla (Jorge, 2027).

Como confirmar. Encerre a interação e procure o contato conhecido, o aplicativo legítimo ou o endereço oficial já utilizado. Se uma mensagem indica um telefone “para confirmar”, esse telefone continua fazendo parte da abordagem. Uma chamada de vídeo feita dentro da mesma conta suspeita também pode conservar o problema de origem.

Exemplo hipotético. Um áudio com voz parecida com a de um gestor pede pagamento fora do procedimento. A equipe confirma pelo telefone corporativo já cadastrado e consulta a solicitação no sistema de compras. O objetivo é verificar a ordem e o destinatário, sem tentar diagnosticar a autenticidade pela voz.

Perguntas baseadas em aniversários, parentes ou locais conhecidos podem ter respostas disponíveis publicamente. Um acordo familiar de confirmação pode ajudar, mas não deve substituir o retorno por canal independente. Se persistir a dúvida, suspenda a operação e peça ajuda a alguém de confiança.

CAPÍTULO 3

Bancos e falsas centrais de atendimento

3.1 O problema inventado e a falsa solução

Na falsa central, alguém se apresenta como funcionário de banco ou empresa e anuncia uma compra, acesso ou risco supostamente identificado. A conversa oferece uma solução que exige ações da vítima. O ponto decisivo é compreender o efeito dessas ações: o que aparece como cancelamento pode ser uma nova transferência ou autorização.

A Anatel descreve abordagens que direcionam a vítima a um falso atendimento e tentam obter dados ou acesso ao dispositivo. A orientação institucional é verificar o assunto nos canais oficiais, escolhidos fora da mensagem recebida (Agência Nacional de Telecomunicações, 2026).

A exibição de nome, logotipo ou número conhecido na chamada não basta para validar o contato. Também não basta que o interlocutor conheça dados pessoais. Um protocolo informado por ele integra a história até ser confirmado por fonte independente.

Exemplo hipotético. Uma ligação afirma que uma compra será cancelada se o cliente confirmar uma operação no aplicativo. Antes de autorizar, o cliente encerra a chamada e consulta sua instituição por canal oficial. O suposto atendente não deve acompanhar essa conferência por compartilhamento de tela.

O banco pode manter serviços legítimos de alerta. A existência desses serviços não dispensa o cuidado com pedidos inesperados. O cliente deve conservar o controle sobre o caminho de atendimento e compreender o que está autorizando.

3.2 Pedidos que exigem interrupção

Uma transferência para supostamente proteger saldo muda o destino do dinheiro. A instalação de programa ou a concessão de acesso remoto pode permitir observar informações ou interferir no aparelho. A aprovação de uma

solicitação de acesso pode abrir uma sessão. Esses efeitos devem ser considerados antes de aceitar a explicação do interlocutor.

Não forneça a quem entrou em contato senhas ou códigos de autenticação. Também não leia nem envie códigos gerados para autorizar operações. Se você iniciou um atendimento legítimo, siga apenas o procedimento oficial e mantenha em sigilo as credenciais de acesso. A orientação do CERT.br (2023a) destaca a proteção das contas e a consulta independente aos canais financeiros.

Uma pessoa pode receber instruções para fazer vários pagamentos de pequeno valor, apresentados como testes. A divisão dos valores não elimina o risco. O mesmo cuidado vale para empréstimos supostamente necessários à regularização ou para entrega de cartão a um mensageiro.

Exemplo hipotético. O interlocutor pede uma captura da tela bancária para “localizar o erro”. A imagem revela saldo, dados de conta e informações de operação. O cliente interrompe o pedido e procura a instituição por outro meio, sem produzir novas imagens para o contato suspeito.

Aprendizado. Avalie a ação pelo resultado que ela pode causar. O nome atribuído ao procedimento durante a conversa não altera seu efeito sobre conta, aparelho ou dinheiro.

3.3 Quando o procedimento já foi iniciado

Se você autorizou algo, relate ao banco exatamente o que aconteceu. Diferencie transferência, instalação, compartilhamento de tela e envio de código. Dizer apenas que recebeu uma ligação pode omitir o acesso que continua ativo. Use outro aparelho confiável quando houver suspeita de controle do dispositivo.

Não mantenha a conversa para tentar descobrir quem está ligando. A contenção deve começar pelo canal oficial da instituição. Guarde protocolos e informações já disponíveis, sem atrasar o bloqueio ou assumir novos riscos. Os detalhes de preservação e recuperação de acesso estão no capítulo 8.

Para quem investiga. A narrativa precisa identificar a sequência das instruções, os momentos em que o cliente entrou no aplicativo e as operações efetivamente executadas. Uma gravação disponível, o histórico de chamadas e as comunicações recebidas podem ajudar a reconstruir a abordagem. O atendimento não deve exigir que a vítima reproduza o golpe.

O livro de referência orienta a examinar a infraestrutura de comunicação junto ao percurso financeiro. Essa correlação pode mostrar que um número foi usado para induzir o pagamento, sem provar que seu titular cadastral foi a pessoa que fez a ligação (Jorge, 2027).

Erro frequente. Tratar a confirmação de uma senha ou biometria como explicação completa do fato. O registro técnico de autorização precisa ser examinado junto ao contexto de possível indução, ao controle do aparelho e às demais informações regularmente obtidas.

CAPÍTULO 4

Fraudes com Pix e transferências eletrônicas

4.1 O pagamento e a história que o motivou

O Pix é um meio de pagamento. A fraude pode usar esse meio para receber valores decorrentes de uma mentira, de um acesso indevido ou de outra conduta. O comprovante ajuda a individualizar a operação; não explica sozinho por que o pagamento ocorreu.

Antes de confirmar uma transferência, confira destinatário, valor e motivo. Se os dados divergem da relação esperada, interrompa a operação e esclareça a divergência por canal independente. A presença de um nome conhecido merece conferência adicional: a conta pode ser legítima e estar sendo usada indevidamente.

Um código QR pode encaminhar a diferentes ações. Em uma cobrança, o leitor deve observar o que o aplicativo apresenta antes de autorizar. Ler o código não significa que a obrigação foi verificada. O CERT.br (2026b) recomenda examinar o contexto e os dados exibidos na confirmação.

Exemplo hipotético. Uma pessoa espera pagar uma loja, mas a tela mostra outra pessoa física. O vendedor alega que é “a conta do financeiro”. A explicação deve ser confirmada pelo canal oficial da loja antes de qualquer pagamento. Uma divergência não comprova crime, mas torna inadequado prosseguir sem esclarecimento.

Também nas transferências por outros meios, conserve o comprovante completo e procure o banco diante de suspeita. O mecanismo de resposta depende da operação efetivamente realizada, identificável no extrato.

4.2 Comprovante recebido precisa ser conferido

Quem vende ou recebe valores deve consultar seu próprio extrato e o estado da transação. Uma imagem encaminhada pelo comprador pode ser alterada, registrar agendamento ou se referir a operação diferente. A entrega de um bem deve considerar a confirmação do ingresso efetivo e as condições da negociação.

Se alguém diz que enviou um Pix por engano, não use a imagem enviada como única referência. Verifique o extrato no aplicativo legítimo. Confirmado o recebimento, utilize a função de devolução vinculada à transação original, quando cabível, para retornar à conta de origem. Se houver dúvida, procure seu banco antes de movimentar o valor. O Banco Central adverte contra pedidos de devolução para outra conta (Banco Central do Brasil, 2026a).

Exemplo hipotético. Após uma entrada de valor, o remetente pede retorno para a conta de um terceiro. A pessoa que recebeu não faz uma nova transferência conforme essa indicação e busca orientação em sua instituição. Assim, evita criar uma operação separada que possa dificultar a compreensão do ocorrido.

O mesmo cuidado vale para um suposto excesso de pagamento. Uma venda anunciada por certo preço não autoriza concluir, pela captura de tela, que houve depósito maior. Conferir a própria conta evita devolver recursos que nunca entraram.

Aprendizado. Mantenha a relação entre recebimento e eventual devolução. Cada nova transferência cria outro fato financeiro, que precisa de justificativa e registro próprios.

4.3 O que o MED permite solicitar

O Mecanismo Especial de Devolução, conhecido como MED, integra o Pix e permite solicitar análise de devolução em situações elegíveis, como fraude. A vítima deve comunicar o caso imediatamente à sua instituição, pelo aplicativo legítimo ou por outro canal oficial, e pedir o acionamento do mecanismo cabível (Banco Central do Brasil, 2026a).

A análise e os bloqueios ocorrem segundo as regras do sistema. A recuperação pode ser integral, parcial ou não ocorrer. Depende do enquadramento, da apuração pelas instituições e da disponibilidade de recursos alcançados pelo procedimento. O MED não é promessa de ressarcimento (Banco Central do Brasil, 2026c).

É importante descrever corretamente o motivo. Ter sido enganado para fazer uma transferência difere de enviar dinheiro por erro de digitação. Uma compra em estabelecimento fictício também difere de uma divergência comercial com

fornecedor de boa-fé. Essas diferenças influenciam a análise; a vítima deve relatar os fatos, sem tentar ajustar artificialmente sua narrativa a uma categoria.

O MED não se destina a Pix enviado por engano nem a mero desacordo comercial, e resguarda recursos de terceiros de boa-fé. O pedido está sujeito a prazo e requisitos próprios. Consulte as regras atuais no banco e no portal do Banco Central, sem aguardar o limite para agir. Não é necessário esperar a conclusão da investigação criminal para comunicar a fraude à instituição.

Erro frequente. Acreditar que só o boletim de ocorrência interrompe o percurso do dinheiro. O registro policial e a comunicação bancária têm funções diferentes e precisam ser providenciados com rapidez, podendo contar com ajuda de uma pessoa de confiança.

4.4 Contestação bancária e investigação criminal

O procedimento bancário procura analisar a operação e aplicar os mecanismos disponíveis. A investigação criminal procura esclarecer o fato e a participação das pessoas. Um bloqueio preventivo não equivale a uma condenação; uma devolução não identifica todos os responsáveis; a ausência de devolução também não afasta, por si, a ocorrência de crime.

Situação comunicada	Providência inicial do cidadão
Pix ligado a suspeita de fraude	Relatar ao banco e solicitar análise pelo MED.
Compra no cartão não reconhecida	Contestar no emissor e pedir medidas de proteção.
Boleto possivelmente adulterado	Avisar o banco e o fornecedor por canal independente.
Divergência comercial	Acionar fornecedor e canais de defesa do consumidor.
Acesso indevido a conta	Proteger o acesso e informar operações e permissões.

A orientação do Banco Central para compras fraudulentas com cartão é comunicar e contestar imediatamente na instituição. O tratamento precisa acompanhar o meio utilizado, sem aplicar o MED a pagamentos que não foram Pix (Banco Central do Brasil, 2026b).

Se o atendimento não resolver a demanda, registre o protocolo e utilize os canais formais de revisão da instituição. Procon, Consumidor.gov.br, reclamação ao Banco Central e orientação jurídica podem ser pertinentes, conforme a relação e o problema. Esses caminhos não garantem restituição nem substituem a comunicação policial quando há suspeita de crime.

Aprendizado. Descrever o evento com precisão permite acionar o mecanismo adequado. A vítima não precisa aguardar uma resposta definitiva em uma esfera para informar o ocorrido na outra.

CAPÍTULO 5

Falso advogado e outras identidades profissionais

5.1 Quando os dados verdadeiros sustentam a mentira

No golpe do falso advogado, o contato pode mencionar um processo existente e usar nome ou imagem de profissional conhecido. O pedido costuma associar pagamento antecipado à liberação de valor. A informação correta sobre o processo cria uma aparência de acesso privilegiado, embora não comprove a identidade do interlocutor.

A OAB Paraná orienta a confirmar a solicitação com o escritório por telefone já conhecido. A recomendação se aplica também quando o contato utiliza voz ou imagem familiar (Ordem dos Advogados do Brasil. Seção do Paraná, 2026).

Exemplo hipotético. Uma cliente recebe mensagem com o número de sua ação e uma suposta guia para liberar indenização. Ela confere com o advogado pelo contato do contrato. O profissional informa que não enviou a cobrança. A consulta independente interrompe o pedido antes do pagamento.

Custas, tributos e honorários podem existir em relações legítimas, com fundamentos e formas próprias. A prevenção exige verificar obrigação, emissor, destinatário e meio de pagamento no canal competente. Regras locais sobre recolhimento não devem ser substituídas por uma promessa genérica recebida em conversa.

Erro frequente. Presumir que conhecer o processo prova a autoria do contato ou demonstra invasão do escritório. A origem das informações precisa ser apurada. A pessoa cuja identidade foi utilizada também pode ser vítima e deve ser comunicada por um canal seguro.

5.2 Conferir inscrição e confirmar o pedido

A inscrição de um advogado pode ser consultada nos sistemas oficiais da OAB. Essa consulta ajuda a verificar a existência e a situação do profissional. Ainda é preciso confirmar que ele fez o contato e autorizou a solicitação específica.

O ConfirmADV é apresentado pelo Conselho Federal da OAB como mecanismo auxiliar de consulta, integrado ao cadastro profissional. Sua utilização acrescenta uma verificação, mas deve ser acompanhada da conferência do pedido pelos contatos já estabelecidos (Ordem dos Advogados do Brasil. Conselho Federal, 2025).

Roteiro seguro. Localize o contrato ou um contato anterior confiável. Procure o escritório por esse caminho e descreva o pedido recebido, sem fazer pagamentos durante a conferência. Se necessário, consulte o andamento no portal oficial do tribunal. Uma tela ou guia enviada pelo interlocutor não substitui essa consulta.

Se houve pagamento, comunique imediatamente a instituição financeira, registre a ocorrência e avise o profissional e a OAB pelos canais oficiais pertinentes. Preserve a mensagem e o documento recebido sem divulgá-los em grupos. Processos podem conter informações de outras pessoas, que precisam de proteção.

Para quem investiga. Compare o documento apresentado com sua fonte oficial e registre quais informações eram públicas ou restritas. A coincidência de dados deve orientar uma verificação sobre a origem, sem ser convertida em conclusão antecipada sobre vazamento ou participação do profissional.

5.3 Prestígio profissional também pode ser imitado

A mesma lógica pode aparecer em contatos que simulam contadores, servidores, fornecedores, responsáveis por recrutamento ou profissionais de saúde. O título apresentado procura dar autoridade a uma cobrança ou coleta de dados. A verificação deve recair sobre a instituição, o vínculo e a ação concreta solicitada.

Exemplo hipotético. Uma empresa recebe mensagem que imita o contador e anuncia nova conta para pagamento de serviço habitual. A equipe consulta o contato cadastrado, confirma a nota e examina o beneficiário. A existência de contrato e cobrança recorrente não dispensa a validação de uma mudança inesperada.

Pedidos em nome de órgãos públicos devem ser conferidos no portal ou atendimento oficial competente. Evite usar números e endereços fornecidos na mensagem suspeita. A presença de brasão, assinatura digitalizada ou documento de identidade não comprova que a ordem partiu da autoridade indicada.

Para organizações, a regra de alteração de dados de pagamento deve prever confirmação por contato anterior, responsável identificado e registro da mudança. Quando há maior risco, a revisão por outra pessoa reduz a dependência de uma única decisão sob pressão.

Aprendizado. Confirmar a profissão não basta. É necessário verificar se aquela pessoa, no exercício daquele vínculo, pediu aquela providência. A confiança pode ser mantida com regras claras de conferência, que protegem clientes e profissionais.

CAPÍTULO 6

Comércio eletrônico e plataformas fraudulentas

6.1 O anúncio e o vendedor são verificações diferentes

Um anúncio pode aparecer em um serviço conhecido e levar a uma página controlada por terceiros. Uma plataforma legítima também pode reunir vendedores diferentes. Antes de comprar, identifique quem oferece, quem recebe e onde a contratação será registrada. O reconhecimento da marca da plataforma não esclarece sozinho essas relações.

O CERT.br (2023b) recomenda examinar a reputação do vendedor, acessar os canais legítimos e conservar a negociação nos ambientes que oferecem seus recursos de segurança. Pedidos para sair do procedimento exigem cuidado, especialmente quando prometem desconto ou atribuem a mudança a uma suposta falha do sistema.

Avaliações, seguidores e tempo aparente de atividade são elementos para consulta, sem funcionar como garantia. Uma conta antiga pode ter mudado de controle; comentários podem não representar experiências verificáveis. Também a presença de CNPJ precisa ser conferida no contexto: um número válido pode ter sido copiado de outra empresa.

Exemplo hipotético. Um anúncio de eletrodoméstico leva a uma página com nome semelhante ao de uma grande loja. Em vez de usar o endereço do anúncio, a compradora abre o aplicativo legítimo e procura a oferta. Como não encontra a condição anunciada, consulta o atendimento oficial antes de pagar.

Aprendizado. A oferta precisa ser confirmada na relação real de compra. Aparência profissional, publicidade paga e grande quantidade de comentários não dispensam a verificação do fornecedor e do destinatário.

6.2 Segurança da conexão e legitimidade da oferta

O cadeado e o uso de HTTPS indicam aspectos da proteção da conexão, sem certificar a honestidade de quem opera o site. Páginas falsas também podem

usar conexão criptografada. Para verificar a loja, considere o endereço efetivamente acessado, a origem do acesso, a identificação do fornecedor e os canais de confirmação.

Não abra um endereço suspeito apenas para testar se é seguro. Se a oferta já despertou dúvida, procure a empresa por um caminho independente. Em celular, endereços longos ou incompletos podem dificultar a leitura. A solução é interromper e conferir, sem tentar adivinhar a parte oculta.

Em boletos e cobranças, observe os dados exibidos no momento da autorização. Uma página pode mostrar a marca de uma empresa e direcionar o pagamento a outra pessoa. Se houver intermediador legítimo, esclareça sua participação no canal oficial antes de prosseguir.

Exemplo hipotético. Um comprador recebe uma segunda cobrança por mensagem, atribuída a falha no primeiro pagamento. Ele consulta o pedido no aplicativo em que contratou e o próprio extrato. Sem confirmação da obrigação, não realiza o pagamento adicional.

O livro de referência recomenda reconstruir a infraestrutura que deu credibilidade ao golpe. Na investigação de uma loja fictícia, isso inclui a relação entre anúncio, página, atendimento e destinatário financeiro. A existência de cada elemento precisa ser documentada, sem presumir que todos têm o mesmo controlador (Jorge, 2027).

6.3 O risco existe dos dois lados da negociação

Quem vende pode receber comprovante falso, pedido de devolução de suposto excesso ou mensagem que imita o suporte da plataforma. Antes de entregar o produto, confira o pagamento na própria conta ou no sistema legítimo. Um e-mail de confirmação precisa ser confrontado com o registro existente no serviço.

Exemplo hipotético. Após anunciar um móvel, o vendedor recebe mensagem dizendo que precisa pagar uma taxa para liberar o valor da venda. Ele acessa o atendimento oficial da plataforma por conta própria. O pedido recebido não aparece no sistema, e nenhum valor foi creditado.

Em negociações presenciais, considere também a segurança do encontro e do transporte. A apresentação de um documento ou uma imagem de saldo não substitui a confirmação da operação. Se houver ameaça ou risco imediato, a proteção pessoal tem prioridade sobre a preservação de detalhes da conversa.

Uma entrega atrasada ou um produto diferente do anunciado exige examinar a relação de consumo e as circunstâncias. A suspeita de crime deve indicar os elementos que sugerem o engano, como identidade simulada e oferta inexistente, sem transformar todo inadimplemento em fraude.

Para problemas com empresas participantes, o Consumidor.gov.br permite registrar demandas e acompanhar respostas. O MJSP orienta reunir os documentos e descrever o ocorrido objetivamente. Esse atendimento não substitui a comunicação policial de um fato possivelmente criminoso (Brasil. Ministério da Justiça e Segurança Pública, 2026).

CAPÍTULO 7

Prevenção e identificação de sinais suspeitos

7.1 Criar condições para decidir com calma

A prevenção funciona melhor quando há uma regra simples para situações de pressão. Em pagamentos inesperados, a pessoa deve conseguir interromper a conversa e consultar alguém ou uma instituição por caminho próprio. A regra precisa ser conhecida antes de aparecer uma solicitação urgente.

Uma família pode combinar que troca de número e pedido de dinheiro serão confirmados por contato anterior. Uma empresa pode exigir verificação adicional para novo beneficiário ou mudança de dados bancários. O procedimento deve indicar quem confirma, por qual canal e onde a decisão será registrada.

O cuidado pode ser ajustado ao risco. Um pagamento habitual para destinatário confirmado exige menos verificação que uma transferência elevada, fora do padrão, para conta recém-indicada. A urgência alegada aumenta a necessidade de conferência, em vez de dispensá-la.

Exemplo hipotético. Uma funcionária recebe ordem aparentemente enviada pelo gestor durante uma reunião. Como se trata de novo destinatário, consulta o contato corporativo cadastrado e registra a confirmação no procedimento financeiro. A regra protege a funcionária e facilita explicar a decisão posteriormente.

Erro frequente. Criar uma regra impossível de cumprir. Se o canal de confirmação é inacessível, as pessoas tendem a improvisar. O acordo precisa oferecer alternativa segura, como outro responsável ou adiamento do pagamento até que a verificação seja possível.

O objetivo é tornar a pausa uma parte normal da decisão, sem exigir que cada cidadão se transforme em especialista em fraude.

7.2 Um sinal pede verificação e não acusação

Pedidos de segredo, transferência fora do procedimento, nova conta e pressão emocional justificam uma conferência adicional. Nenhum sinal isolado comprova crime. Uma pessoa legítima pode trocar de número; uma cobrança real pode ser urgente. O problema é prosseguir sem verificar uma solicitação que reúne condições de risco.

Sinal percebido	Verificação útil
Contato inesperado com pedido de dinheiro	Retomar o contato conhecido fora da conversa.
Mudança de beneficiário	Confirmar a alteração no cadastro e no canal anterior.
Promessa de vantagem excepcional	Conferir oferta e condições na fonte legítima.
Pedido de código ou acesso ao aparelho	Interromper e procurar o serviço oficial.
Proibição de consultar outra pessoa	Suspender a decisão e buscar apoio.

Não existe uma quantidade de sinais que transforme automaticamente uma mensagem em fraude. O quadro ajuda a escolher uma resposta protetiva. A classificação jurídica e a atribuição pessoal pertencem a outro processo de análise.

Exemplo hipotético. Uma prestadora muda de banco e avisa por e-mail. O cliente confirma com o responsável já cadastrado, recebe documentação coerente e atualiza o registro da relação. A cautela foi útil mesmo sem haver golpe.

Aprendizado. Suspender uma operação duvidosa pode ser uma decisão provisória. Não é necessário acusar alguém publicamente para recusar um pedido ainda não confirmado.

7.3 Reduzir exposição e limitar consequências

A proteção da conta e do aparelho complementa a verificação de pedidos. Senhas diferentes reduzem a propagação de um comprometimento entre serviços. A autenticação adicional aumenta a proteção de acesso, mas uma aprovação feita sob indução ainda precisa ser evitada. Recuse solicitações de autenticação que você não iniciou.

Mantenha sistema e aplicativos atualizados e use os canais legítimos para obtê-los. Ajuste limites financeiros às necessidades e acompanhe notificações e extratos. Essas medidas podem reduzir a exposição e permitir perceber operações inesperadas, sem eliminar todo risco (CERT.br, 2023a).

Organize a recuperação das contas para não depender exclusivamente de um aparelho que pode se perder ou ser comprometido. Proteja também o e-mail utilizado para recuperar senhas. Ao mudar de telefone ou número, revise sessões, permissões e meios de recuperação pelos recursos oficiais dos serviços.

Exemplo hipotético. Uma pessoa mantém o mesmo código em vários serviços e o informa em página falsa. O problema pode atingir outras contas que aceitem essa credencial. A resposta deve considerar onde ela foi reutilizada e começar por um dispositivo confiável.

Compartilhe orientações com familiares sem expor extratos, documentos ou detalhes desnecessários. Para organizações, treinar a equipe deve incluir o caminho de comunicação de incidentes, com acolhimento e registro. A descoberta rápida perde utilidade quando o responsável teme contar o que aconteceu.

CAPÍTULO 8

Providências iniciais diante da fraude

8.1 Conter o dano e pedir ajuda

A primeira resposta deve acompanhar o risco que continua ativo. Interrompa pagamentos e o contato com o suspeito. Se houve operação financeira, procure imediatamente sua instituição por canal oficial, informe o que aconteceu e peça medidas de proteção e contestação adequadas. Não espere o fraudador cumprir uma promessa de estorno.

Se você concedeu acesso remoto ou suspeita de controle do aparelho, pare de utilizá-lo para operações sensíveis. Procure o banco e os serviços afetados em outro dispositivo confiável. Interrompa o acesso indevido, inclusive a conexão do aparelho afetado quando isso puder ser feito com segurança, e busque orientação técnica. Anote a medida adotada e o horário aproximado.

Não faça uma restauração do aparelho por impulso. Essa alteração pode apagar registros úteis; a limpeza pode exigir orientação especializada. A prioridade continua sendo impedir danos, sem manter um acesso perigoso apenas para conservar uma tela. A preservação profissional deve considerar o estado concreto do dispositivo.

O CERT.br (2026a) recomenda cortar o contato e não enviar novos valores ou informações. A pessoa de apoio pode ajudar a localizar os canais legítimos e registrar protocolos, sem assumir senhas ou divulgar os documentos do caso.

Exemplo hipotético. A vítima percebe o golpe durante uma chamada e pede ajuda a um familiar para contatar o banco em outro aparelho. A conversa é encerrada e o pedido de proteção ocorre antes da organização completa dos arquivos.

8.2 O que informar ao banco e à polícia

Descreva os fatos na ordem em que ocorreram. Informe o primeiro contato, o pedido recebido, as ações realizadas e o momento em que percebeu o problema.

Diferencie o que viu do que o interlocutor afirmou. Se não souber um horário ou detalhe, registre essa incerteza.

No banco, individualize as operações com os comprovantes disponíveis e relate acessos, códigos ou permissões compartilhados. Solicite protocolo e guarde a resposta. No Pix, peça a análise pelo MED quando se tratar de suspeita de fraude; nos demais meios, pergunte qual contestação ou medida é cabível.

Na comunicação policial, apresente mensagens já recebidas, identificação aparente dos contatos, comprovantes e protocolos. O boletim de ocorrência registra a notícia do fato e subsidia as providências. Seu registro não confirma automaticamente a autoria de quem aparece no relato.

O CERT.br (2026a) destaca a utilidade de guardar informações do golpe e dos atendimentos. A organização pode ser simples: uma pasta com arquivos recebidos, outra com documentos financeiros e uma anotação das providências, sem alterar os originais.

Exemplo hipotético. A vítima não lembra se o pedido de instalação veio antes ou depois do primeiro pagamento. Ela relata a dúvida e apresenta as mensagens existentes. A sequência pode ser esclarecida por registros, sem exigir que complete a memória com uma suposição.

Aprendizado. A vítima oferece informações e documentos disponíveis. A investigação verifica sua relação com o fato e os limites de cada elemento.

8.3 Guardar o disponível sem ampliar o risco

Uma captura de tela pode ajudar a mostrar uma mensagem, mas deve conservar informações de contexto, como identificação do contato e sequência disponível. Quando viável e seguro, mantenha também os arquivos recebidos e os registros no serviço de origem. Não edite o único exemplar para destacar ou ocultar trechos.

Anote o endereço que já aparece na mensagem sem abri-lo. Não baixe anexos adicionais nem reexecute um arquivo para verificar seu efeito. Quem já recebeu conteúdo suspeito deve informar essa circunstância no atendimento, para que o material seja tratado pelo meio adequado.

Exemplo hipotético. Uma pessoa quer recortar dados de terceiros antes de publicar um alerta. Ela preserva o material disponível para os canais competentes e produz, se necessário, uma mensagem preventiva sem comprovantes ou nomes. A divulgação pública não é etapa obrigatória de preservação.

Para o profissional, a documentação deve identificar origem, forma de recebimento, responsável, data e movimentações do material. A cadeia de custódia prevista nos arts. 158-A a 158-F do CPP exige rastreabilidade; a captura apresentada pelo cidadão é ponto de partida para exame e contextualização (Brasil, 1941).

A orientação metodológica do livro de referência conecta preservação, obtenção e interpretação. Um arquivo conservado pode continuar exigindo verificação de autenticidade e atribuição. A ausência de um dado não deve ser preenchida por presunção (Jorge, 2027).

8.4 A resposta continua depois do primeiro atendimento

Recupere os acessos pelos procedimentos oficiais, revise sessões desconhecidas e altere credenciais comprometidas em dispositivo confiável. Se dados de cartão foram expostos, comunique o emissor e solicite a proteção adequada. Se terceiros recebem pedidos em seu nome, avise-os por outro canal, com mensagem objetiva.

Acompanhe os protocolos e verifique se surgiram operações ou vínculos desconhecidos. Os serviços oficiais do Banco Central podem ajudar a consultar informações financeiras disponíveis ao próprio titular. Uma alteração inesperada precisa ser esclarecida; ela não demonstra sozinha a identidade de quem a causou.

O pedido bancário pode exigir informações complementares. Guarde a resposta e, se necessário, utilize os canais de revisão, defesa do consumidor ou orientação jurídica. O Consumidor.gov.br atende relações com empresas participantes e deve ser acessado pelo endereço oficial (Brasil. Ministério da Justiça e Segurança Pública, 2026).

Exemplo hipotético. Depois de registrar o golpe, a vítima recebe proposta de recuperação mediante taxa antecipada e envio de nova senha. Ela não paga nem entrega a credencial e confere o suposto serviço nos canais competentes. A referência ao caso anterior pode fazer parte de uma nova abordagem fraudulenta.

Aprendizado. Não negocie com alguém que promete acesso privilegiado a bloqueios ou restituição garantida. A comunicação deve continuar pelos canais oficiais e pelos profissionais escolhidos de forma independente, com identificação e condições verificadas.

CAPÍTULO 9

Investigação e atribuição de autoria

9.1 Planejar perguntas e fontes

Esta seção se destina à compreensão do trabalho profissional. Ao Delegado de Polícia cabe conduzir a investigação policial e requisitar os elementos pertinentes nos limites legais. O indiciamento exige ato fundamentado da autoridade, com análise de autoria, materialidade e circunstâncias. O apoio analítico e pericial possui funções próprias, sem substituir essa decisão (Brasil, 2013).

O planejamento deve estabelecer quais fatos precisam de esclarecimento e quais fontes podem ajudar. O relato da vítima, as comunicações e os documentos financeiros permitem formular hipóteses iniciais. Em seguida, é preciso escolher diligências capazes de diferenciá-las, em vez de acumular dados sem propósito.

No método desenvolvido no livro de referência, as fases de identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação se articulam de modo iterativo. Nas fraudes, a análise da abordagem e a do percurso financeiro devem se informar mutuamente (Jorge, 2027).

Exemplo hipotético. O comprovante aponta uma conta, mas há dúvida entre cessão consciente e uso sem conhecimento do titular. O plano precisa buscar informações sobre abertura, acesso, controle e destino dos recursos. A diligência escolhida deve produzir informação útil a essa distinção.

A equipe deve registrar o que está documentado, o que foi apenas relatado e o que continua como hipótese. Essa disciplina evita que uma sugestão de pesquisa se transforme em acusação ao ser copiada para outro relatório.

9.2 Urgência exige uma via juridicamente adequada

A Constituição protege privacidade, sigilo, dados pessoais e devido processo. A obtenção de informações deve ter finalidade delimitada, necessidade demonstrável e respeito à competência. A disponibilidade técnica não cria

autorização jurídica para consultar contas ou aparelhos de terceiros (Brasil, 1988, art. 5º).

No Marco Civil da Internet, preservação e acesso a registros são providências distintas. Os arts. 13 e 15 permitem os requerimentos cautelares previstos na lei, sem dispensar autorização judicial para disponibilização. O art. 22 disciplina requisitos do pedido de registros. O acompanhamento dos prazos é parte da diligência, inclusive quanto ao pedido judicial após a preservação (Brasil, 2014).

Dados cadastrais também exigem identificar a competência e o alcance da norma. A referência a cadastro não autoriza incluir conteúdo de mensagens ou histórico completo de acesso. Para dados financeiros, devem ser observadas a LC nº 105/2001 e as hipóteses legais de fornecimento; o comprovante da vítima não abre acesso geral às contas de terceiros. Na investigação policial, acesso a movimentações protegidas exige a via judicial pertinente, ressalvadas hipóteses legais específicas de fornecimento (Brasil, 2001).

Exemplo hipotético. Uma equipe pede preservar registros de um perfil para o intervalo do contato fraudulento e prepara o acesso pela via cabível. A resposta de que os dados foram guardados não permite tratá-los como se já tivessem sido entregues.

Medidas patrimoniais judiciais dependem de pressupostos próprios. O bloqueio bancário no MED não se confunde com uma decisão judicial de constrição. O profissional deve explicar qual providência solicita e a quem compete decidi-la.

9.3 Dinheiro e comunicação precisam de corroboração

Uma conta recebedora pode ser ponto de passagem, conta usada indevidamente ou instrumento conscientemente disponibilizado. Essas possibilidades exigem verificações. O vínculo cadastral é relevante para localizar perguntas, sem demonstrar automaticamente a ação, o conhecimento ou o benefício de determinada pessoa.

Também um endereço IP identifica uma relação técnica em certo contexto. Para interpretar um registro, considere data, horário, fuso e demais campos pertinentes. Compartilhamento de conexão, dispositivos usados por terceiros e

controle de contas são possibilidades que precisam ser examinadas conforme o caso. A titularidade não substitui a atribuição pessoal.

O Controle de Viés Investigativo, desenvolvido no livro de referência, exige trabalhar com alternativa plausível, suporte e diligência discriminante. Na fraude, uma pergunta útil é o que se esperaria encontrar se a conta tivesse sido usada sem conhecimento do titular e o que diferenciaria essa situação de uma cessão consciente (Jorge, 2027).

Exemplo hipotético. Duas contas recebem valores de vítimas diferentes e enviam pagamentos ao mesmo fornecedor. A coincidência orienta a pesquisa sobre a relação. O fornecedor pode ter recebido pagamento comercial legítimo; é preciso examinar operação, contexto e vínculos, sem incluí-lo automaticamente no grupo criminoso.

Erro frequente. Contar duas cópias do mesmo comprovante como fontes independentes. Corroboração exige considerar de onde vem cada informação e se uma apenas reproduz a outra. A conclusão deve expor o alcance dos registros e as alternativas efetivamente examinadas.

9.4 Apresentar resultados que possam ser conferidos

O relatório deve permitir relacionar cada afirmação à sua fonte. Identifique as operações com chaves de referência próprias, organize a linha do tempo e conserve os dados originais de horário junto às eventuais conversões. Em diagramas, diferencie transferência documentada, contato relatado e vínculo ainda hipotético.

Uma função de resumo criptográfico, o hash, pode apoiar o controle de integridade de arquivos. Seu cálculo não comprova que a informação é verdadeira nem que determinada pessoa produziu o conteúdo. O contexto e a forma de obtenção continuam necessários (Jorge, 2027).

Proteja documentos de vítimas, terceiros e investigados. O art. 4º, III e § 1º, da LGPD diferencia o tratamento para investigação e repressão penal e conserva exigências de proporcionalidade, devido processo e direitos. Essa previsão não autoriza divulgação irrestrita ou processamento sem controles (Brasil, 2018).

Uma eventual falha de registro deve ser descrita com seus efeitos sobre a verificação. A equipe precisa avaliar o que ainda pode ser esclarecido e quais limites permanecem. Ocultar a lacuna compromete o exame crítico do resultado.

Aprendizado. A apuração deve individualizar condutas, considerar elementos favoráveis e desfavoráveis às hipóteses e indicar pendências relevantes. Um percurso financeiro é parte da reconstrução. A conclusão sobre participação exige fundamento adicional, com respeito às competências e à presunção de inocência.

CAPÍTULO 10

Estudos de caso e revisão prática

10.1 Caso hipotético da falsa central

Todos os nomes, valores, documentos e resultados deste capítulo são fictícios. Os códigos identificam peças didáticas, sem representar autos ou testes reais. Os casos mostram decisões possíveis e não modelos universais de enquadramento.

Clara recebe uma ligação que anuncia compra suspeita. O interlocutor a orienta a transferir R\$ 4.800 para uma suposta conta protegida. Depois pede mais R\$ 1.200 para concluir a regularização. Clara faz os dois Pix. Ao falar com uma pessoa de confiança, percebe a possibilidade de golpe, encerra o contato e procura seu banco por canal oficial.

Ela solicita análise das duas operações, guarda o protocolo e registra ocorrência policial. Informa que não instalou programa, mas acessou o aplicativo enquanto ouvia as instruções. A equipe recebe os comprovantes D-01 e D-02 e uma captura de mensagem D-03. O relato é identificado como R-01.

O primeiro cuidado é separar os registros: D-01 e D-02 documentam operações; R-01 descreve a ligação; D-03 mostra parte da comunicação disponível. Ainda não há registro que identifique quem falou ao telefone. Os dois destinatários precisam de exame individual.

Decisão prática. A resposta bancária pode começar com as informações disponíveis, sem aguardar a identificação criminal. A equipe policial formula perguntas sobre a abordagem, o controle das contas e o destino dos valores, com diligências juridicamente adequadas.

10.2 Hipóteses e diligências no primeiro caso

O recebimento dos dois valores totaliza R\$ 6.000. Para descrever o prejuízo, deve-se verificar se os pagamentos foram concluídos e se houve alguma devolução. Um valor bloqueado não pode ser apresentado como já restituído.

Neste exercício, as duas operações foram concluídas e não há devolução confirmada.

Pergunta	Elemento disponível	Verificação necessária
Qual foi o engano?	R-01 e D-03.	Reconstruir a conversa e sua sequência.
Onde entraram os valores?	D-01 e D-02.	Confirmar os registros das operações.
Quem controlou as contas?	Titulares aparentes nos comprovantes.	Obter dados pertinentes pela via legal e testar alternativas.
Quem fez a ligação?	Número relatado em R-01.	Examinar registros e corroboração, sem presumir o operador.

O planejamento estabelece hipótese de atuação coordenada e alternativa de uso indevido de uma das contas. Os pedidos precisam indicar a pergunta, o intervalo e o dado necessário. Cada resposta pode modificar o plano; não há obrigação de conservar a primeira hipótese se novos elementos a enfraquecerem.

Conclusão provisória do exercício. Há elementos para apurar uma possível fraude, mas os documentos iniciais não permitem atribuir o telefonema aos titulares das contas. A ausência de identificação imediata do responsável não impede a proteção da vítima nem justifica preencher a lacuna com uma presunção.

Erro a evitar. Redigir que Clara transferiu “por vontade própria” sem registrar o engano relatado. A descrição deve distinguir execução material da operação e contexto em que ela foi induzida.

10.3 Caso hipotético do falso advogado

Rafael aguarda uma decisão em processo judicial. Recebe mensagem com nome e foto de sua advogada, número do processo e suposta cobrança de R\$ 950. O remetente afirma que o pagamento precisa ocorrer no mesmo dia para liberar

um valor. Rafael consulta a advogada pelo telefone constante do contrato antes de transferir.

A profissional informa que não enviou a mensagem. Rafael conserva os registros disponíveis e comunica a tentativa pelos canais competentes. Neste exercício, não houve pagamento. O fato de o contato conhecer o processo não demonstra de onde obteve os dados nem indica participação de alguém do escritório.

Para compreender a tentativa, a equipe identifica os campos presentes na mensagem, a origem aparente do contato e a guia já recebida. A consulta ao processo oficial ajuda a verificar o que existia e o que foi alegado. Acesso a contas privadas e dados protegidos exige fundamento próprio.

Aprendizado para o cidadão. A confirmação útil veio do contato anterior, escolhido fora da abordagem. O número do processo e a fotografia não foram tratados como prova de identidade. A consulta profissional oficial poderia auxiliar, sem substituir essa conferência.

Aprendizado para o profissional. A hipótese de fraude deve ser investigada com o mesmo cuidado de origem e atribuição. A ausência de perda financeira não dispensa o exame da conduta e de sua relevância jurídica, inclusive quanto à fase de execução efetivamente alcançada.

10.4 Caso hipotético de comércio eletrônico

Lúcia compra um produto e paga R\$ 780. Dias depois, recebe mensagem que exige R\$ 120 adicionais para liberar a entrega. A página da compra não fornece informação verificável, e o suposto atendimento insiste no pagamento. Lúcia consulta a empresa cuja marca foi utilizada, por canal independente, e descobre que a oferta não partiu dela.

Ela interrompe o contato, comunica o banco e apresenta os registros. A investigação precisa verificar a compra, o pagamento, a página e a origem da cobrança. A afirmação de que houve loja fictícia deve ser sustentada por esses elementos; um atraso isolado não levaria à mesma conclusão.

Checklist de revisão dos casos. [] A abordagem e as ações foram descritas separadamente?

[] Cada operação tem valor, origem, destino e estado identificados?

[] O que é relato está diferenciado do que está documentado?

[] Há alternativa plausível para o controle de cada conta?

[] As diligências têm finalidade e via jurídica definidas?

[] A resposta ao cidadão explica o que foi solicitado e o que falta?

Os casos mostram pontos comuns de verificação e respostas diferentes conforme o fato. A pressa em conter o dano deve coexistir com a precisão do registro. Na conclusão, informe o que se pode sustentar e o que permanece em aberto, sem prometer o resultado da investigação ou da recuperação financeira.

Considerações finais

Golpes digitais se tornam mais convincentes quando aproveitam relações conhecidas e momentos de pressão. A prevenção precisa permitir que o cidadão interrompa a interação e confirme o pedido por um canal que escolheu de forma independente. Ferramentas de proteção ajudam, mas não dispensam compreender a ação solicitada.

Quando o incidente ocorre, a resposta deve ser rápida e possível. Comunicar a instituição financeira, proteger acessos e registrar o fato não exige que a vítima descubra previamente o autor. Uma pessoa de confiança pode ajudar a executar essas providências e conservar informações sem ampliar a exposição.

A investigação, por sua vez, precisa reunir a história da abordagem e o percurso do dinheiro. Contas, perfis, aparelhos e conexões fornecem vestígios, cujo significado depende de contexto e obtenção regular. A titularidade aparente é uma pergunta a desenvolver, sem funcionar como resposta antecipada sobre a participação individual.

Esse compromisso acompanha a Investigação Criminal Tecnológica apresentada no livro de referência: identificar, preservar, obter, tratar, correlacionar, interpretar e apresentar informações com controle jurídico e crítico. O método deve tornar a conclusão compreensível e verificável (Jorge, 2027).

Os instrumentos a seguir organizam providências, sinais e registros. Podem ser adaptados ao atendimento e à educação preventiva, conservando a prioridade da proteção, a separação de competências e o respeito às pessoas envolvidas.

APÊNDICE A

Protocolo das primeiras horas

Roteiro para cidadãos e pessoas de apoio. A ordem deve acompanhar o risco concreto. As medidas podem ocorrer em paralelo; não é preciso concluir toda a documentação para pedir proteção.

A.1 Interromper e comunicar

Pare o contato e os pagamentos. Não negocie, não faça testes e não envie novas informações. Se houver risco imediato à integridade pessoal, procure o serviço de emergência adequado e um local seguro.

Fale com seu banco. Use o aplicativo legítimo, o contato oficial já conhecido ou outro canal independente. Informe operações, valores e ações realizadas. Solicite proteção e contestação cabíveis. Para Pix fraudulento, peça análise pelo MED. Guarde o protocolo e acompanhe a resposta, sem pressupor devolução.

Proteja os acessos. Se houve código, senha ou permissão compartilhados, informe o serviço afetado. Use dispositivo confiável quando houver suspeita de controle do aparelho. Interrompa o acesso indevido e busque ajuda técnica. Não restaure o equipamento por impulso.

Peça apoio. Uma pessoa de confiança pode localizar os canais oficiais e anotar as providências. Mantenha senhas e códigos sob seu controle. A ajuda não deve depender de acesso a links recebidos do suspeito.

Fonte: elaboração própria a partir dos capítulos 4 e 8, Banco Central do Brasil (2026a, 2026c) e CERT.br (2026a).

A.2 Registrar e acompanhar

Conserve os documentos já disponíveis sem reabrir conteúdo suspeito. Registre a ocorrência policial e apresente uma sequência dos fatos. Não faça investigação particular para descobrir acessos, contas ou endereços de terceiros.

Anote atendimentos e respostas. Revise operações e acessos pelos canais oficiais. Se necessário, utilize os meios formais de revisão, defesa do consumidor e orientação jurídica. Desconfie de cobrança para suposta recuperação garantida.

Figura 1. Providências que podem ocorrer em paralelo



Fonte: elaboração própria. A contenção não deve aguardar a organização completa dos documentos. O atendimento bancário não substitui a comunicação policial, nem esta aciona automaticamente a contestação no banco.

APÊNDICE B

Sinais de alerta e respostas seguras

Os sinais orientam a conferência; não são prova automática de crime. Não é necessário responder ao contato para testar a suspeita.

Sinal	Resposta segura
Pressa para pagar	Suspenda e confirme por canal independente.
Novo número de pessoa conhecida	Procure o contato anterior ou outro familiar.
Conta diferente da relação habitual	Confirme o beneficiário antes da operação.
Pedido de senha ou código	Não entregue; procure o serviço oficial.
Suposta conta para proteger saldo	Interrompa e consulte seu banco.
Programa para resolver problema bancário	Não instale por orientação do contato.
Taxa inesperada para liberar valor	Confira obrigação e emissor na fonte legítima.
Comprovante como condição de entrega	Consulte o próprio extrato ou sistema.
Devolução para conta de terceiro	Verifique o recebimento e fale com seu banco.
Recuperação garantida mediante taxa	Não pague; verifique a oferta por conta própria.

Se já realizou a ação, utilize o Apêndice A. A preservação de uma mensagem não exige manter a conversa ou seguir novas instruções do suspeito.

Fonte: síntese editorial dos capítulos 2 a 8.

APÊNDICE C

Registro inicial do incidente

Uso reservado à organização do relato e do atendimento. Não substitui boletim de ocorrência nem formulário da instituição financeira. Não anote senhas, códigos de autenticação ou número completo de cartão.

Pessoa que organiza o relato e data

Como começou e o que foi solicitado

O que foi feito e quando o problema foi percebido

Operação	Data e horário conhecidos	Valor e referência do comprovante

Acessos ou informações compartilhados

Arquivos disponíveis e onde foram conservados

Instituições contatadas, protocolos e pendências

Separe dúvida, informação recebida e fato observado. Guarde este registro em local protegido; não o publique em redes sociais.

Referências

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Golpes atuais mais comuns.**

Brasília, DF: Anatel, 2026. Publicada em 3 abr. 2023; atualizada em 30 abr. 2026.

Disponível em:

<https://www.gov.br/anatel/pt-br/assuntos/dicas-contras-fraudes/golpes-atuais-mais-comuns>. Acesso em: 25 ago. 2026.

BANCO CENTRAL DO BRASIL. **O que é e como funciona o Mecanismo Especial de Devolução (MED).** Brasília, DF: BCB, 2026a. Atualizada em 18 set. 2026. Disponível

em: <https://bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-mecanismo-especial-de-devolucao-med>. Acesso em: 24 set. 2026.

BANCO CENTRAL DO BRASIL. **Perguntas e respostas: golpes.** Brasília, DF: BCB, 2026b. Conjunto de respostas com atualizações próprias. Disponível em:

<https://www.bcb.gov.br/meubc/faqs/s/golpes>. Acesso em: 31 ago. 2026.

BANCO CENTRAL DO BRASIL. **Segurança no Pix.** Brasília, DF: BCB, [2026?].c. Página institucional consultada em sua versão disponível. Disponível em:

<https://www.bcb.gov.br/estabilidadefinanceira/pix-seguranca>. Acesso em: 27 set. 2026.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.**

Brasília, DF: Câmara dos Deputados, 1988. Texto atualizado. Disponível em:

<https://www2.camara.leg.br/legin/fed/consti/1988/constitucao-1988-5-outubro-1988-322142-normaatuizada-pl.html>. Acesso em: 18 out. 2026.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Câmara dos Deputados, 1940. Texto atualizado. Disponível em:

<https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-normaatuizada-pe.html>. Acesso em: 28 jun. 2026.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal.

Brasília, DF: Câmara dos Deputados, 1941. Texto atualizado. Disponível em:

<https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-3689-3-outubro-1941-322206-normaatuizada-pe.html>. Acesso em: 8 ago. 2026.

BRASIL. **Lei Complementar nº 105, de 10 de janeiro de 2001.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília, DF:

Câmara dos Deputados, 2001. Texto atualizado. Disponível em:

<https://www2.camara.leg.br/legin/fed/leicom/2001/leicomplementar-105-10-janeiro-2001-355754-normaatualizada-pl.html>. Acesso em: 11 ago. 2026.

BRASIL. **Lei nº 12.830, de 20 de junho de 2013**. Dispõe sobre a investigação criminal conduzida pelo delegado de polícia. Brasília, DF: Câmara dos Deputados, 2013. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2013/lei-12830-20-junho-2013-776286-publicacaooriginal-140173-pl.html>. Acesso em: 2 jun. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Câmara dos Deputados, 2014. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2014/lei-12965-23-abril-2014-778630-normaatualizada-pl.html>. Acesso em: 27 out. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Câmara dos Deputados, 2018. Texto atualizado. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-normaatualizada-pl.html>. Acesso em: 20 ago. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. **Consumidor.gov.br: saiba como registrar uma reclamação pela plataforma**. Brasília, DF: MJSP, 2026. Publicada em 10 jul. 2026; atualizada em 26 out. 2026. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/consumidor-gov-br-saiba-como-registrar-uma-reclamacao-pela-plataforma>. Acesso em: 30 out. 2026.

CERT.br. **Banco via internet**. [S. l.]: NIC.br, abr. 2023a. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/banco-via-internet/fasciculo-banco-via-internet.pdf>. Acesso em: 9 jul. 2026.

CERT.br. **Comércio via internet**. [S. l.]: NIC.br, nov. 2023b. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/comercio-via-internet/fasciculo-comercio-via-internet.pdf>. Acesso em: 3 out. 2026.

CERT.br. **Golpes: caiu? Veja o que fazer**. [S. l.]: NIC.br, maio 2026a. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/golpes-o-que-fazer/fasciculo-golpes-o-que-fazer.pdf>. Acesso em: 12 jun. 2026.

CERT.br. **Golpes: evite fraudes**. [S. l.]: NIC.br, mar. 2026b. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/golpes-evite-fraudes/fasciculo-golpes-evite-fraudes.pdf>. Acesso em: 9 out. 2026.

CERT.br. **Golpes: não se deixe enganar**. [S. l.]: NIC.br, mar. 2026c. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/golpes/fasciculo-golpes.pdf>. Acesso em: 17 out. 2026.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais**. 1. ed. Salvador: Juspodivm, 2027. ISBN 9788544277386.

ORDEM DOS ADVOGADOS DO BRASIL. Conselho Federal. **ConfirmADV**. [S. l.]: OAB, [2025?]. Mecanismo auxiliar de consulta profissional. Disponível em: <https://confirmadv.oab.org.br/>. Acesso em: 23 jun. 2026.

ORDEM DOS ADVOGADOS DO BRASIL. Seção do Paraná. **Golpe do falso advogado**. [S. l.]: OAB-PR, [2026?]. Página de orientação com ações de 2026. Disponível em: <https://portal.oabpr.org.br/golpe-do-falso-advogado>. Acesso em: 19 set. 2026.

Minicurrículo do autor

HIGOR VINICIUS NOGUEIRA JORGE

Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor, escritor e pesquisador nas áreas de Direito, tecnologia, investigação criminal e inteligência cibernética. Autor e coordenador de mais de 80 obras jurídicas publicadas, integra o Conselho de Direito Digital, Transformação e Novas Tecnologias da Editora Juspodivm.

Mestre em Educação pela Universidade Estadual de Mato Grosso do Sul (UEMS) e graduado em Direito pelo Centro Universitário Toledo de Araçatuba (UniToledo/SP), é professor concursado da Academia de Polícia Dr. Coriolano Nogueira Cobra (Acadepol/SP). Possui pós-graduações em Polícia Comunitária (Unisul), Repressão e Prevenção à Corrupção (Faculdade Estácio), VANTs e Drones: Legislação, Planejamento e Aplicações (Uniminas), Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais (Uniminas) e Investigação Digital (WB Educação).

Sua atuação acadêmica compreende o ensino, a pesquisa e a produção de conhecimento nas áreas de investigação criminal tecnológica, direito digital, crimes cibernéticos, inteligência cibernética, prova digital e aplicação de novas tecnologias à segurança pública. Além de sua atividade docente na Acadepol/SP, ministra aulas de inteligência cibernética no âmbito do Ministério da Justiça e Segurança Pública (MJSP). Também atuou em cursos de pós-graduação e programas de formação especializada de instituições como a Escola Brasileira de Direito (EBRADI), o Complexo de Ensino Renato Saraiva (CERS), a Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP), a Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), a Escola Mineira de Direito (EMD), o Damásio Educacional, a Verbo Jurídico, o MeuCurso, a WB Educação e a Associação dos Diplomados da Escola Superior de Guerra (ADESG, Campinas).

Em 2015, desenvolveu a disciplina Investigação Criminal Tecnológica, concebida como uma proposta teórico-metodológica voltada à aplicação sistemática, juridicamente fundamentada e tecnicamente controlada de recursos tecnológicos à investigação criminal. Diferentemente da investigação

de crimes cibernéticos, cujo objeto está relacionado às infrações penais praticadas no ambiente digital ou mediante o emprego de tecnologias, a Investigação Criminal Tecnológica possui abrangência transversal, aplicando-se à apuração de delitos de qualquer natureza. Sua abordagem compreende a identificação, a preservação, a obtenção, o tratamento, a correlação, a interpretação e a apresentação de vestígios informacionais relevantes à persecução penal, com observância das garantias fundamentais, dos requisitos de validade probatória e da cadeia de custódia.

Integra a Associação Internacional de Informática Forense (ASIIF) e a Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA). É titular da Cadeira nº 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e Diretor de Relações Institucionais da Associação dos Delegados de Polícia do Estado de São Paulo (ADPESP), na gestão 2024-2026.

Entre 2017 e 2026, recebeu, em dez edições consecutivas, reconhecimento na categoria Jurídica do levantamento Melhores Delegados de Polícia do Brasil, promovido pelo Portal Nacional dos Delegados e pela Revista da Defesa Social.

Para aprofundar o estudo

Investigação criminal tecnológica

Fundamentos, método e limites na era dos vestígios informacionais

Higor Vinicius Nogueira Jorge. Salvador: Editora Juspodivm, 1ª edição, ano editorial 2027. ISBN 9788544277386.

O livro apresenta a Investigação Criminal Tecnológica como disciplina de abrangência transversal, aplicável à apuração de crimes de qualquer natureza. Desenvolve o vestígio informacional juridicamente relevante como objeto de estudo, o método em sete fases (identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação) e o Controle de Viés Investigativo, além de examinar prova digital, fontes abertas, inteligência artificial, inteligência criminal, drones, fraudes, dados em nuvem, cooperação jurídica internacional e governança.

Esta cartilha é um material educativo gratuito, escrito para aproximar esses fundamentos da prática. O livro é uma publicação comercial da Editora Juspodivm, indicada a quem deseja aprofundar o estudo.

Conheça o livro no site da editora: editorajuspodivm.com.br

A coleção

A Coleção Investigação e Proteção na Era Digital reúne oito cartilhas gratuitas sobre investigação criminal, prova digital, uso responsável da tecnologia e proteção de pessoas e famílias no ambiente digital. Todos os volumes estão disponíveis em www.higorjorge.com.br, em formato PDF.

- Vol. 01** **Investigação Criminal Tecnológica.** Fundamentos, métodos e aplicações práticas
- Vol. 02** **Provas digitais e cadeia de custódia.** Da coleta à valoração jurídica
- Vol. 03** **Inteligência artificial na investigação criminal.** Aplicações, limites e boas práticas
- Vol. 04** **Golpes digitais e fraudes eletrônicas.** Prevenção, identificação e investigação (este volume)
- Vol. 05** **Investigação de crimes na internet.** Dados, registros, sigilos e medidas judiciais
- Vol. 06** **Raciocínio investigativo e decisão fundamentada.** Do indício ao relatório final
- Vol. 07** **Internet segura.** Guia prático para proteger você e sua família
- Vol. 08** **Crianças e adolescentes na internet.** Guia de proteção para pais e responsáveis

Canais oficiais do autor

- Site** www.higorjorge.com.br
- YouTube** youtube.com/@direitoetecnologia
- Instagram** [@higorjorge](https://www.instagram.com/higorjorge)
- Facebook** facebook.com/professorhigorjorge