MESSIAS COSTA

O MUNDO DOS Ggolpes

COMO ELES FUNCIONAM,
POR QUE AINDA FUNCIONAM
E O QUE VOCÊ PODE FAZER
PARA SE PROTEGER

COMPREENDER
RECONHECER
CONFERIR
EVITAR
REAGIR



INFORMAÇÃO,
CONSCIÊNCIA E DECISÃO
EM UM MUNDO REAL

APRESENTAÇÃO

Golpes costumam ser apresentados como uma coleção de histórias extraordinárias: o falso banco, o falso profissional, o investimento irresistível, o parente que pede dinheiro, a mensagem urgente, o perfil clonado. Os nomes mudam, as plataformas mudam e as tecnologias mudam. O problema é que decorar essas modalidades não basta.

Este livro parte de uma ideia mais útil: **para se proteger melhor, é preciso compreender o que existe por trás do golpe.** Antes da internet, do telefone e dos bancos modernos, pessoas já manipulavam pesos, moedas, documentos, identidades e relações de confiança para obter vantagem. A tecnologia ampliou velocidade, alcance e capacidade de imitação, mas não criou o engano.

Por isso, *O Mundo dos Golpes* não foi construído como um catálogo de fraudes. As situações concretas aparecem para revelar mecanismos que se repetem: criação de credibilidade, exploração da confiança, uso de autoridade, medo, esperança, afeto, oportunidade e pressão para levar alguém a agir antes de conferir.

Isso também significa abandonar uma ideia confortável: a de que somente pessoas ingênuas caem em golpes. Conhecimento ajuda, experiência ajuda e cautela ajuda, mas ninguém toma todas as decisões nas mesmas condições. Cansaço, urgência, preocupação, familiaridade, contexto e informações verdadeiras misturadas a uma história falsa podem tornar plausível algo que, visto depois com calma, pareceria evidente.

O objetivo destas páginas não é ensinar você a desconfiar de tudo. A confiança é necessária para a vida. O objetivo é aprender **quando a confiança precisa ser acompanhada de verificação.**

Ao longo do livro, veremos como os golpes se constroem, por que continuam funcionando, como se transformaram em atividade de grande escala e como seus mecanismos aparecem em situações financeiras, profissionais, afetivas e digitais. Depois, passaremos àquilo que mais importa na prática: reconhecer sinais de risco, interromper a pressão, conferir fora da história apresentada, proteger-se antes que o problema aconteça e reagir quando a fraude já ocorreu.

COMPREENDER → RECONHECER → CONFERIR → EVITAR → REAGIR

Esse é o caminho deste livro.

Primeiro, compreenderemos por que o golpe acompanha a própria história da confiança e por que pessoas inteligentes, experientes e cuidadosas também podem ser atingidas. Em seguida, veremos como uma fraude constrói credibilidade, manipula a percepção, cria pressão e procura transformar uma narrativa em ação.

Depois, observaremos esses mecanismos em diferentes ambientes: dinheiro, identidade, oportunidades, relações afetivas, redes sociais, meios digitais e tecnologias capazes de tornar imagens, vozes e mensagens cada vez mais convincentes. O foco não estará em memorizar nomes, mas em reconhecer padrões.

A partir daí, a leitura se transforma em decisão prática. Você aprenderá a parar antes de agir, identificar o que está sendo pedido, conferir a situação por um caminho independente e decidir somente depois da verificação.

E, se o golpe já tiver acontecido, o livro seguirá adiante. Interromper o dano, proteger dinheiro, contas e dispositivos, preservar provas, comunicar quem precisa ser comunicado, conhecer caminhos possíveis e evitar uma segunda fraude fazem parte da mesma preparação.

Nenhum método elimina completamente o risco. Novas fraudes continuarão surgindo, novas tecnologias serão exploradas e histórias diferentes continuarão sendo construídas para pessoas diferentes. É justamente por isso que a proteção mais duradoura não está em conhecer todos os golpes que existem.

Está em desenvolver uma forma melhor de olhar para aquilo que parece verdadeiro.

Ao final, a proposta é simples: que você dependa menos de reconhecer o nome de um golpe e esteja mais preparado para perceber o mecanismo, interromper a pressão, conferir a realidade e decidir com mais segurança.

Porque o próximo golpe talvez ainda não tenha nome. Mas os princípios que ajudam a reconhecê-lo podem ser aprendidos antes que ele apareça.



MESSIAS COSTA

ADVOGADO

www.messiascosta.adv.br

SOBRE O AUTOR

Messias Costa é advogado e atua na área empresarial, reunindo formação jurídica e experiência em gestão de negócios.

Graduado em Direito pela Universidade Federal de Mato Grosso — UFMT, em 1997, é inscrito na Ordem dos Advogados do Brasil, Seccional de Mato Grosso, sob o nº 9.437.

Possui MBA em Gestão Empresarial pela Fundação Getulio Vargas — FGV e pós-graduação em Direito Empresarial, Direito Tributário, Direito Ambiental e Direito do Trabalho.

Sua formação multidisciplinar e sua atuação profissional aproximam o Direito de situações concretas em que informação, confiança, decisão e responsabilidade produzem consequências relevantes para pessoas e organizações.

Em O Mundo dos Golpes, essa perspectiva é direcionada à compreensão das fraudes e dos mecanismos que as tornam convincentes, com o propósito de ajudar o leitor a reconhecer situações de risco, conferir informações, reduzir vulnerabilidades e reagir de forma mais segura quando o golpe já ocorreu.

DISTRIBUIÇÃO GRATUITA

Esta obra é disponibilizada gratuitamente. É permitida sua reprodução e compartilhamento, por qualquer meio, desde que o conteúdo seja mantido integralmente, sem alterações, e sejam preservados o nome do autor e os créditos da obra. É vedada a comercialização desta obra sem autorização do autor.

CARTILHA GRATUITA

Acesse a cartilha e a página do projeto
messiascosta.adv.br/omundodosgolpes

SUMÁRIO

CAPÍTULO 1 — UMA HISTÓRIA TÃO ANTIGA QUANTO A CONFIANÇA 8

1.1. Antes da internet, antes do telefone, antes dos bancos
1.2. O golpe muda com o mundo
1.3. O que permanece

CAPÍTULO 2 — NINGUÉM ESTÁ IMUNE 18

2.1. O mito da vítima ingênua
2.2. Vulnerabilidade é circunstancial
2.3. A pessoa certa no momento certo
2.4. Conhecimento protege, mas não produz imunidade

CAPÍTULO 3 — COMO FUNCIONA UM GOLPE 28

3.1. Mais do que uma mentira
3.2. Da abordagem à confiança
3.3. Os mecanismos da manipulação
3.4. A pressa é inimiga da verificação
3.5. O momento da ação
3.6. A estrutura do golpe

CAPÍTULO 4 — A INDÚSTRIA DOS GOLPES 40

4.1. Um problema em grande escala
4.2. Do improviso à especialização
4.3. Quando aplicar golpes vira atividade organizada
4.4. Informação como matéria-prima
4.5. Escala, tecnologia e fronteiras
4.6. Do rudimentar ao sofisticado

CAPÍTULO 5 — QUANDO O ALVO É O SEU DINHEIRO 43

5.1. A aparência de uma operação legítima
5.2. Bancos, Pix, transferências e cartões
5.3. Boletos, cobranças, empréstimos e crédito
5.4. Investimentos e promessas de retorno

CAPÍTULO 6 — QUANDO O GOLPISTA SE TORNA ALGUÉM EM QUEM VOCÊ CONFIA 51

6.1. O novo número e a personificação
6.2. Quando alguém fala em nome de um banco, empresa ou autoridade
6.3. O falso profissional
6.4. Informações verdadeiras a serviço de uma identidade falsa
6.5. Quando a identidade roubada é a sua

CAPÍTULO 7 — OPORTUNIDADES BOAS DEMAIS 60

7.1. Comprar, vender e negociar
7.2. Emprego e renda
7.3. Negócios e bens de maior valor
7.4. Prêmios, vantagens e dinheiro inesperado

CAPÍTULO 8 — QUANDO O GOLPE EXPLORA SENTIMENTOS 68

8.1. Afeto e relacionamento
8.2. A falsa emergência com alguém amado
8.3. Solidariedade e compaixão
8.4. Medo, ameaça, vergonha e segredo
8.5. A dificuldade de admitir o engano

CAPÍTULO 9 — QUANDO JÁ NÃO PODEMOS CONFIAR NO QUE VEMOS E OUVIMOS 75

9.1. A fraude digital
9.2. Redes sociais e exposição
9.3. Inteligência artificial e conteúdo sintético
9.4. A crise da evidência aparente
9.5. A tecnologia também protege

CAPÍTULO 10 — PARE, CONFIRA, DEPOIS DECIDA 83

10.1. Reconheça a situação de risco
10.2. Interrompa o roteiro
10.3. Verifique fora da história
10.4. Proteja antes de precisar
10.5. Um método para o golpe que ainda não existe

CAPÍTULO 11 — CAÍ NO Ggolpe. E AGORA? 91

11.1. Interrompa o dano
11.2. Proteja dinheiro, contas e dispositivos
11.3. Preserve provas
11.4. Comunique e registre
11.5. Tente recuperar
11.6. Não caia no segundo golpe
11.7. Protocolo imediato

CAPÍTULO 12 — DEPOIS DO GOLPE: DIREITOS, RESPONSABILIDADES E CAMINHOS 100

12.1. As repercussões depois da fraude
12.2. Quem pode ser responsável
12.3. Relações bancárias, financeiras e de consumo
12.4. Caminhos extrajudiciais e judiciais
12.5. Quando procurar orientação jurídica

CAPÍTULO 13 — PROTEÇÃO TAMBÉM SE COMPARTILHA 107

13.1. Pessoas diferentes, riscos diferentes
13.2. Conversar sem humilhar
13.3. Protocolos familiares simples
13.4. Quando alguém próximo caiu
13.5. Empresas também precisam de protocolos

CAPÍTULO 14 — O PRÓXIMO GOLPE 115

14.1. O futuro que ainda não conhecemos
14.2. Por que listas envelhecem
14.3. O que permanece quando o golpe muda
14.4. O que deve permanecer com você

REFERÊNCIAS BIBLIOGRÁFICAS 123

“A fraude constrói confiança nas pequenas coisas para, quando valer a pena, enganar com grande proveito.”

TITO LÍVIO

Ab Urbe Condita, livro XXVIII, 42.7

CAPÍTULO 1

UMA HISTÓRIA TÃO ANTIGA QUANTO A CONFIANÇA

1.1. Antes da internet, antes do telefone, antes dos bancos

Uma pequena moeda conservada no British Museum traz, de um lado, a figura de Vulcano; do outro, uma águia. O catálogo a identifica como uma falsificação antiga do período republicano romano: uma moeda revestida de prata.[1] Ela chegou até nós como objeto de museu. Quando foi produzida, porém, imitava algo destinado a circular, ser reconhecido e aceito.

Não sabemos, a partir desse registro, quem a fabricou, quem a recebeu ou se alguém percebeu o engano antes de concluir uma troca. Inventar uma conversa entre vendedor e comprador tornaria o episódio mais movimentado, mas esconderia o que o objeto permite observar com segurança. A falsificação procurava reproduzir uma aparência reconhecível. A diferença entre aquilo que parecia ser e aquilo que efetivamente era já podia interessar a quem pretendia obter vantagem.

Esse pequeno objeto desloca o começo da nossa história. O golpe não nasceu com a mensagem de celular, o cartão ou a transferência instantânea. A possibilidade de fazer alguém aceitar uma aparência enganosa existia muito antes. Não dependia de conexão, tela nem senha. Podia estar no próprio objeto que mudava de mãos.

Para perceber o problema, imagine uma negociação hipotética muito simples. Duas pessoas combinam a entrega de uma quantidade de mercadoria em troca de um pagamento. Quem compra precisa avaliar o produto; quem vende precisa avaliar o que recebe. Se a mercadoria foi adulterada ou o pagamento imita um valor que não possui, a troca deixa de corresponder ao acordo. Uma das partes toma sua decisão com base em uma informação materialmente falsa.

Há duas dificuldades diferentes nessa cena. Uma é saber o que foi prometido. A outra é descobrir se aquilo que foi entregue corresponde à promessa. Mesmo quando todos conhecem as condições da negociação, pode haver uma distância entre o que os olhos reconhecem e o que uma conferência mais cuidadosa revelaria.

Outro vestígio antigo mostra como é importante examinar essa distância sem afirmar mais do que o documento permite. Uma tabuinha de argila preserva uma reclamação de Nanni dirigida a Ea-nasir. O catálogo do British Museum descreve uma queixa sobre a qualidade do cobre entregue e problemas relacionados a outra entrega.[2] Temos, portanto, um registro de insatisfação comercial. Isso não equivale, por si só, a uma decisão que tenha demonstrado a intenção de fraudar.

Uma reclamação documenta aquilo que alguém contestou. Uma falsificação material documenta outra coisa. A distinção parece pequena, mas evita que toda disputa antiga seja transformada em golpe apenas porque a história fica mais atraente. Um produto inadequado pode resultar de engano deliberado, erro, descumprimento ou divergência sobre o que foi contratado. Para escolher entre essas explicações, precisamos de evidências.

Essa cautela acompanhará o livro. Não é necessário chamar alguém de fraudador para reconhecer um problema de confiança. Também não é necessário encontrar “o primeiro golpe da história” para demonstrar que a falsificação antecede as tecnologias modernas. A moeda romana já fornece uma evidência material; o registro comercial acrescenta outra perspectiva sobre a preocupação com o que se promete e o que se entrega.

Os textos antigos também registraram esse interesse pela aparência dos objetos. No livro XXXVII de sua História natural, Plínio, o Velho, trata de pedras preciosas e menciona imitações em vidro e formas de adulteração.[3] Seu texto é testemunho de uma preocupação antiga com autenticidade. Não precisamos adotar suas explicações sobre minerais nem converter seus procedimentos em recomendações atuais. O que importa aqui é a presença documentada do problema: algo menos valioso podia ser apresentado sob a aparência daquilo que o comprador procurava.

Uma imitação, naturalmente, não é necessariamente uma fraude. Uma peça vendida como imitação pode cumprir exatamente o que foi oferecido. O engano aparece quando se oculta a diferença relevante e se conduz outra pessoa a decidir como se estivesse diante do original. O mesmo objeto pode participar de uma venda transparente ou de uma negociação enganosa, conforme a informação prestada e a maneira como é apresentado.

Essa diferença ajuda a localizar o centro do fenômeno. Não está simplesmente na existência de objetos parecidos. Está na utilização da semelhança para produzir uma conclusão falsa. Uma pessoa não compra apenas uma cor ou um brilho: compra aquilo que acredita que esses sinais representam.

Pense em duas etiquetas hipotéticas. Uma identifica uma peça como adorno de vidro. A outra a apresenta como pedra rara e cobra por essa condição. Mesmo que as peças sejam visualmente idênticas, a decisão do comprador é diferente. No segundo caso, ele pode aceitar um preço ou uma finalidade que recusaria se conhecesse a composição verdadeira. A informação escondida não é detalhe; participa do motivo pelo qual ele entrega seu dinheiro.

Mercadorias, pesos, medidas, moedas e documentos oferecem diferentes pontos de apoio para esse tipo de engano. O objeto pode não ter a qualidade anunciada; a quantidade pode não corresponder à unidade combinada; um sinal de autoridade pode não ter a origem que aparenta. Essas são possibilidades de construção da fraude, não uma afirmação de que toda sociedade ou toda troca tenha funcionado da mesma maneira.

Não precisamos desconfiar retrospectivamente de todo comércio para compreender por que a confiança é importante. Ao contrário: a fraude só faz sentido em um mundo no qual as pessoas normalmente procuram atribuir significado aos sinais que encontram. Um nome identifica alguém. Uma medida organiza uma quantidade. Uma moeda permite reconhecer um valor. Um documento registra uma informação. A vida prática depende dessas correspondências.

Se cada troca exigisse descobrir tudo novamente, negociar se tornaria muito mais difícil. Confiamos em procedimentos, referências e conhecimentos que não produzimos sozinhos. O problema surge quando alguém utiliza essa organização da vida comum para apresentar uma coisa como se fosse outra.

Os vestígios antigos permitem, assim, uma primeira mudança de perspectiva. A tecnologia pode alterar o instrumento, mas não é condição necessária para que exista engano. Uma mensagem falsa pode fazer algo semelhante: oferecer sinais que sustentem uma conclusão diferente da realidade.

1.2. O golpe muda com o mundo

Agora substitua a moeda por um documento. Depois, substitua o documento entregue pessoalmente por uma correspondência. Em cada mudança, parte da avaliação passa a depender de novos sinais. A pessoa pode reconhecer uma assinatura, um nome, uma aparência oficial ou uma referência conhecida sem encontrar quem produziu aquilo.

Esse deslocamento permite entender a adaptação dos golpes sem construir uma cronologia de todas as fraudes. Os meios usados para negociar e comunicar também são os meios pelos quais uma informação enganosa pode chegar. Quando um procedimento se torna familiar, sua aparência passa a ter valor para quem pretende imitá-lo.

A correspondência oferece um exemplo claro. Receber uma carta não comprova, por si só, a identidade de quem a assina. O envelope entrega uma mensagem; não resolve automaticamente a veracidade de seu conteúdo. Uma cobrança pode mencionar uma obrigação

existente e, ainda assim, indicar um destinatário indevido. Uma oferta pode descrever um serviço real e mentir sobre a participação de quem a envia. A existência do canal e a autenticidade da proposta são questões diferentes.

Isso não torna a carta suspeita por natureza. Mostra apenas que o meio de transporte da informação não pode garantir tudo o que ela afirma. A mesma distinção será necessária diante de mensagens digitais, páginas de internet e conversas por aplicativos.

No início do século XX, Charles Ponzi associou uma promessa de rendimento a cupons postais. O FBI registra que ele prometia retorno de 50% e que, embora os primeiros participantes recebessem pagamentos, o esquema acabou sem condições de pagar quem entrou depois.[4] O episódio é importante aqui pela combinação entre uma referência concreta — os cupons — e uma promessa financeira. A existência do objeto mencionado não demonstrava que a atividade oferecida produzisse os resultados anunciados.

É possível compreender o limite dessa evidência sem reconstruir toda a operação. Mostrar que determinado instrumento existe responde a uma pergunta. Demonstrar que uma proposta baseada nele é verdadeira responde a outra. Entre as duas coisas há um caminho que a pessoa interessada talvez não consiga observar apenas pela apresentação recebida.

Considere uma comparação hipotética. Alguém apresenta uma fotografia de uma fazenda para oferecer participação em uma produção agrícola. A fotografia pode ser autêntica e a fazenda pode existir. Isso ainda não demonstra que o anunciante seja proprietário, tenha autorização para captar recursos ou destine o dinheiro à atividade descrita. Um fragmento verdadeiro não confirma, sozinho, a relação que a proposta estabelece entre as partes.

O desenvolvimento dos meios de comunicação tornou possível sustentar relações a distâncias cada vez maiores. Em uma conversa telefônica, a resposta imediata acrescenta algo que uma carta não oferece: a sensação de estar tratando diretamente com alguém que compreende o problema. Mas conversar em tempo real também não

encerra a questão da identidade. Uma pessoa pode responder às perguntas e ainda representar um papel falso.

Na situação presencial, o interlocutor podia ser avaliado por gestos, aparência e documentos. No telefone, parte dessa avaliação recai sobre voz, vocabulário e conhecimento do assunto. Em uma página digital, entram em cena organização visual, textos, imagens e funcionamento aparente. O que muda é o conjunto de sinais disponível; permanece necessário perguntar o que eles realmente demonstram.

Cartões, computadores e serviços pela internet acrescentam outra mudança: a informação pode permitir uma ação. Uma sequência de dados não serve apenas para contar uma história sobre alguém. Dependendo do serviço e dos controles existentes, pode participar da identificação, da autorização ou do acesso a uma conta. Por isso, o objetivo de uma abordagem pode ser obter uma informação antes de buscar diretamente dinheiro.

Não se deve imaginar, entretanto, que todo golpe digital depende de invadir um sistema. Uma instrução enganosa pode levar o próprio usuário a realizar uma operação. O procedimento pode funcionar conforme foi projetado, enquanto a pessoa se engana sobre a finalidade do que está fazendo. Essa diferença será desenvolvida adiante, porque altera a maneira de reconhecer o risco.

Uma comparação hipotética ajuda. Uma pessoa entrega dinheiro porque acredita estar pagando uma compra; outra autoriza um pagamento eletrônico pelo mesmo motivo. Se a compra é fictícia, o problema comum não está no papel-moeda ou na tela. Está na justificativa que fez o pagamento parecer adequado. Os instrumentos exigem cuidados próprios, mas trocar um pelo outro não elimina a necessidade de conferir a negociação.

As redes sociais acrescentaram sinais de familiaridade à comunicação distante. Uma fotografia, um nome e referências a interesses ou relações podem fazer um contato parecer conhecido. Esses elementos também podem circular separados de seu contexto original. Encontrar uma imagem que você reconhece não é o mesmo que confirmar quem controla a conta que a apresenta.

Em um pagamento que se conclui imediatamente, a conferência precisa acompanhar esse ritmo. Pense em uma transferência hipotética: se a pessoa confirma primeiro e só depois examina o destinatário, sua dúvida aparece quando a operação já foi realizada. A conveniência da rapidez permanece; o cuidado precisa entrar antes da confirmação.

A inteligência artificial amplia novamente o conjunto de aparências disponíveis. Em alerta de dezembro de 2024, o FBI descreveu o uso de conteúdo gerado por IA em fraudes, incluindo textos, imagens, áudios e vídeos. O documento menciona, entre outras possibilidades, mensagens de voz destinadas a imitar familiares e conteúdo utilizado para dar credibilidade a identidades falsas.[5] O alerta não significa que qualquer áudio seja manipulado nem fornece motivo para tratar toda comunicação digital como fraude. Demonstra que determinados sinais podem ser produzidos de maneira diferente daquela que o destinatário imagina.

A consequência dessa passagem histórica não é que a fraude tenha seguido uma escada simples, do rudimentar ao perfeito. Uma falsidade pouco elaborada e uma apresentação sofisticada podem coexistir. Tampouco uma ferramenta nova elimina as anteriores. Uma conversa comum pode sustentar uma fraude mesmo em um ambiente repleto de recursos tecnológicos.

Essas mudanças exigem rever o que cada sinal permite confirmar. Houve situações em que a pessoa precisava avaliar uma mercadoria diante dos olhos. Em outras, precisava confiar no relato de alguém distante. Hoje, pode receber uma combinação de texto, imagem, voz, documento e pedido de pagamento em um único aparelho. A quantidade de sinais aumentou, mas sinais que dependem da mesma origem não se transformam automaticamente em confirmações independentes.

1.3. O que permanece

Uma moeda revestida, uma promessa financeira e uma voz imitada não são o mesmo tipo de fraude. Exigem conhecimentos diferentes e podem produzir consequências distintas. Aproximá-las só é útil se a comparação revelar alguma coisa além da constatação de que pessoas mentem.

O ponto comum está na decisão que a aparência procura sustentar. Aceitar o objeto como autêntico, acreditar na proposta ou reconhecer uma identidade pode abrir caminho para uma ação. Não basta perguntar se uma história parece convincente. É preciso perceber o que se pretende obter quando você aceita essa história.

Imagine, em um exemplo hipotético, que alguém mostre um documento e diga precisar de ajuda. O documento pode chamar sua atenção, mas o risco concreto dependerá do pedido: informar um endereço público, entregar uma cópia de documento pessoal, transferir dinheiro ou permitir acesso a uma conta são ações muito diferentes. A análise da aparência precisa ser acompanhada da análise da consequência.

Algumas histórias oferecem uma vantagem. Outras anunciam uma perda que precisa ser evitada. Há as que se apoiam em uma relação de afeto e as que recorrem à autoridade de uma instituição. O objetivo pode ser fazer a pessoa ajudar, obedecer, corrigir um problema ou aproveitar uma oportunidade. Esses elementos não são defeitos humanos. São partes reconhecíveis da maneira como lidamos com outras pessoas e com as necessidades da vida.

Você pode desejar que um familiar esteja seguro, que seu dinheiro seja protegido ou que uma oportunidade de trabalho seja verdadeira. Nada disso constitui, por si só, falta de discernimento. A questão é saber se a situação apresentada corresponde ao que afirma e se a ação solicitada realmente atende ao objetivo declarado.

Um exemplo hipotético permite separar as duas coisas. Receber um pedido de ajuda de alguém próximo pode justificar atenção imediata. Não demonstra, porém, que o pagamento indicado seja necessário, que

a conta informada pertença ao destinatário legítimo ou que o interlocutor seja quem diz ser. A disposição de ajudar e a necessidade de confirmar podem existir ao mesmo tempo.

Da mesma forma, reconhecer o nome de uma instituição pode tornar um contato relevante. Não obriga a aceitar todas as instruções atribuídas a ela. A confiança depositada na instituição não se transfere automaticamente a qualquer pessoa que utilize seu nome.

Medo, esperança, autoridade, afeto e expectativa de vantagem aparecerão muitas vezes nesta obra. Serão examinados como elementos que podem participar de situações de engano, não como comandos infalíveis sobre o comportamento. Pessoas respondem de formas diferentes; uma história fracassa diante de alguém e parece plausível a outra pessoa. A presença de emoção não prova fraude, assim como a ausência de agitação não prova segurança.

A urgência merece desde já uma observação. Quando uma proposta não admite tempo para confirmar um elemento relevante, a decisão fica dependente do que está sendo apresentado naquele contato. O problema não é simplesmente a rapidez. Uma emergência verdadeira pode exigir rapidez. O ponto é perceber se a ação solicitada ajuda a enfrentar a situação ou apenas impede que sua versão seja examinada fora da conversa.

Ao olhar para golpes antigos, seria fácil imaginar que hoje temos informação suficiente para não repetir erros semelhantes. Mas informação disponível e informação verificada não são a mesma coisa. Um documento pode ser encontrado; sua origem, não conferida. Um nome pode ser conhecido; sua ligação com o pedido, presumida. Uma explicação pode ser detalhada e ainda esconder justamente a parte necessária para avaliar a proposta.

Por isso, conhecer histórias de fraude deve servir para desenvolver julgamento. Memorizar um roteiro oferece ajuda quando a próxima situação se parece com ele. Compreender a relação entre aparência, pedido e consequência permite fazer perguntas úteis mesmo quando o cenário é novo.

Isso não exige transformar a vida em investigação permanente. As verificações precisam acompanhar a relevância da decisão. Escolher uma conversa não é o mesmo que entregar credenciais; ouvir uma oferta não é o mesmo que comprometer uma reserva financeira. À medida que a ação se torna mais difícil de desfazer ou pode afetar outras pessoas, aumenta a importância de confirmar os elementos dos quais ela depende.

A história não ensina que confiar foi um erro e continuará sendo. Ensina que a confiança pode ser explorada e, em determinadas decisões, precisa de apoio. O caminho da proteção não está em abandonar relações, comércio ou tecnologia, mas em reconhecer o momento em que uma aparência ainda não basta.

Se esse problema atravessa instrumentos tão diferentes, a pergunta seguinte é inevitável: por que uma história falsa continua encontrando espaço entre aquilo que sabemos e aquilo que decidimos fazer?

CAPÍTULO 2

NINGUÉM ESTÁ IMUNE

2.1. O mito da vítima ingênua

Imagine uma pessoa que recebe uma mensagem sobre uma encomenda. Ela não comprou nada, não espera nenhuma entrega e apaga o aviso. Mais tarde, comenta que seria impossível acreditar naquela história. Para ela, naquele momento, o primeiro elemento da mensagem já não fazia sentido.

Agora imagine outra pessoa recebendo o mesmo texto enquanto aguarda um produto necessário para trabalhar. A compra existe, a entrega está atrasada e ela já tentou saber o que aconteceu. O aviso encontra uma preocupação concreta. Isso não significa que ela vá pagar uma cobrança ou abrir um endereço recebido. Significa que a mensagem começa em condições diferentes.

Nenhuma dessas cenas descreve um caso real. A comparação serve para mostrar um problema na maneira como julgamos os golpes: muitas vezes comparamos pessoas quando deveríamos também comparar as situações nas quais elas decidiram. Recusar uma história incompatível com sua vida não demonstra que você identificaria todas as histórias compatíveis com ela.

É confortável imaginar que a vítima pertence a um grupo distante. Se o engano exige pouca inteligência, basta considerar-se inteligente. Se exige desconhecimento de tecnologia, basta saber utilizar o aparelho. Se exige ambição, basta acreditar que seus desejos são

moderados. A explicação parece oferecer uma proteção pessoal, mas não examina o que ocorreu.

Saber operar uma conta, por exemplo, é diferente de confirmar a identidade de alguém que pede uma operação. Conhecer um produto é diferente de verificar se o vendedor tem condições de entregá-lo. Entender o significado de um documento não demonstra que a cópia recebida veio de quem aparenta tê-la emitido. A competência pode ser verdadeira e ainda não responder à pergunta decisiva daquela situação.

Uma revisão sistemática sobre a psicologia da vitimização por fraudes na internet analisou fatores relacionados à mensagem, à experiência e às características das pessoas. Os pesquisadores também ressaltaram limitações importantes da evidência disponível para explicar processos específicos de vulnerabilidade.[6] Esse resultado recomenda prudência diante de explicações que pretendem identificar, em uma única característica, por que alguém foi enganado.

Não decorre daí que conhecimento, experiência e cautela sejam inúteis. Decorre que não devem ser tratados como certificados de imunidade. Uma pessoa pode reconhecer um risco com facilidade e desconhecer outro. Pode dominar uma atividade e precisar de ajuda em uma decisão diferente. Pode conhecer o sinal de alerta, mas não identificá-lo sob a forma em que aparece.

Também é preciso separar ser exposto a uma tentativa, interagir com ela e perder dinheiro. Receber uma mensagem não é cair em um golpe. Responder não significa necessariamente concluir a ação desejada pelo fraudador. E uma perda financeira não é a única consequência possível: a entrega de informações ou o acesso indevido a uma conta podem ter relevância própria.

Essa separação muda a pergunta dirigida à vítima. Em vez de procurar o instante em que ela “deveria ter sabido”, podemos examinar o caminho: o que chegou, o que foi interpretado, o que foi conferido e qual ação aconteceu. O exame deixa de funcionar como julgamento de caráter e passa a ajudar a reconhecer pontos de interrupção.

Dados de reclamações também exigem cuidado antes de virar rótulo. Ao analisar os relatos de 2024 recebidos pela Consumer Sentinel Network, nos Estados Unidos, a FTC observou que adultos mais velhos relataram perda de dinheiro em proporção menor do que adultos mais jovens, embora as perdas medianas individuais fossem maiores entre os mais velhos. A própria instituição apontou explicações possíveis relacionadas tanto à prevenção quanto à disposição de comunicar tentativas sem prejuízo.[7] Isso não mede a probabilidade de cada brasileiro sofrer fraude. Mostra por que uma comparação simples entre idades pode esconder fenômenos diferentes.

O mesmo cuidado vale para histórias de pessoas com formação elevada que foram enganadas. Um caso desses pode contrariar a afirmação absoluta de que “pessoas instruídas nunca caem”. Não permite concluir que formação aumenta o risco, que todos estão expostos da mesma forma ou que qualquer pessoa cairia naquele roteiro. A evidência tem um alcance; o comentário não deve ultrapassá-lo.

Abandonar o mito da vítima ingênua não é aceitar que nada possa ser feito. É substituir uma proteção imaginária — acreditar que o problema pertence aos outros — por uma pergunta que permite agir: em quais circunstâncias eu também poderia aceitar uma explicação antes de conferir o necessário?

2.2. A vulnerabilidade não está apenas na pessoa

Uma decisão não acontece fora da vida. Há uma tarefa em andamento, um horário, uma expectativa, pessoas esperando uma resposta. Você pode receber o contato enquanto trabalha, se desloca, acompanha um familiar ou tenta resolver uma dificuldade. Esses elementos não determinam o resultado, mas fazem parte das condições nas quais a mensagem será avaliada.

Chamaremos de vulnerabilidade circunstancial essa combinação entre pessoa, momento e situação. Não é um diagnóstico nem uma

classificação permanente. É uma forma de lembrar que a avaliação do risco precisa incluir mais do que idade, profissão ou escolaridade.

Considere uma cobrança hipotética que chega durante uma viagem. O destinatário encontra uma informação incomum, mas está com pouco tempo e não dispõe dos documentos que costuma consultar. Pode adiar a decisão, buscar ajuda ou conferir por outro meio. Também pode concluir que é melhor resolver imediatamente para não carregar o problema. O que importa observar é a condição concreta: a dificuldade de verificar entrou na decisão.

Compare esse cenário com o da mesma pessoa em casa, diante dos documentos e sem compromisso imediato. Não é necessário afirmar que o cansaço ou a pressa "desligam a razão". Basta reconhecer que as oportunidades de conferir são diferentes. A prevenção precisa funcionar também quando o ambiente não é o ideal.

Há situações em que o obstáculo é emocional. Em outro exemplo hipotético, alguém espera notícias de um familiar e recebe uma comunicação alarmante. Antes de descobrir se ela é verdadeira, já existe um problema a ser esclarecido. A preocupação pode tornar o contato relevante, mesmo para uma pessoa normalmente cautelosa. Essa relevância não comprova a história; explica por que ela merece atenção.

A esperança também pode participar da avaliação. Quem busca emprego tem motivos para abrir uma comunicação sobre seleção. Quem enfrenta uma dívida pode querer conhecer uma possibilidade de negociação. Quem precisa vender um bem tem razões para responder a um interessado. O interesse não é uma falha. A dificuldade está em distinguir a necessidade verdadeira da solução que apenas se apresenta como verdadeira.

É importante não transformar essas observações em explicações prontas para qualquer vítima. Não sabemos que alguém respondeu "porque estava sozinho" apenas porque mora sozinho. Não sabemos que uma perda decorreu de distração apenas porque a pessoa tinha uma rotina intensa. Uma circunstância pode ser relevante sem ser a causa demonstrada de um episódio.

O estudo Exposed to Scams, conduzido por instituições ligadas à educação financeira e à pesquisa, examinou pessoas que haviam comunicado tentativas de fraude, comparando experiências com e sem perda. A pesquisa encontrou pouca ou nenhuma diferença por escolaridade nas taxas de envolvimento e vitimização de sua amostra. Seu desenho também distingue o contato inicial da perda efetiva.[8] Como pesquisa realizada em um universo específico de relatos, não oferece uma previsão individual nem uma taxa aplicável a qualquer população.

Para o leitor, o uso mais produtivo dessa perspectiva é examinar condições que podem ser modificadas. Se a informação necessária não está disponível, a decisão pode precisar esperar. Se a emoção é intensa, outra pessoa pode ajudar a separar o que foi confirmado do que foi apenas anunciado. Se a operação envolve um recurso importante, sua conferência não precisa depender da memória de um procedimento pouco utilizado.

Não se trata de pedir que você esteja sempre descansado, atento e sereno. Essa exigência seria pouco útil: a vida não organiza os contatos suspeitos para os nossos melhores horários. Trata-se de reconhecer que uma proteção baseada somente em “eu vou perceber” pode falhar justamente quando a atenção precisa ser dividida.

Há diferença entre uma regra que depende do humor do dia e uma decisão previamente combinada. Imagine uma pessoa que só confere o destinatário quando a cobrança parece estranha. Agora imagine que ela decidiu conferir o destinatário de pagamentos relevantes antes de confirmá-los. No segundo caso, não é necessário sentir desconfiança para começar a verificação. O procedimento pode entrar na rotina sem um julgamento imediato sobre a honestidade de quem enviou a cobrança.

Os procedimentos concretos serão organizados adiante. Aqui importa compreender por que eles são úteis: retiram parte da proteção do campo da autoconfiança e a colocam em ações observáveis. Você não precisa saber se é uma pessoa difícil de enganar para confirmar um elemento relevante antes de agir.

2.3. A pessoa certa no momento certo

Uma história não precisa convencer todo mundo para produzir uma vítima. Basta encontrar alguém para quem seus elementos pareçam fazer sentido. Às vezes isso depende de informações específicas. Em outras situações, o contato só coincide com uma experiência comum.

Retome a mensagem de entrega do início do capítulo. Para ser relevante, ela não precisa necessariamente conter uma investigação detalhada sobre o destinatário. Muitas pessoas compram produtos e aguardam encomendas. Uma comunicação distribuída de forma ampla pode chegar a alguém que esteja justamente tentando resolver uma entrega. A coincidência não prova que o remetente conhecia a compra.

Essa observação evita atribuir ao golpista poderes que ele talvez não tenha. Uma mensagem que coincide com um problema pode parecer pessoal mesmo quando foi enviada sem conhecimento daquele problema. A pessoa destinatária acrescenta o contexto que já possui e conecta os pontos. O aviso menciona entrega; ela pensa na compra atrasada. A ligação entre os dois fatos ainda precisa ser confirmada.

Em uma abordagem direcionada, a situação é diferente. O contato pode incorporar dados específicos, como informações sobre uma atividade profissional ou uma negociação anunciada. Nesse caso, a plausibilidade recebe apoio de elementos reais. Ainda assim, conhecer o contexto não demonstra autorização para agir dentro dele.

Imagine, como exemplo, alguém que anunciou um automóvel. Receber mensagens de compradores é esperado. A pessoa não precisa considerar suspeito todo desconhecido que pergunta pelo veículo; foi justamente para encontrar interessados que publicou o anúncio. O cuidado aparece quando a negociação passa a exigir uma ação diferente da conversa: entregar documentos, aceitar um comprovante ou transferir algum valor.

O anúncio explica por que houve contato. Não valida automaticamente o que o contato pede depois. Essa distinção permite

preservar a utilidade da negociação sem conferir ao primeiro elemento plausível o poder de justificar todo o restante.

Outro exemplo hipotético envolve uma seleção de trabalho. Uma pessoa envia currículos e recebe notícia de uma entrevista. O tema corresponde ao que ela procura. Mas o reconhecimento desse tema não responde se a empresa existe, se a pessoa representa a empresa ou se a exigência recebida faz parte de um procedimento legítimo. A expectativa tornou o contato relevante; não concluiu sua verificação.

É possível, portanto, que a mesma mensagem produza avaliações muito distintas. Uma pessoa a ignora porque não precisa do serviço. Outra pede informações. Uma terceira reconhece uma incoerência. Uma quarta pode avançar sem confirmar. Essas possibilidades mostram caminhos de decisão, não tipos fixos de personalidade.

A comparação também permite perceber por que o comentário “eu jamais acreditaria nisso” tem alcance limitado. Talvez você realmente não acreditasse naquela versão, naquele contexto. A conclusão útil seria identificar o elemento que a tornaria incoerente para você. Isso ensina mais do que transformar sua reação imaginada em uma característica permanente.

Uma pessoa pode ser especialmente cuidadosa com propostas de investimento e tratar uma solicitação de trabalho como parte da rotina. Outra pode conferir toda compra, mas aceitar com menos perguntas um pedido atribuído a um familiar. Uma terceira pode reconhecer ameaças grosseiras e ainda ter dúvidas diante de uma comunicação educada e detalhada. Não é preciso escolher qual delas seria “mais inteligente”. As decisões envolvem referências diferentes.

Essa é a razão para procurar conhecimento transferível. Um roteiro conhecido pode não coincidir com a próxima tentativa. A pergunta sobre o que está sendo solicitado, o que foi efetivamente confirmado e por que seria necessário agir agora pode acompanhar a mudança de cenário.

O contexto importa também depois da primeira resposta. Uma abordagem inicialmente vaga pode receber informações durante a conversa. Você explica o atraso, menciona uma dificuldade ou

descreve a providência que já tentou. Isso não significa que qualquer pergunta seja maliciosa. Significa que o conhecimento demonstrado mais tarde pode ter sido fornecido no próprio contato, em vez de existir antes dele.

Ao avaliar uma situação, vale distinguir a informação que o interlocutor trouxe da informação que você entregou. É uma diferença pequena, mas ajuda a evitar que a repetição de seus próprios dados seja interpretada como confirmação independente.

2.4. Conhecimento protege, mas não torna invulnerável

O objetivo deste livro não é oferecer uma promessa de que você nunca mais poderá ser enganado. Uma promessa assim exigiria conhecer todas as situações futuras, todos os recursos utilizados e todas as condições em que uma decisão será tomada. O objetivo é mais concreto: aumentar sua capacidade de perceber o risco, verificar o que importa e interromper uma ação antes que ela produza dano.

Isso pode acontecer em momentos diferentes. Você pode reconhecer um sinal antes de responder. Pode perceber uma inconsistência durante a conversa. Pode interromper quando surge uma exigência inesperada. Se a fraude já ocorreu, pode evitar novas ações e procurar os caminhos adequados de reação. A proteção não se resume a uma única oportunidade de acertar.

Também não depende de aprender todos os detalhes técnicos de cada serviço. Entender uma ferramenta pode ajudar, mas há perguntas que continuam necessárias mesmo quando seu funcionamento é conhecido. Quem pediu a operação? O que ela fará? Qual elemento confirma que atende à finalidade anunciada? O conhecimento técnico não substitui essas perguntas; pode ajudar a respondê-las.

Uma pessoa que reconheceu corretamente uma tentativa deve aproveitar a experiência sem transformá-la em garantia para a próxima. O que funcionou? O pedido era incompatível com uma informação conhecida? A confirmação veio de outro canal? Houve

tempo para consultar alguém? Identificar a ação protetiva permite repeti-la. Apenas concluir “sou atento” não mostra o que repetir.

O mesmo raciocínio vale quando houve prejuízo. Em vez de reduzir o episódio à frase “fui ingênuo”, é possível reconstruir os elementos relevantes: a abordagem encontrou uma necessidade? Uma informação verdadeira pareceu confirmar toda a história? A decisão foi tomada antes de uma conferência? Essas perguntas não transferem ao fraudador menos responsabilidade. Ajudam a descobrir como impedir a continuidade ou a repetição do processo.

O respeito à vítima tem, portanto, uma função prática. Se a conversa sobre golpes só admite vergonha, o relato de uma dúvida pode ser adiado. Um ambiente em que é possível dizer “não sei se isso é verdadeiro” oferece espaço para examinar a situação antes de agir. Não precisamos transformar essa observação em promessa psicológica para reconhecer seu valor cotidiano.

Conhecimento e procedimento cumprem funções complementares. O conhecimento ajuda a entender por que algo merece atenção. O procedimento organiza o que fazer quando a atenção é necessária. Uma verificação simples e previamente conhecida pode ser mais utilizável do que uma longa explicação lembrada apenas depois do problema.

Haverá ocasiões em que a conferência confirmará a legitimidade do contato. Esse também é um resultado útil. Prevenção não significa rejeitar automaticamente o que chega; significa criar condições melhores para aceitar ou recusar. A confiança pode continuar depois da confirmação, sem que a dúvida inicial tenha sido ofensa a ninguém.

Você não precisa escolher entre acreditar em tudo e viver em permanente suspeita. Pode reconhecer seus conhecimentos, admitir o que ainda não foi verificado e ajustar o cuidado à consequência da decisão. Essa posição permite aprender sem se considerar incapaz e agir com segurança sem se considerar imune.

Se a vulnerabilidade depende também do encontro entre pessoa, momento e situação, a próxima pergunta já não é apenas quem pode

cair. É o que acontece dentro desse encontro: como um contato ganha credibilidade e se transforma em uma ação favorável a quem engana.

CAPÍTULO 3

COMO FUNCIONA UM GOLPE

3.1 Mais do que uma mentira

Uma mensagem chega dizendo que houve uma compra suspeita no seu cartão. O número parece de uma central de atendimento. A pessoa do outro lado conhece seu nome, menciona o banco correto e informa parte de um dado que você reconhece. Em seguida, explica que é preciso “cancelar a operação” e orienta uma sequência de passos. Até esse ponto, talvez nenhuma frase isolada pareça extraordinária. O golpe começa a revelar sua estrutura quando toda a história passa a conduzir você a uma ação que beneficia quem está do outro lado.

Essa é uma diferença importante. Mentir e aplicar um golpe não são exatamente a mesma coisa. Uma falsidade pode existir sem produzir qualquer consequência prática. No golpe, a falsidade é organizada para alterar a percepção de uma situação e induzir uma decisão: pagar, transferir, entregar, informar, instalar, autorizar, assinar, permitir acesso ou assumir algum compromisso. O engano tem uma finalidade.

Por isso, muitas fraudes não dependem de uma mentira única e espetacular. Elas podem combinar informações verdadeiras, elementos plausíveis e uma ou duas falsidades decisivas. O nome do banco pode estar correto. A existência de uma encomenda pode ser real. Um processo judicial pode de fato existir. A fotografia pode ser autêntica. O documento pode reproduzir dados verdadeiros. O

problema está na relação construída entre esses elementos e na conclusão para a qual a pessoa é conduzida.

Imagine uma situação hipotética. Você recebe uma mensagem sobre uma compra que realmente fez no dia anterior. A mensagem informa corretamente o nome da loja e o valor aproximado. Depois afirma que houve um problema na confirmação do pagamento e fornece um link para "regularizar" a operação. Os primeiros dados verdadeiros tornam a explicação mais plausível, mas não demonstram que quem enviou a mensagem seja a loja nem que o link pertença a ela. O golpe pode se apoiar justamente no que é verdadeiro para tornar convincente aquilo que precisa permanecer falso.

Esse processo pode durar segundos ou meses. Em uma fraude rápida, o intervalo entre contato e ação é mínimo: uma cobrança, um código, um Pix, um clique. Em outras, a construção é lenta. A pessoa pode conversar durante semanas, acompanhar supostos resultados, receber documentos, participar de grupos ou desenvolver um vínculo antes de ser convidada a agir. O tempo muda, mas a pergunta central permanece: que realidade está sendo apresentada e qual comportamento ela pretende produzir?

A pesquisa sobre vitimização por fraudes na internet mostra que não há uma explicação psicológica única e simples para a adesão a golpes; diferentes estudos encontram combinações de fatores ligados à mensagem, ao contexto e às características individuais, com limitações importantes.[6] Isso é útil porque impede uma conclusão sedutora, mas errada: a de que existe um "botão" que, apertado corretamente, faz qualquer pessoa obedecer. O que existe são condições que podem tornar uma história mais convincente ou uma decisão menos cuidadosa.

Olhar para o golpe como processo muda a forma de se proteger. Em vez de perguntar apenas "isto é mentira?", você passa a observar a sequência. Como esse contato surgiu? O que está sendo usado para parecer legítimo? Que emoção ou expectativa está sendo acionada? Existe pressão para decidir? O que exatamente querem que eu faça? Essa mudança de perspectiva será a base dos capítulos seguintes.

3.2 Da abordagem à confiança

Todo golpe precisa chegar à vítima de algum modo. O contato pode ocorrer por mensagem, ligação, e-mail, anúncio, rede social, aplicativo, correspondência, encontro presencial ou por uma combinação desses meios. Pode ser distribuído para milhares de pessoas sem qualquer conhecimento prévio sobre elas ou construído com informações específicas de uma pessoa, de uma empresa ou de uma situação real.

Na abordagem massificada, o fraudador não precisa saber previamente quem está esperando uma encomenda, quem possui conta em determinado banco ou quem procura emprego. Basta enviar a mesma história a muita gente. Para parte dos destinatários, ela não fará sentido e será ignorada. Para alguns, porém, coincidirá com uma circunstância verdadeira. A pessoa que realmente aguarda uma entrega pode interpretar uma falsa cobrança como continuação natural daquela compra. Quem acabou de enviar currículos pode considerar plausível o contato de um suposto recrutador. A coincidência faz parte da credibilidade percebida, mesmo sem qualquer seleção individual anterior.

Em abordagens direcionadas, a história pode chegar acompanhada de informações mais específicas: nome, profissão, parentes, empresa, fornecedor, banco, cargo, fotografia, número de processo, produto anunciado ou algum acontecimento recente. A personalização não precisa ser perfeita. Às vezes, alguns dados corretos são suficientes para reduzir a dúvida inicial e fazer a conversa avançar.

É nesse ponto que aparência e confirmação precisam ser separadas. Credibilidade é a impressão de que algo merece confiança. Verificação é o processo de confirmar, por evidência adequada e independente, que a pessoa, instituição, conta, documento ou pedido é realmente aquilo que afirma ser. Uma história pode parecer muito credível e continuar falsa.

O CERT.br alerta que golpes combinam engenharia social e recursos técnicos para levar pessoas a fornecer informações ou seguir passos que facilitam a fraude. O material também destaca que mensagens podem explorar temas cotidianos, sentimentos, urgência e aparência

de legitimidade.[10] A utilidade dessa observação não está em transformar qualquer comunicação persuasiva em fraude, mas em lembrar que sinais familiares podem ser fabricados ou apropriados.

Considere outro exemplo hipotético. Um fornecedor habitual de uma pequena empresa envia mensalmente a mesma cobrança. Certo dia chega uma mensagem com o nome correto do fornecedor, a identificação do contrato e uma explicação sobre mudança de conta bancária. O documento está bem apresentado e o texto usa a linguagem habitual do negócio. Nada disso, isoladamente, confirma que a mudança tenha sido solicitada pelo fornecedor real. Quanto mais importante for a alteração, mais necessário se torna confirmá-la por um canal que não dependa da própria mensagem recebida.

O mesmo vale para autoridade aparente. Uniforme, logotipo, número de protocolo, linguagem técnica, fotografia profissional, assinatura, endereço de e-mail semelhante ao verdadeiro e conhecimento de procedimentos internos podem aumentar a sensação de legitimidade. Alguns desses elementos podem ser autênticos; outros, copiados; outros, apenas visualmente parecidos. A função deles dentro do golpe é diminuir a necessidade sentida de perguntar “quem é você?” e deslocar a atenção para “o que preciso fazer agora?”.

Essa mudança é decisiva. Quando a identidade parece resolvida, a pessoa tende a concentrar-se no problema apresentado: a compra suspeita, a dívida, a emergência, a oportunidade, o bloqueio, a vaga, o prêmio. O fraudador não precisa provar tudo. Precisa construir credibilidade suficiente para que a conversa continue até a etapa seguinte.

Por isso, informação verdadeira não comprova identidade. Esse princípio já apareceu na obra e aqui ganha função dentro do processo: dados corretos podem ser parte da credibilidade construída, mas a confirmação de quem está do outro lado exige um caminho independente quando a decisão envolve dinheiro, dados, acesso ou outra consequência relevante.

3.3 Os mecanismos da manipulação

Depois que a abordagem parece plausível, o golpe precisa produzir movimento. A pessoa precisa fazer algo. É aí que entram mecanismos que não pertencem exclusivamente ao mundo das fraudes. Autoridade, confiança, medo, urgência, afeto, solidariedade, oportunidade, expectativa de ganho, curiosidade, vergonha e segredo também fazem parte de relações legítimas. Um médico pode transmitir autoridade real; uma emergência pode ser verdadeira; uma promoção pode ser autêntica; alguém próximo pode realmente precisar de ajuda. O risco aparece quando esses elementos são usados para orientar a decisão sem permitir a verificação necessária.

A autoridade é um exemplo claro. Em muitas situações sociais, é racional dar peso adicional à orientação de quem ocupa determinada função. O problema surge quando a função é apenas representada. Uma voz segura, um vocabulário técnico e a afirmação “sou do setor de segurança” podem criar uma relação hierárquica que nunca existiu. Estudos experimentais com mensagens de phishing encontraram efeitos relevantes de apelos de autoridade sobre a avaliação de mensagens, embora os resultados variem conforme desenho, contexto e tipo de estímulo. Em um estudo de 2025 com 200 participantes, mensagens com apelo de autoridade estiveram associadas a menor capacidade de distinguir mensagens fraudulentas das legítimas, enquanto outros princípios produziram efeitos diferentes.[9] A conclusão prudente é que autoridade pode influenciar a avaliação; não que funcione sempre ou da mesma forma para todas as pessoas.

O medo opera por outra via. A história apresenta uma perda que precisa ser evitada: sua conta será bloqueada, alguém querido está em perigo, uma dívida produzirá consequência imediata, uma informação será exposta. O ponto prático não é discutir se o medo “desliga” a razão. É observar que uma ameaça pode deslocar a prioridade da pessoa para a solução mais rápida do problema apresentado. Se o mesmo interlocutor que anuncia o perigo também oferece o único caminho para resolvê-lo, a situação merece verificação adicional.

O afeto e a solidariedade exploram algo diferente: a disposição legítima de ajudar. Um pedido atribuído a um filho, amigo ou parceiro pode parecer menos uma operação financeira e mais um dever relacional. A pessoa não pensa apenas em dinheiro; pensa em não abandonar alguém. O mesmo ocorre com campanhas e histórias de sofrimento. A proteção não exige eliminar a compaixão. Exige separar a vontade de ajudar da confirmação de quem está pedindo e de onde o auxílio realmente chegará.

A oportunidade e a expectativa de ganho podem reduzir a disposição de esperar. Uma oferta com grande vantagem, uma vaga excepcional, um investimento aparentemente promissor ou um prêmio inesperado cria uma tensão simples: se eu demorar, posso perder. O mecanismo não depende de ganância. Pode envolver necessidade de renda, desejo de economizar, expectativa profissional ou interesse legítimo em aproveitar uma boa oportunidade. Quanto mais a vantagem depender de decisão imediata, mais importante se torna criar espaço para conferir.

A curiosidade também pode abrir a porta. Uma mensagem sobre uma fotografia, uma suposta denúncia, um documento, uma encomenda ou um acontecimento envolvendo a própria pessoa pode provocar o impulso de clicar ou responder antes de avaliar a origem. O conteúdo não precisa ser assustador nem vantajoso; basta ser suficientemente relevante para vencer a hesitação inicial.

Vergonha e segredo podem atuar de modo ainda mais silencioso. Uma história pode exigir confidencialidade: “não fale com ninguém porque estamos investigando”, “não avise o fornecedor”, “não conte à família”, “esta condição é exclusiva”. Em outras situações, a própria vítima pode sentir constrangimento em consultar alguém porque já avançou na conversa, forneceu informação ou assumiu um compromisso. O efeito prático é semelhante: diminui a possibilidade de uma segunda pessoa observar a situação com distância.

Esses mecanismos podem aparecer combinados. Uma falsa autoridade pode anunciar um risco, impor urgência e exigir segredo. Uma relação afetiva pode criar confiança, introduzir uma emergência e depois pedir dinheiro. Uma oportunidade pode vir acompanhada de

prova social, escassez e promessa de retorno. A combinação é importante porque explica por que procurar um único “sinal clássico” nem sempre funciona.

Também é importante não inverter o raciocínio. Urgência não prova fraude. Autoridade não prova fraude. Emoção não prova fraude. Segredo pode ser legítimo em determinadas situações. O que esses elementos fazem é alterar o nível de atenção que uma decisão merece. Quando vários aparecem ao mesmo tempo e culminam em pedido de dinheiro, dados, código, acesso ou mudança de procedimento, a necessidade de verificação cresce.

O objetivo, portanto, não é decorar uma lista de técnicas de persuasão. É perceber quando a conversa está tentando transformar uma emoção, uma relação ou uma posição de autoridade em justificativa suficiente para agir. A pergunta prática continua simples: o que querem que eu faça antes que eu tenha tempo ou condições de conferir?

3.4 Pressa é inimiga da verificação

Muitas fraudes têm pressa porque a verificação cria risco para o fraudador. Se a pessoa encerra a ligação e telefona para o número oficial, conversa com um familiar, consulta o aplicativo verdadeiro, procura o fornecedor conhecido ou simplesmente espera alguns minutos, a história pode perder consistência. O tempo não garante segurança, mas abre espaço para comparar informações e buscar uma fonte que não esteja sob controle de quem fez a abordagem.

É por isso que a pressão temporal merece atenção especial. O Banco Central, ao orientar usuários do Pix, recomenda conferir os dados antes de confirmar operações e alerta para urgência, pressão e promessas de vantagens como estratégias que podem induzir decisões rápidas.[11] O CERT.br, em material de orientação sobre phishing e outros golpes, também inclui senso de urgência, ameaças, apelos emocionais e pedidos de sigilo entre os sinais que justificam cautela.[10]

A pesquisa experimental, porém, aconselha precisão. Estudos sobre phishing não mostram uma regra universal segundo a qual toda

pressão de tempo produz automaticamente mais erro. Em experimentos diferentes, os efeitos variam. No estudo de Auton e Sturman, participantes submetidos a menor pressão de tempo distinguiram melhor mensagens fraudulentas e legítimas, mas a interação entre tempo e os diferentes princípios de persuasão não foi significativa.[9] Isso reforça uma ideia mais útil do que qualquer slogan: tempo adicional pode favorecer avaliação, mas não transforma sozinho uma decisão em decisão correta.

Na vida cotidiana, a pressão pode ser explícita: “faça agora”, “você tem cinco minutos”, “a oferta termina hoje”, “não desligue”. Pode também ser construída pela própria história: alguém querido estaria em perigo; uma conta estaria sob ataque; um documento venceria; um negócio dependeria de resposta imediata. Nesses casos, a urgência parece pertencer ao problema, e não ao interlocutor. É justamente por isso que pode ser convincente.

Urgências legítimas existem. Um cartão perdido precisa ser bloqueado. Uma pessoa pode realmente precisar de socorro. Uma oportunidade comercial pode ter prazo. A diferença não está na presença da pressa, mas no que acontece quando você tenta verificar. Uma instituição legítima pode ter procedimentos para confirmação. Uma pessoa conhecida pode ser contatada por outro meio. Um fornecedor real pode confirmar uma mudança. Quando a história exige que toda verificação ocorra apenas pelos canais fornecidos por quem está pressionando, a cautela deve aumentar.

Criar tempo é, portanto, uma forma de recuperar autonomia. Pode significar dizer que retornará depois, encerrar a ligação, não clicar imediatamente, não concluir o pagamento enquanto fala com alguém, ou simplesmente deixar a decisão para depois de uma conferência independente. Não é necessário confrontar o interlocutor nem demonstrar que você descobriu um golpe. O objetivo é sair do ritmo imposto.

Essa pausa tem outra função: permitir que a pergunta correta apareça. Sob pressão, a atenção tende a ficar presa ao problema apresentado — “como impedir o bloqueio?”, “como ajudar meu filho?”, “como não perder a vaga?”. Ao interromper o roteiro, torna-se possível

perguntar: “quem confirmou que esse problema existe?”, “por que esta solução precisa ser feita deste modo?”, “posso verificar por um canal que eu mesmo procurei?”.

O método completo de decisão será desenvolvido mais adiante. Por enquanto, basta guardar uma regra: quando alguém tenta reduzir o tempo disponível para conferir uma decisão relevante, aumentar o tempo é uma resposta defensiva simples. A pressa pode ser legítima; a verificação também.

3.5 O momento da ação

Toda a construção anterior converge para algum comportamento. Esse é o ponto em que a análise do golpe fica especialmente concreta. Em vez de tentar adivinhar intenções, observe o pedido.

Pode ser dinheiro: fazer um Pix, uma transferência, pagar um boleto, comprar um vale, autorizar uma cobrança. Pode ser informação: fornecer senha, código de autenticação, dados de cartão, documento, fotografia, endereço, informações sobre a empresa. Pode ser acesso: instalar um aplicativo, compartilhar a tela, permitir controle remoto, aprovar um novo dispositivo, clicar em um link e entrar em uma conta. Pode ser uma decisão jurídica ou comercial: assinar, alterar dados bancários, aceitar uma proposta, entregar um bem, enviar mercadoria, mudar um procedimento.

O objetivo imediato nem sempre é o objetivo final. Um código pode permitir acesso posterior. Um documento pode ser usado em outra etapa. Uma conversa aparentemente sem pedido financeiro pode coletar informações que tornarão a abordagem seguinte mais convincente. Uma pequena transferência pode funcionar como início de uma relação que depois exigirá valores maiores. Isso não significa que toda solicitação de dados seja parte de uma fraude em várias fases. Significa apenas que “não pediram dinheiro” não é sinônimo de “não há risco”.

Aqui surge uma pergunta que vale para modalidades muito diferentes: o que estão tentando me fazer fazer?

Ela é útil porque desloca a atenção da história para a consequência. Uma narrativa pode ser complexa, técnica e difícil de avaliar. O pedido costuma ser mais simples. Se alguém afirma que sua conta está em risco, o que pede em seguida? Se diz ser um familiar, para onde quer que o dinheiro seja enviado? Se oferece uma vaga, por que precisa de pagamento ou de determinados dados? Se anuncia um prêmio, por que a liberação depende de uma transferência? Se se apresenta como profissional, qual ação deseja que você pratique e como essa ação pode ser confirmada fora da conversa?

Nem toda ação tem o mesmo risco. Informar um dado já público não é igual a fornecer uma senha. Abrir uma página institucional conhecida não é igual a instalar um programa indicado por um desconhecido. Pagar uma pequena compra por um meio com mecanismos de contestação não é igual a transferir grande valor para uma conta recém-informada. A proteção exige proporcionalidade: quanto maior a consequência potencial e mais difícil a reversão, maior deve ser a qualidade da confirmação.

Isso também ajuda a identificar o ponto de interrupção. Um golpe pode ter avançado bastante sem que o dano principal tenha ocorrido. Você pode ter respondido mensagens, acreditado parcialmente na história ou até fornecido alguma informação e ainda assim conseguir parar antes da ação decisiva. A ideia de que “já fui longe demais” é perigosa. Cada nova solicitação pode ser reavaliada.

Por isso, o momento da ação não deve ser tratado apenas como o final do golpe. Ele é também uma oportunidade de defesa. Antes de qualquer comportamento que entregue valor, informação sensível, acesso ou controle, a história precisa suportar uma pergunta independente: eu confirmei que essa ação é necessária, que o destinatário é correto e que o canal utilizado é legítimo?

3.6 A estrutura do golpe

Podemos agora organizar o que foi visto em um modelo simples:

CONTATO CREDIBILIDADE MANIPULAÇÃO PRESSÃO AÇÃO VANTAGEM

O contato coloca a história em movimento. A credibilidade faz com que ela pareça suficientemente possível para continuar. A manipulação utiliza motivações, relações, emoções ou expectativas que dão força à narrativa. A pressão reduz o espaço para dúvida e verificação. A ação é o comportamento que transfere dinheiro, informação, acesso, controle ou outra vantagem. A vantagem é aquilo que o fraudador obtém direta ou indiretamente.

O modelo não é uma definição rígida nem um roteiro que todo golpe precisa seguir. As etapas podem se sobrepor. Algumas podem quase desaparecer. Em uma fraude muito rápida, contato, credibilidade e pressão cabem em poucas linhas de uma mensagem. Em uma fraude construída ao longo do tempo, a credibilidade pode ser cultivada durante semanas e a pressão surgir apenas no momento do pedido. Há golpes em que a vantagem financeira é imediata e outros em que a primeira ação apenas prepara uma etapa posterior.

Imagine três situações hipotéticas.

Na primeira, chega uma mensagem atribuída a um familiar dizendo que mudou de número. Esse é o contato. A fotografia e o modo de falar fornecem credibilidade. A relação afetiva cria a base de manipulação. Surge uma conta que precisa ser paga imediatamente: pressão. A pessoa faz a transferência: ação. O dinheiro recebido é a vantagem.

Na segunda, uma empresa recebe uma comunicação aparentemente enviada por fornecedor conhecido. O documento usa dados corretos e informa mudança de conta bancária. O contato e a credibilidade praticamente se confundem. Não há ameaça nem forte apelo emocional; a manipulação está na normalidade aparente do procedimento. A pressão pode ser apenas o vencimento próximo. A ação é pagar para a nova conta. A vantagem é o desvio do valor.

Na terceira, alguém encontra uma oportunidade de investimento anunciada na internet. O primeiro contato parte da própria vítima ao pedir informações. A credibilidade é construída por aparência

profissional, documentos e supostos resultados. A expectativa de ganho sustenta o envolvimento. A pressão pode aparecer gradualmente, com condições que parecem temporárias ou exigências para liberar valores. A ação ocorre em sucessivos aportes. A vantagem pode crescer ao longo do tempo.

As três histórias são diferentes, e é justamente essa diferença que torna o modelo útil. Ele não serve para dizer que todos os golpes são iguais. Serve para fazer perguntas semelhantes diante de aparências diferentes.

Onde começou o contato? O que produziu credibilidade? Que elemento está influenciando minha decisão? Existe pressão para impedir ou reduzir a conferência? Qual ação está sendo pedida? Quem se beneficia se eu a realizar?

Essas perguntas não transformam qualquer situação incomum em fraude. Elas organizam a observação. Em vez de depender do reconhecimento de um nome — "golpe do falso parente", "golpe da falsa central", "golpe do investimento" —, você passa a enxergar a arquitetura que pode existir por trás de histórias novas.

Esse é o modelo mental que o restante do livro utilizará. Nos próximos capítulos, confiança, autoridade, urgência, medo, afeto, oportunidade e os demais mecanismos não precisarão ser reapresentados como teoria a cada vez. Eles aparecerão em funcionamento, combinados de maneiras diferentes. O objetivo será reconhecer o processo enquanto ele acontece.

Compreender a estrutura, porém, abre uma questão maior. Se um roteiro convincente pode ser repetido, adaptado e distribuído por meios digitais, o golpe deixa de ser apenas um encontro entre um fraudador e uma vítima. Ele pode ganhar volume, especialização, infraestrutura e alcance. É esse salto de escala que precisamos observar a seguir.

CAPÍTULO 4

A INDÚSTRIA DOS GOLPES

4.1 Um problema em grande escala

A fraude contemporânea não pode ser entendida apenas como o ato improvisado de um indivíduo. Há campanhas capazes de alcançar milhares de pessoas, infraestrutura para registrar domínios, disparar mensagens, movimentar dinheiro e reutilizar dados. Em 2025, a FTC recebeu cerca de 3 milhões de relatos de fraude nos Estados Unidos, com perdas reportadas de US$ 15,9 bilhões; golpes de impostores foram os mais frequentemente relatados.[7] Os números são de um sistema específico e não medem toda a fraude mundial, mas ajudam a dimensionar a escala.

4.2 Do improviso à especialização

A mesma operação pode envolver funções diferentes: quem obtém dados, quem prepara páginas falsas, quem aborda vítimas, quem recebe valores e quem tenta afastar o dinheiro da conta de origem. A especialização reduz a necessidade de que uma única pessoa domine todo o processo.

Isso também explica por que alguns golpes parecem profissionais. Texto bem escrito, atendimento rápido e documentos convincentes não demonstram legitimidade; podem ser resultado de repetição, treinamento e divisão de tarefas.

4.3 Quando aplicar golpes vira atividade organizada

Órgãos internacionais têm documentado ecossistemas de fraude digital associados a redes criminosas transnacionais, inclusive operações com recrutamento, lavagem de dinheiro e exploração de trabalhadores.[13,14] A existência dessas estruturas não significa que todo golpe pertença ao crime organizado. Significa que o leitor deve abandonar a imagem única do “malandro solitário”.

A escala permite testar histórias, selecionar vítimas responsivas e repetir o que funciona. O golpe passa a ter algo de processo produtivo: abordagem, triagem, convencimento, pagamento e dispersão dos recursos.

4.4 Informação como matéria-prima

Dados tornam uma mentira específica. Nome, profissão, parentesco, processo, compra recente ou fotografia podem ser usados para criar contexto. Parte dessas informações é pública; parte pode vir de vazamentos, cadastros comprometidos ou engenharia social.

O caso do falso advogado ilustra bem o mecanismo. A OAB registrou abordagens em que criminosos utilizam nomes, fotos e informações de processos para pedir pagamentos sob pretexto de liberar valores judiciais.[8] O dado verdadeiro não torna verdadeira a pessoa que o apresenta.

4.5 Escala, tecnologia e fronteiras

A internet permite que contato, infraestrutura e movimentação financeira estejam em lugares diferentes. Isso dificulta investigação e recuperação, enquanto automatização reduz o custo de abordar grandes grupos. Tradução automática e ferramentas de geração de conteúdo ampliam a capacidade de adaptar mensagens.

Para a vítima, a consequência prática é simples: aparência local não garante origem local, e familiaridade do canal não garante identidade.

4.6 Do rudimentar ao sofisticado

Nem todo golpe precisa ser tecnicamente sofisticado. Às vezes, uma mensagem curta funciona melhor que uma falsificação complexa porque encontra a pessoa certa no momento certo. Em outros casos, páginas clonadas, dados reais e automação elevam a aparência de legitimidade.

A defesa não deve depender de avaliar se o criminoso parece “amador”. O critério continua sendo o procedimento: identificar o pedido, interromper a pressão e verificar por fora da história apresentada.

CAPÍTULO 5

QUANDO O ALVO É O SEU DINHEIRO

5.1 A aparência de uma operação legítima

Quando o alvo é o dinheiro, a fraude quase nunca se apresenta com a aparência de um roubo. Ela se parece com uma operação normal. Pode vir como um aviso de segurança, uma cobrança, uma atualização cadastral, um pagamento, uma transferência, a liberação de um crédito ou uma oportunidade de investimento. A vítima não entrega o patrimônio porque decidiu correr um risco absurdo. Em geral, age porque acredita estar fazendo algo justificável naquele contexto.

É aí que o modelo visto no capítulo anterior se torna concreto. O contato cria uma explicação plausível; a explicação dá sentido ao pedido; a pressão reduz o espaço de conferência; e a ação financeira produz a vantagem. Em muitos golpes, a parte decisiva não está em convencer a pessoa de uma história longa, mas em fazê-la autorizar uma única operação: transferir, pagar, aproximar o cartão, informar um código, contratar algo ou enviar dinheiro para uma conta indicada.

Há uma inversão especialmente perigosa nos golpes financeiros: a vítima pode acreditar que está protegendo o próprio dinheiro quando, na verdade, está realizando a operação que provoca a perda. A mensagem diz que existe uma compra suspeita; a falsa central oferece uma “solução”. Surge um boleto que parece corrigir uma pendência. Um suposto atendente orienta a “cancelar” uma transação fazendo

outra. A ação recebe um nome tranquilizador, mas o efeito financeiro é o oposto.

Por isso, a pergunta útil não é apenas “isso parece verdadeiro?”. É preciso observar o que a história está tentando produzir. Se o resultado esperado é uma transferência, um pagamento, a entrega de credenciais ou outra alteração patrimonial, a verificação deve ocorrer antes da ação e fora do caminho indicado por quem fez o contato.

Reconhecer parte do contexto também não basta. Uma dívida pode existir e a cobrança ser falsa. Um cartão pode ser seu e a ligação não ser do banco. Você pode realmente estar esperando um crédito e a taxa exigida para “liberá-lo” não existir. Pode ter feito uma compra e receber, dias depois, uma falsa cobrança relacionada a ela. O fato verdadeiro aumenta a plausibilidade; não confirma a legitimidade da operação proposta.

Esse princípio acompanha todo o capítulo: antes de concluir uma operação financeira, é preciso distinguir a razão apresentada do destino real do dinheiro. Quem receberá? Por qual canal? Em nome de quem? A operação aparece também no ambiente oficial que você acessou por iniciativa própria? Quando essas respostas não são claras, interromper a ação é mais seguro do que tentar resolver a dúvida dentro da própria conversa que criou a urgência.

5.2 Banco, Pix, transferências e cartões

Fraudes bancárias exploram uma vantagem evidente: bancos fazem parte da rotina de milhões de pessoas e realmente enviam alertas, bloqueiam operações, confirmam compras e oferecem atendimento. O criminoso não precisa inventar uma instituição desconhecida. Basta ocupar, por alguns minutos, o lugar de uma instituição legítima.

No golpe da falsa central, por exemplo, o contato pode mencionar uma compra, uma tentativa de acesso, um empréstimo ou uma movimentação supostamente suspeita. O objetivo é fazer a vítima aceitar a premissa de que existe um problema urgente e de que o interlocutor tem autoridade para resolvê-lo. Diagnóstico produzido no âmbito da ENCCLA descreve essa modalidade como fraude de

engenharia social baseada na personificação de instituições financeiras e na indução da vítima a praticar atos que resultam em prejuízo.[12]

A partir daí, as instruções podem assumir formas diferentes. Em algumas situações, pedem transferência para uma conta apresentada como “segura”. Em outras, orientam a instalar aplicativo, compartilhar tela, informar dados ou realizar procedimentos que, para a vítima, parecem etapas de segurança. O formato muda; a lógica permanece: transformar uma ação financeira favorável ao fraudador em uma ação aparentemente favorável ao cliente.

É importante distinguir duas situações. Há operações que a vítima não reconhece e que podem decorrer de uso indevido de cartão, conta ou credenciais. E há operações que a própria vítima autoriza porque foi enganada sobre sua finalidade. As duas podem envolver fraude, mas o caminho que levou ao prejuízo é diferente. Essa distinção será importante mais adiante, quando o livro tratar de reação, direitos e responsabilidades. Aqui, ela serve para uma conclusão preventiva: o fato de você mesmo digitar a senha ou confirmar uma transferência não significa que a decisão tenha surgido de informação verdadeira.

No Pix, a velocidade que torna o sistema útil também exige atenção antes da confirmação. O aplicativo bancário mostra dados do recebedor antes da conclusão; essa etapa não deve ser tratada como detalhe automático. Nome, instituição e contexto do pagamento precisam fazer sentido. Se o pedido surgiu por ligação, mensagem ou link, a existência da chave Pix não prova que a pessoa ou empresa por trás da conversa seja legítima.

O Banco Central mantém o Mecanismo Especial de Devolução (MED) para casos de fraude, golpe ou crime envolvendo Pix. Em orientação atualizada em agosto de 2026, o BC informa que a vítima deve comunicar seu banco e solicitar a devolução; as instituições analisam o caso e podem bloquear valores disponíveis na conta recebedora.[15] Esse mecanismo aumenta a possibilidade de recuperação, mas não transforma a devolução em garantia. Por isso, ele pertence principalmente ao momento posterior ao golpe, que será tratado no

Capítulo 11; antes da transferência, a defesa mais forte continua sendo evitar que a operação fraudulenta seja autorizada.

Transferências tradicionais seguem a mesma lógica. Uma mudança inesperada de conta de fornecedor, prestador ou empresa pode ser apresentada como simples alteração administrativa. Se a decisão produzir deslocamento relevante de dinheiro, a alteração merece confirmação independente pelo contato habitual. Não é necessário desconfiar de toda mudança; é necessário não tomar a própria mensagem que anunciou a mudança como prova suficiente de que ela é verdadeira.

Com cartões, o pedido pode envolver dados, códigos, aproximação, inserção em maquininha ou uma cobrança apresentada como teste, estorno ou validação. Aqui também convém abandonar a ideia de que a aparência do equipamento ou do atendimento resolve a questão. O que importa é saber qual operação está sendo efetivamente autorizada e qual valor aparece antes da confirmação. Em uma compra presencial, conferir o visor é parte do ato de pagar; em uma compra remota, conferir o ambiente e o destinatário cumpre função semelhante.

O denominador comum é simples: banco, cartão, Pix e transferência não são golpes em si. São instrumentos legítimos que podem ser usados dentro de uma narrativa fraudulenta. A proteção não consiste em temer o instrumento, mas em separar a operação real da história contada para justificá-la.

5.3 Boletos, cobranças, empréstimos e crédito

Cobranças são especialmente convincentes quando encontram uma obrigação verdadeira. A pessoa tem uma mensalidade a vencer, comprou um produto, contratou um serviço, possui um financiamento ou aguarda uma encomenda. Um documento falso que chega nesse momento não precisa criar toda a realidade; ele apenas se encaixa em algo que já existe.

No boleto, a aparência visual é secundária diante de uma informação decisiva: quem receberá o pagamento. Logotipo, nome do

contrato, valor correto e dados pessoais podem tornar o documento familiar, mas o pagamento se materializa no beneficiário indicado pelo sistema. Antes de concluir, é preciso conferir se o recebedor corresponde à entidade que deveria receber aquele valor. Quando a cobrança é inesperada ou chegou por um canal incomum, a confirmação deve ser feita no ambiente oficial do credor.

O mesmo vale para cobranças vinculadas a encomendas, impostos ou taxas. A Receita Federal mantém alertas específicos sobre falsas mensagens de liberação de mercadorias. Em orientação atualizada, informa que não envia links de pagamento por SMS para cobrança de tributos de encomendas e recomenda que o usuário acesse diretamente os canais oficiais dos Correios ou das empresas responsáveis, sem usar o caminho enviado na mensagem.[17] O aprendizado é mais amplo do que o exemplo: uma cobrança pode mencionar uma situação real e ainda assim direcionar o pagamento para um destino fraudulento.

A fraude também pode começar pela necessidade de dinheiro. Quem procura empréstimo costuma estar tentando resolver um problema concreto e, por isso, pode interpretar rapidez e facilidade como solução. O falso crédito se aproveita exatamente desse ponto. A proposta oferece aprovação simples, juros atraentes ou liberação imediata e, quando a pessoa acredita que o dinheiro está próximo, surge a exigência de um pagamento antecipado: taxa, seguro, cadastro, imposto ou algum nome técnico semelhante.

O Banco Central orienta que não se faça pagamento antecipado para receber empréstimo e recomenda verificar se a instituição é autorizada a funcionar, além de confirmar informações pelos canais oficiais.[16] O ponto central não é decorar o nome das taxas usadas em cada versão do golpe. É perceber a inversão: a pessoa buscava receber dinheiro, mas a operação começa exigindo que ela envie dinheiro.

Em renegociações de dívida, o mecanismo pode ser parecido. O contato conhece ou afirma conhecer a obrigação, oferece desconto expressivo e cria uma janela curta para pagamento. O desconto pode existir em negociações legítimas; por isso, o valor vantajoso, sozinho, não prova fraude. A verificação deve recair sobre o canal, o credor, o

acordo e o destino do pagamento. Se a dívida consta no ambiente oficial do credor e as condições podem ser confirmadas sem depender da mensagem recebida, a decisão passa a se apoiar em elementos independentes.

Há ainda golpes em que a própria informação de crédito é usada como argumento de autoridade: suposta aprovação, limite liberado, restituição, benefício, indenização ou valor bloqueado aguardando uma pequena taxa. Em todos eles, a estrutura merece atenção quando a promessa de receber uma quantia exige primeiro uma transferência para destravar o recebimento. Não é uma regra absoluta sobre toda cobrança legítima; é um sinal forte de que a operação precisa ser verificada antes de qualquer pagamento.

Essa seção mostra por que “eu realmente devia” ou “eu realmente pedi um empréstimo” são respostas incompletas. A pergunta seguinte é: esta cobrança específica, esta conta específica e esta condição específica pertencem de fato à obrigação ou ao crédito que eu reconheço?

5.4 Investimentos e promessa de rendimento

Nos golpes de investimento, o dinheiro não sai para resolver um problema. Sai porque a vítima acredita que está construindo patrimônio. Isso muda o tom da narrativa, mas não elimina o processo já conhecido: credibilidade, expectativa, pressão e ação financeira.

Ofertas fraudulentas podem se apresentar como investimentos tradicionais, negócios privados, operações automatizadas, criptoativos, moedas estrangeiras ou plataformas com aparência tecnológica. Nenhuma dessas categorias, por si só, define fraude. Existem ativos e serviços legítimos em várias delas. O problema surge quando a aparência de investimento é usada para ocultar a inexistência da operação, a irregularidade da oferta ou um esquema cuja sustentabilidade depende da entrada contínua de novos recursos.

A Comissão de Valores Mobiliários alerta para ofertas e atuações irregulares, pirâmides e esquemas Ponzi. Nas pirâmides, a entrada de novos participantes sustenta pagamentos anteriores até que a

expansão se torne insuficiente; em esquemas Ponzi, o investidor pode receber rendimentos aparentes pagos com recursos de novos clientes, sem que exista a atividade econômica prometida.[18] A possibilidade de alguém receber no início, portanto, não demonstra que o investimento seja real. Em certos esquemas, esse pagamento inicial é justamente parte da aparência de legitimidade.

Esse detalhe é importante porque muda o significado da "prova". Um extrato exibido em uma plataforma, um saldo crescente na tela, um saque inicial ou o relato de alguém que recebeu podem parecer evidências de que a operação funciona. Mas cada uma dessas informações precisa ser ligada à pergunta central: existe um investimento verificável por trás do número apresentado? A interface pode mostrar um resultado sem demonstrar a origem econômica daquele resultado.

A pesquisa da própria CVM sobre fraudes financeiras registrou, entre participantes, fatores de credibilidade como aparência do site, bom atendimento e participação de familiares ou amigos. O estudo também reuniu relatos de processos em que ganhos aparentes e estruturas profissionais ajudavam a sustentar a confiança. Isso reforça um ponto já aprendido: sinais de organização e experiência de terceiros podem aumentar a plausibilidade, mas não substituem a verificação da oferta e de quem a realiza.[19]

Promessas de retorno elevado merecem atenção, sobretudo quando vêm acompanhadas de linguagem de segurança absoluta, urgência para aproveitar a oportunidade ou pressão para aumentar o aporte. O problema não é apenas "ganho alto". Investimentos legítimos podem ter retornos altos em determinados períodos e também perdas relevantes. O sinal preocupante é a tentativa de apresentar retorno extraordinário como praticamente certo, dissociado de risco compreensível e de informações verificáveis sobre produto, emissor, intermediário e condições de retirada.

Outro momento crítico ocorre quando retirar o dinheiro se torna mais difícil do que colocá-lo. Surgem justificativas para novo aporte, pagamento de taxa, imposto, desbloqueio, atualização ou aumento de margem antes que o saldo possa ser liberado. A vítima, que já investiu,

pode sentir que precisa enviar mais para não perder o que colocou antes. O valor anterior passa a pressionar a decisão seguinte.

É exatamente nessa hora que o objetivo da verificação muda. Em vez de perguntar apenas quanto aparece na tela, é preciso perguntar quem detém os recursos, qual entidade responde pela operação, se a atividade exige autorização ou registro e como essas informações podem ser confirmadas fora da própria plataforma ou do interlocutor. A CVM mantém mecanismos de consulta e alertas sobre participantes e ofertas irregulares; quando a atividade estiver dentro de sua esfera de supervisão, esses canais são parte da verificação.[18]

Criptoativos merecem a mesma cautela conceitual. A tecnologia ou o tipo de ativo não transforma automaticamente uma operação em fraude, assim como um contrato formal não torna automaticamente um investimento legítimo. Golpistas podem usar o vocabulário de qualquer mercado para construir credibilidade. O leitor deve resistir a duas simplificações: “se envolve cripto, é golpe” e “se existe aplicativo, contrato ou painel, é investimento”. Em ambos os casos, a conclusão vem cedo demais.

Ao reunir falsas centrais, Pix, cartões, cobranças, crédito e investimentos, aparece uma estrutura comum. O dinheiro raramente é pedido com a frase “entregue seu patrimônio”. Ele é apresentado como solução, proteção, pagamento devido, condição de liberação ou oportunidade. O nome dado à operação pode mudar; a consequência precisa ser observada do mesmo modo.

Antes de agir, três verificações atravessam quase todas essas situações sem substituir o método completo que será apresentado no Capítulo 10: identificar exatamente qual operação está sendo solicitada; conferir quem recebe ou controla o recurso; e confirmar a justificativa em um canal independente. Quando o risco financeiro é relevante, alguns minutos usados para essa separação podem impedir que uma narrativa convincente se transforme em perda concreta.

CAPÍTULO 6

QUANDO O GOLPISTA SE TORNA ALGUÉM EM QUEM VOCÊ CONFIA

6.1 “Sou eu. Este é meu novo número.”

Há golpes que começam tentando convencer você de que um desconhecido é confiável. Outros fazem algo mais simples: tentam convencer você de que o desconhecido não é um desconhecido. A fotografia é familiar, o nome também, a maneira de escrever parece plausível e a conversa parte de uma relação que já existe. Em vez de construir confiança do zero, o golpista procura ocupar o lugar de alguém que já a possui.

A mensagem “sou eu, este é meu novo número” funciona justamente por isso. Ela oferece uma explicação para a única coisa que não combina com a identidade apresentada: o número diferente. Se essa explicação for aceita, os demais sinais — foto, nome, parentesco, algum detalhe da rotina — passam a parecer suficientes. O pedido vem depois: pagar uma conta, fazer uma transferência, resolver uma emergência ou ajudar porque o aplicativo bancário “não está funcionando”.

A Anatel descreve o chamado golpe do WhatsApp falso como a criação de uma conta com foto e identidade de outra pessoa para solicitar dinheiro a conhecidos, amigos ou familiares. A modalidade não depende de o golpista assumir o controle da conta verdadeira:

pode haver apenas um novo número usando a imagem e o nome da pessoa imitada.[20] Essa diferença é importante porque a presença do perfil legítimo ainda ativo não impede que exista outro perfil falso circulando.

Familiaridade, então, não é confirmação. Uma fotografia pode ser copiada. Um nome pode ser reproduzido. Informações sobre parentes, trabalho ou rotina podem estar disponíveis em redes sociais, bases de dados, cadastros ou conversas anteriores. Até a linguagem pode ser imitada de maneira aproximada. Quanto maior a semelhança, mais natural parece continuar a conversa sem interrompê-la para conferir.

O caminho mais seguro é deslocar a confirmação para fora do contato recebido. Se alguém conhecido aparece com novo número e pede dinheiro ou outra ação relevante, a verificação deve usar um canal que já existia antes daquela mensagem: o número antigo, uma ligação iniciada por você, outro familiar, um contato presencial ou outro meio confiável. A confirmação não precisa ser hostil. Ela apenas precisa ser independente.

Perguntas pessoais podem ajudar, mas têm limitações. Informações que parecem privadas podem ter sido descobertas, e respostas podem ser inferidas a partir do que está publicado ou do que a própria vítima diz durante a conversa. Quando há dinheiro, dados sensíveis ou mudança importante de cadastro, o melhor critério é não depender de um teste conduzido dentro do mesmo canal cuja identidade está em dúvida.

Isso vale além de aplicativos de mensagem. Um perfil em rede social, uma conta de e-mail, uma ligação telefônica ou qualquer canal digital pode carregar sinais conhecidos sem que o interlocutor seja a pessoa conhecida. O princípio não muda com a plataforma: reconhecer elementos da identidade é apenas o começo; confirmar a pessoa exige uma evidência que não tenha sido fornecida pelo próprio contato suspeito.

6.2 “Estamos entrando em contato para resolver um problema.”

A personificação também funciona quando a identidade emprestada não é de uma pessoa próxima, mas de uma instituição. Banco, operadora de telefonia, loja, plataforma digital, órgão público, cartório, empresa de entrega ou serviço conhecido podem ser usados como ponto de partida. A credibilidade não vem do relacionamento pessoal; vem da autoridade atribuída à organização.

Nesse tipo de abordagem, a mensagem costuma apresentar um problema e uma solução no mesmo movimento. Há uma compra suspeita, um cadastro irregular, uma pendência fiscal, uma encomenda retida, uma conta a ser protegida, um benefício a ser atualizado ou uma suposta infração que precisa ser resolvida. O contato cria o motivo para agir e, ao mesmo tempo, oferece o caminho pelo qual a ação deve ocorrer.

O Centro Integrado de Segurança Cibernética do Governo Federal alertou, em 2026, para campanhas em que criminosos usam perfis falsos com imagens de órgãos públicos, identidade visual do gov.br e até dados pessoais verdadeiros — como nome, CPF, data de nascimento, endereço e nomes de familiares — para dar aparência oficial à abordagem.[21] O valor desses elementos está justamente em reduzir a sensação de estranhamento.

Mas reconhecer a instituição é diferente de confirmar que aquela comunicação veio dela. Um logotipo prova que alguém teve acesso ao logotipo. Um número de protocolo pode ter sido inventado. Um documento com aparência institucional pode ter sido montado. Um número de telefone exibido na tela não deve ser tratado, isoladamente, como certificado de origem. A instituição pode ser real e o contato, falso.

A forma mais útil de romper esse roteiro é separar duas perguntas: “essa instituição existe?” e “este contato pertence realmente a ela?”. A primeira costuma ser fácil. A segunda exige sair da mensagem, da ligação ou do link recebido e procurar, por iniciativa própria, o

aplicativo oficial, o endereço digitado diretamente, o telefone já conhecido ou outro canal público confiável.

Se existe uma pendência verdadeira, ela tende a poder ser confirmada no ambiente legítimo. Esse deslocamento é importante porque retira do interlocutor o controle sobre a verificação. Em vez de perguntar ao suposto representante se ele é verdadeiro e aceitar a própria resposta como prova, o leitor compara a história recebida com uma fonte independente.

Esse raciocínio também evita um erro comum: imaginar que somente mensagens mal escritas ou endereços evidentemente estranhos são perigosos. A personificação pode usar linguagem correta, símbolos oficiais, atendimento organizado e informações precisas. Qualidade visual é um sinal de produção; não é prova de autoria.

6.3 O falso profissional

Algumas identidades carregam uma forma específica de confiança: a confiança profissional. Advogados, contadores, corretores, técnicos, prestadores de serviço, gerentes, médicos, servidores e outros profissionais são procurados justamente porque detêm conhecimento, acesso ou atribuições que o cliente não domina. Quando um golpista ocupa esse papel, ele se beneficia da autoridade que a profissão já possui.

O falso profissional não precisa inventar tudo. Pode copiar nome, fotografia, registro, endereço comercial, logotipo do escritório e informações sobre um serviço verdadeiro. Pode ainda escolher o momento em que há algo realmente acontecendo: um processo em andamento, uma declaração a entregar, uma manutenção contratada, uma negociação imobiliária ou uma questão técnica pendente. O contexto real funciona como cenário para uma identidade falsa.

O golpe do falso advogado tornou esse mecanismo especialmente visível. Em 2025, o Conselho Federal da OAB lançou a plataforma ConfirmADV para permitir a verificação da identidade profissional. Em abril de 2026, a OAB informou que a ferramenta já havia recebido

mais de 32 mil solicitações de verificação.[22] A própria existência de uma ferramenta institucional desse tipo mostra a necessidade de distinguir dados profissionais verdadeiros da pessoa que efetivamente está fazendo o contato.

Em uma abordagem falsa, o nome do advogado pode estar correto. O número de inscrição pode existir. O processo pode ser verdadeiro. O nome da parte, a vara, o valor discutido e até movimentações processuais podem ser reproduzidos a partir de informações acessíveis. O ponto vulnerável não está necessariamente nos fatos citados. Está no salto lógico que transforma esses fatos em prova de que o interlocutor é o profissional legítimo.

O mesmo aprendizado vale para outras profissões. Um falso contador pode conhecer dados da empresa; um falso corretor pode copiar fotografias e documentos de um imóvel; um falso técnico pode saber o modelo de um equipamento; um falso prestador pode mencionar contrato ou visita anteriores. Em todos esses casos, informação contextual aumenta a plausibilidade, mas não resolve a identidade.

Quando o contato produz pedido de pagamento, envio de documento, instalação de programa, compartilhamento de senha ou outra ação relevante, a confirmação deve voltar ao relacionamento original. Ligue para o número do escritório que você já usava, acesse o cadastro oficial da profissão quando houver, confirme com a empresa ou procure o profissional por canal previamente conhecido. O objetivo não é desconfiar de toda comunicação profissional, e sim não permitir que o próprio contato seja sua única fonte de autenticação.

6.4 Quando informações verdadeiras sustentam uma identidade falsa

Este é um dos pontos mais importantes do livro porque contraria uma reação intuitiva. Quando alguém demonstra conhecer seu nome completo, CPF, endereço, banco, profissão, familiares ou detalhes de um processo, a sensação natural é pensar: “se sabe tudo isso, deve ser quem diz ser”. O problema está na palavra “deve”. Ela transforma conhecimento de dados em identidade confirmada.

Dados verdadeiros podem chegar às mãos de terceiros por caminhos muito diferentes. Alguns são públicos por natureza. Outros foram publicados pela própria pessoa, aparecem em documentos, circulam entre empresas, foram compartilhados em cadastros, expostos em incidentes, obtidos por engenharia social ou extraídos de contas comprometidas. Para a decisão imediata do leitor, nem sempre é possível saber de onde vieram. E essa investigação não precisa ser resolvida antes de perceber o essencial: o dado correto não autentica quem o apresenta.

Imagine uma pessoa que sabe seu nome, informa corretamente o banco que você utiliza e cita os quatro últimos dígitos de um documento. Esses elementos podem aumentar muito a credibilidade subjetiva do contato. Mas eles respondem apenas à pergunta “essa pessoa conhece algumas informações sobre mim?”. Não respondem à pergunta “essa pessoa é realmente representante do meu banco?”. São questões diferentes.

O alerta do Governo Federal sobre falsos representantes públicos torna essa distinção concreta: campanhas identificadas usavam dados pessoais reais justamente para reforçar a aparência de legitimidade.[21] A informação correta, nesse contexto, não era um detalhe acidental. Era parte do mecanismo de convencimento.

Por isso, uma boa verificação procura uma característica que o fraudador não controle. Pode ser o acesso a um ambiente oficial iniciado por você, uma chamada para número já conhecido, uma consulta pública independente, uma confirmação presencial ou outro procedimento que não dependa do link, telefone ou documento

enviado pelo interlocutor. Quanto mais a prova de identidade é produzida pelo próprio suspeito, menor sua força.

Esse princípio também ajuda a interpretar documentos digitais, fotografias e capturas de tela. Eles podem ser úteis, mas devem ser relacionados à origem. Uma imagem de documento enviada por alguém não prova, sozinha, que o remetente é seu titular. Uma captura de uma página oficial não prova que a conversa esteja ocorrendo com o órgão. Uma fotografia ao lado de um crachá não transforma o canal em oficial.

O leitor não precisa se tornar especialista em falsificação documental para se proteger. A pergunta mais simples continua suficiente: “qual parte desta confirmação independe da pessoa que está tentando me convencer?”. Se a resposta for “nenhuma”, ainda falta uma etapa de verificação.

6.5 Quando a identidade roubada é a sua

Até aqui, vimos a identidade falsa do ponto de vista de quem recebe o contato. Mas a situação pode se inverter: seu nome, sua fotografia, seus documentos, sua conta ou seu perfil podem ser usados para convencer outras pessoas. Nesse momento, você deixa de ser apenas alvo de uma história falsa e passa a ser, sem consentimento, parte da credibilidade usada contra terceiros.

É útil separar três situações que muitas vezes são chamadas indistintamente de “clonagem”. A primeira é o perfil falso: alguém cria outra conta ou outro número e copia elementos da sua identidade. A segunda é a tomada de conta: o criminoso obtém acesso à conta verdadeira e passa a operar a partir dela. A terceira é o uso indevido de dados ou documentos para abrir cadastros, contratar serviços ou realizar operações em seu nome. As consequências podem se cruzar, mas o mecanismo é diferente.

O Ministério da Justiça orienta que, quando uma rede social é invadida ou clonada, a pessoa use os mecanismos oficiais de recuperação ou denúncia, avise contatos e preserve evidências. A própria orientação distingue a conta hackeada, em que há necessidade

de recuperação de acesso, do perfil clonado, em que outro perfil se passa pela pessoa.[24] Aqui interessa menos o procedimento posterior — tratado adiante no livro — e mais perceber que "alguém está falando como você" pode ocorrer sem que sua conta verdadeira tenha sido tomada.

O uso indevido de identidade também pode chegar ao sistema financeiro. O Banco Central informa que o Relatório de Contas e Relacionamentos (CCS), disponível no Registrato, permite verificar em quais instituições uma pessoa possui relacionamento e pode ajudar a identificar se CPF ou CNPJ foi usado indevidamente para abertura de conta fraudulenta.[23] Isso mostra uma consequência importante: a identidade apropriada pode ser usada não apenas para abordar seus conhecidos, mas também para criar relações formais em seu nome.

Outras consequências possíveis incluem tentativas de contratação de crédito, criação de cadastros, recuperação indevida de senhas, personificação perante empresas ou uso de perfis para solicitar dinheiro. Nem toda exposição de dado produz automaticamente uma dessas consequências, e conhecer um dado não significa ter controle sobre sua identidade inteira. O risco depende do conjunto de informações, dos mecanismos de autenticação e do que o serviço permite fazer.

Por isso, também é importante não transformar a proteção da identidade em uma busca impossível por segredo absoluto. Nome, profissão e outros dados podem precisar circular legitimamente. O objetivo realista é reduzir a exposição desnecessária, proteger credenciais e contas, utilizar autenticação adicional quando disponível e perceber rapidamente sinais de uso indevido. A identidade digital é sustentada por vários elementos, e nenhum deles deveria ser tratado isoladamente como prova definitiva.

Os procedimentos detalhados depois de um dano — registros, comunicação a instituições, recuperação de contas, medidas financeiras e direitos — ficarão para os Capítulos 11 e 12. Neste ponto, basta consolidar o aprendizado que atravessa todo o capítulo: conhecer informações verdadeiras sobre você não prova que alguém

seja quem afirma ser. E ver seu nome, sua foto ou seus dados em um canal não prova que aquele canal esteja sob seu controle.

Quando a identidade é o instrumento do golpe, a melhor defesa não é tentar perceber se a pessoa "parece" convincente. É mudar a pergunta. Em vez de "reconheço esta pessoa ou esta instituição?", pergunte: "como posso confirmar, por um caminho independente, que estou realmente falando com ela?". Essa mudança simples desloca a decisão da aparência para a verificação — e prepara o leitor para as oportunidades e negociações do próximo capítulo, em que a identidade de quem oferece algo continuará sendo apenas uma parte daquilo que precisa ser confirmado.

CAPÍTULO 7

OPORTUNIDADES BOAS DEMAIS

7.1 Comprar, vender e negociar

Nem todo golpe começa com medo. Alguns começam com uma sensação agradável: a de ter encontrado uma oportunidade. Um produto aparece por preço abaixo do habitual, um comprador surge rapidamente, uma negociação parece simples, alguém oferece intermediação e tudo indica que basta agir antes que outra pessoa aproveite. Nesses casos, a pressa não nasce de uma ameaça. Nasce do receio de perder algo vantajoso.

Esse mecanismo é especialmente forte em compras e vendas porque a própria negociação legítima já contém elementos que podem ser explorados: preço, escassez, comparação com outras ofertas, avaliações, prazo, reserva, sinal e formas de pagamento. O problema não está em algum desses elementos isoladamente. Está em como eles são combinados para reduzir a verificação e deslocar a pessoa para um ambiente em que o fraudador controla a informação.

Em uma compra falsa, a vitrine pode ser convincente. Fotografias reais podem ter sido copiadas, avaliações podem ter sido fabricadas ou retiradas de outro lugar, e o site pode imitar uma loja conhecida. A Receita Federal mantém alerta específico para compras em sites falsos ou redes sociais e descreve situações em que até confirmações de pagamento, mensagens de envio e páginas de rastreamento são produzidas para prolongar a aparência de uma compra legítima.[25] A

fraude, portanto, pode continuar parecendo uma compra mesmo depois que o dinheiro já saiu.

Preço muito abaixo do mercado merece atenção, mas não deve ser tratado como fórmula automática. Promoções verdadeiras existem, liquidações existem e vendedores podem aceitar valores menores por razões legítimas. O critério útil é proporcional: quanto mais excepcional a vantagem, mais importante se torna verificar vendedor, canal, forma de pagamento, existência do produto e condições da negociação antes de agir.

No marketplace, outra variável relevante é a proteção oferecida pelo próprio ambiente. Plataformas podem registrar conversa, pagamento, anúncio e entrega. Quando alguém insiste em levar a negociação para outro aplicativo, enviar um link diferente, alterar o modo de pagamento ou resolver tudo "por fora", uma parte das salvaguardas deixa de acompanhar a transação. Isso não transforma toda conversa externa em golpe, mas altera o nível de risco e exige conferência adicional.

Quem vende também pode ser alvo. Um falso comprador pode demonstrar interesse imediato, afirmar que já pagou, enviar comprovante, criar uma falsa mensagem de confirmação ou introduzir um suposto intermediário. O vendedor, animado com a conclusão do negócio, pode entregar o produto antes de verificar se o dinheiro realmente entrou. Aqui, a oportunidade atua do lado oposto: não é comprar barato, mas vender rápido.

Comprovante não é recebimento. Mensagem não é saldo. E-mail de confirmação não substitui consulta ao aplicativo, à conta ou ao ambiente oficial da plataforma. Essa distinção é pequena, mas transfere a decisão da aparência para um fato verificável.

Leilões merecem o mesmo raciocínio. O Banco Central recomenda pesquisar se a loja ou a empresa de leilão realmente existe quando houver compras pela internet e preços muito abaixo do mercado.[28] A palavra "leilão", por si só, não torna o desconto suspeito nem legítimo. O que precisa ser confirmado é quem está promovendo a venda, qual é o canal oficial e para onde o pagamento será direcionado.

A lição desta seção é simples: em uma negociação, a sensação de vantagem pode ser verdadeira e, ainda assim, a verificação continuar necessária. O risco cresce quando a oferta excepcional vem acompanhada de pressão para sair do ambiente habitual, pagar rapidamente ou aceitar uma confirmação produzida pelo próprio interlocutor.

7.2 Emprego e renda

Uma oportunidade de emprego toca em algo diferente de uma compra. Para quem precisa trabalhar, mudar de renda ou voltar ao mercado, a proposta pode representar alívio, autonomia e esperança. Isso torna a oferta importante antes mesmo de qualquer contratação. E é justamente essa importância que pode ser explorada.

Falsas vagas podem copiar nomes de empresas reais, usar logotipos, fotografias de escritórios, perfis de supostos recrutadores e descrições plausíveis de cargos. Algumas se apresentam como seleções convencionais; outras prometem trabalho remoto, renda extra, comissões ou tarefas simples remuneradas. Em todos os casos, a oportunidade ganha força porque parece resolver uma necessidade concreta.

A Funtrab alertou em 2026 para anúncios falsos de cursos e vagas que usavam indevidamente o nome da instituição, com promessas de emprego fácil, salários elevados e solicitação de pagamentos para acesso a vagas ou processos seletivos. A fundação reforçou que sua intermediação é gratuita.[26] O exemplo é útil porque mostra como a credibilidade de uma instituição verdadeira pode ser emprestada a uma oportunidade inexistente.

Pedir dinheiro durante um processo seletivo não prova sozinho que exista fraude em qualquer situação imaginável, mas muda profundamente a análise. Se a proposta de trabalho exige pagamento por curso, cadastro, uniforme, certificado, exame, equipamento ou liberação antes que a contratação possa prosseguir, é necessário confirmar diretamente com a empresa ou instituição, usando canais obtidos de forma independente.

A mesma cautela vale para pedidos de documentos. Processos seletivos legítimos podem precisar de informações pessoais em algum momento. O problema surge quando a quantidade, a sensibilidade ou o momento do pedido não combinam com a etapa da seleção. Documento, selfie, dados bancários e códigos não devem ser fornecidos apenas porque o contato parece profissional ou usa o nome de uma empresa conhecida.

Alguns golpes de renda extra começam com tarefas pequenas. A pessoa recebe uma atividade simples, obtém um pequeno retorno ou vê um saldo crescente e passa a acreditar que encontrou uma fonte de renda. Em seguida, a dinâmica pode exigir depósitos, recargas ou aportes para liberar tarefas de maior valor. Quando a oportunidade de ganhar passa a depender de enviar dinheiro continuamente, a direção do fluxo financeiro merece atenção: quem buscava receber renda está sendo levado a financiar o próprio processo.

Não é necessário decorar formatos específicos de “tarefas remuneradas”. Eles mudam. A pergunta transferível é outra: qual é a atividade econômica real que explica o pagamento? Quem é a empresa? Como ela ganha dinheiro? Por que o trabalhador precisa antecipar recursos para poder receber? Se essas respostas dependem exclusivamente do recrutador ou da plataforma suspeita, ainda não existe confirmação suficiente.

Uma vaga legítima suporta verificação. A empresa pode ser pesquisada fora do anúncio; a pessoa responsável pode ser confirmada por canal oficial; as etapas do processo podem ser comparadas com as práticas divulgadas pela própria organização. A urgência do desemprego não desaparece, mas a decisão deixa de depender inteiramente de quem fez a promessa.

7.3 Negócios e bens de maior valor

Quanto maior o valor do bem, maior pode ser a perda produzida por uma única decisão. Veículos, imóveis, locações e outros negócios relevantes costumam envolver documentação, visitas, intermediários, sinais e prazos. A complexidade legítima desses negócios cria espaço para que uma fraude pareça apenas mais uma etapa burocrática.

Um anúncio de imóvel pode usar fotografias verdadeiras de um bem que existe. Um veículo pode ser real, estar fisicamente disponível e até ser mostrado à pessoa. A existência do bem, porém, não confirma que quem negocia tenha legitimidade para vendê-lo, alugá-lo ou receber valores em nome da operação.

Em 2025, o CRECI-MS alertou para fraudes de falso aluguel em que imóveis reais eram anunciados com fotografias retiradas da internet e oferecidos por valores abaixo do mercado, com cobrança antecipada de caução. O conselho recomendou verificar o registro profissional quando houver corretor, conferir documentação e evitar pagamento antecipado sem as verificações adequadas.[27] O ponto central não é transformar toda caução em suspeita, mas perceber que a presença de um imóvel real não autentica a pessoa que está negociando.

Negociações de veículos apresentam risco semelhante quando aparece um intermediário que afirma representar o proprietário, um parente, uma loja ou outro interessado. O bem pode existir e os documentos podem ser verdadeiros, mas a história que explica quem deve receber o dinheiro pode ser falsa. Quando há terceiros entre comprador e vendedor, é importante que todos saibam claramente quem são as partes, qual é o preço efetivo e qual é a razão da intermediação.

A urgência costuma ser justificada pelo negócio: há outro interessado, o proprietário precisa vender rapidamente, o imóvel será reservado apenas até certa hora, o veículo está abaixo da tabela porque surgiu uma necessidade. Nada disso é impossível em transações reais. Por isso, o sinal de alerta não está na história em si, mas no uso da história para impedir verificações compatíveis com o valor da decisão.

Em bens de maior valor, pequenas confirmações podem ser insuficientes. Uma fotografia de documento, uma conversa por vídeo ou uma visita ao bem podem aumentar a confiança, mas cada uma responde apenas a uma parte da questão. É preciso confirmar também titularidade ou legitimidade para negociar, identidade das partes, condições efetivas e destino do pagamento, conforme o tipo de negócio.

Este livro não pretende substituir análise jurídica, documental ou contratual especializada. A regra preventiva é anterior a isso: quanto maior a consequência financeira e mais difícil a reversão, menos razoável é permitir que a urgência da oportunidade reduza a verificação. Um bom negócio não precisa ser decidido com base apenas na versão de quem tem interesse em receber.

7.4 Prêmios, vantagens e dinheiro inesperado

Algumas oportunidades dispensam até a ideia de trabalho ou compra. O contato anuncia um prêmio, uma herança, uma restituição, um benefício, um brinde, uma recompensa ou algum dinheiro inesperado. A vítima não precisa desejar algo que estava procurando; basta aceitar a possibilidade de receber uma vantagem que surgiu de repente.

Esse tipo de abordagem cria uma inversão fácil de perceber quando observada com distância: para receber dinheiro, a pessoa começa a ser orientada a enviar dinheiro. Aparecem taxas, despesas administrativas, frete, imposto, seguro, cadastro, desbloqueio ou algum pagamento apresentado como pequeno diante da quantia prometida.

O Banco Central inclui entre suas orientações gerais a recomendação de desconfiar de promessas de herança, doação ou prêmios em moeda estrangeira que exijam transferência de dinheiro para receber o valor prometido.[28] O princípio é mais amplo do que essas modalidades específicas: quando uma vantagem inesperada depende de uma ação financeira prévia, a origem da promessa e a necessidade do pagamento precisam ser confirmadas antes de qualquer transferência.

Nem sempre a exigência inicial é dinheiro. Um brinde ou benefício pode ser usado para obter dados, fotografias ou imagens destinadas a reconhecimento facial. O Banco Central descreve o golpe do “presente”, em que uma suposta oferta de produto, renda extra ou brinde é usada para solicitar dados pessoais ou selfie, que podem depois ser utilizados para abrir conta ou contratar empréstimo em nome da vítima.[29] Aqui, a vantagem funciona como porta de entrada para outra finalidade.

Pequenas exigências podem parecer aceitáveis justamente porque são pequenas. Se alguém promete uma quantia elevada e pede apenas uma taxa modesta, a vítima pode raciocinar que o risco compensa. Depois do primeiro pagamento, podem surgir novas justificativas: faltou um documento, houve erro no cadastro, apareceu uma tarifa final. A decisão anterior passa a influenciar a próxima, porque desistir significa admitir que o primeiro valor talvez tenha sido perdido.

É importante não transformar essa observação em regra contra prêmios ou benefícios legítimos. Sorteios existem, promoções existem, restituições existem e programas públicos ou privados podem efetivamente conceder vantagens. A diferença está na possibilidade de confirmar a existência da promoção, da instituição responsável e das condições por uma fonte independente, sem depender do link ou do interlocutor que anunciou o benefício.

O mesmo vale para mensagens que informam dinheiro a receber de órgãos públicos, empresas, plataformas ou ações judiciais. O leitor não precisa decidir se a história é impossível. Precisa apenas transferir a verificação para o canal oficial antes de fornecer credenciais, instalar programas, enviar documentos ou pagar qualquer valor.

Uma oportunidade pode ser exatamente aquilo que afirma ser. Esse é o ponto que impede o livro de substituir prudência por desconfiança generalizada. A defesa não é rejeitar tudo que pareça vantajoso. É aumentar a disposição para verificar à medida que crescem a vantagem prometida, a urgência e a consequência da ação solicitada.

Nos capítulos anteriores, vimos que o golpista pode fabricar credibilidade e identidade. Neste capítulo, vimos que ele também pode fabricar oportunidade. O elemento comum não é o preço baixo, o

emprego, o imóvel ou o prêmio. É a tentativa de fazer com que o valor percebido da oportunidade seja maior do que o espaço reservado à conferência. Quando isso acontece, a vantagem deixa de ser apenas uma boa notícia e passa a exigir uma pergunta adicional: o que eu consigo confirmar fora da própria oferta?

Essa pergunta prepara o próximo passo. Algumas fraudes não oferecem apenas dinheiro, trabalho ou um bem. Elas oferecem afeto, proteção, pertencimento e a sensação de estar ajudando alguém. Quando sentimentos intensos entram na história, verificar pode se tornar ainda mais difícil.

CAPÍTULO 8

QUANDO O GOLPE EXPLORA SENTIMENTOS

8.1 Afeto e relacionamento

Nem todo golpe começa com um pedido de dinheiro. Alguns começam com conversa, presença e atenção. A relação se constrói antes da cobrança. O patrimônio aparece depois, quando ajudar já parece coerente com o vínculo que foi formado.

Nas fraudes afetivas, o tempo pode trabalhar a favor do golpista. Mensagens frequentes, confidências, planos para o futuro, demonstrações de cuidado e a sensação de exclusividade podem transformar um contato inicialmente desconhecido em alguém emocionalmente importante. A revisão sistemática de Lazarus e colaboradores, baseada em estudos empíricos sobre fraude amorosa, mostra que a literatura descreve justamente processos de aproximação e persuasão que antecedem a solicitação de dinheiro.[30]

Isso não significa que relacionamentos iniciados pela internet sejam suspeitos. Milhões de relações legítimas começam em aplicativos, redes sociais e outros ambientes digitais. O problema não está no meio. Está na combinação entre vínculo, dificuldade de confirmação e pedidos que passam a exigir dinheiro, documentos, acesso a contas ou outras concessões relevantes.

Uma história fraudulenta pode explicar repetidamente por que encontros presenciais não acontecem, por que chamadas de vídeo são

evitadas ou por que sempre surge uma nova emergência. Cada justificativa, isoladamente, pode parecer possível. O risco aumenta quando a relação depende de uma sequência de exceções que impedem a verificação e, ao mesmo tempo, aumentam o compromisso emocional.

Entrevistas com vítimas de fraude amorosa mostram que o prejuízo não se resume ao dinheiro. Para algumas pessoas, a ruptura da relação percebida como verdadeira pode ser tão ou mais dolorosa que a perda financeira.[31] Isso ajuda a compreender por que a simples apresentação de uma suspeita por familiares ou amigos nem sempre encerra imediatamente o envolvimento.

Por isso, a prevenção não deve se apoiar em frases como “não se apaixone pela internet” ou “desconfie de quem demonstra carinho”. Essas recomendações são inúteis e injustas. O ponto prático é outro: relações importantes também precisam suportar realidade verificável. Quanto maior o pedido e quanto mais difícil for confirmar fatos básicos da vida da outra pessoa, maior deve ser a pausa antes de transformar afeto em decisão patrimonial.

Uma relação legítima pode sobreviver a perguntas, limites e tempo. O golpista, ao contrário, pode tentar transformar a verificação em ofensa: “se você confiasse em mim, não perguntaria”; “depois de tudo o que vivemos, você ainda duvida?”. Quando a prova de amor passa a ser pagar, transferir, emprestar ou silenciar dúvidas, a emoção deixou de ser apenas contexto e passou a ser usada como pressão.

8.2 “Aconteceu alguma coisa com alguém que você ama.”

Poucas situações comprimem tanto o tempo de decisão quanto a notícia de que alguém próximo está em perigo. Acidente, hospital, prisão, sequestro, perda de telefone ou qualquer outra emergência pode produzir uma reação imediata: primeiro ajudar, depois entender. É exatamente essa ordem que uma fraude procura explorar.

Em 2026, a Polícia Civil do Paraná registrou um caso em que criminosos mantiveram uma criança ao telefone sob ameaças e,

simultaneamente, ligaram para os pais afirmando que ela havia sido sequestrada e exigindo dinheiro. A orientação policial, em situações desse tipo, é tentar contato com a pessoa envolvida por outros meios e acionar as forças de segurança.[32] O caso é extremo, mas deixa claro o mecanismo: medo e urgência são usados para impedir a conferência.

Nem toda falsa emergência envolve sequestro. A mensagem pode dizer que um filho quebrou o telefone, que um familiar sofreu acidente, que alguém está sem acesso ao banco ou que é preciso pagar rapidamente uma despesa médica. O conteúdo muda, mas a estrutura permanece: a pessoa amada estaria em dificuldade, e qualquer demora pareceria irresponsável.

Quando isso acontece, verificar não é abandonar quem precisa de ajuda. É aumentar a chance de ajudar a pessoa certa. Tente o número conhecido, procure outro familiar, ligue para o hospital ou instituição por contato obtido de forma independente, ou peça a alguém próximo que confirme a situação. O objetivo é criar uma segunda fonte antes de realizar uma ação difícil de reverter.

A emoção pode tornar até sinais estranhos aceitáveis. Uma voz diferente pode ser atribuída ao choro; uma escrita incomum, ao nervosismo; um número novo, ao telefone perdido. No Capítulo 9 veremos que recursos tecnológicos podem aumentar ainda mais a força desses sinais aparentes. Aqui basta reter um princípio: quando a situação parece urgente demais para conferir, a conferência se torna ainda mais necessária.

Esse cuidado não exige frieza. É possível agir com rapidez e, ainda assim, reservar alguns minutos para confirmar. Em emergências reais, esses minutos podem direcionar a ajuda corretamente. Em emergências falsas, podem interromper o golpe antes da transferência.

8.3 Solidariedade e compaixão

A solidariedade é outra porta possível para a fraude porque pessoas legítimas realmente precisam de ajuda. Campanhas para tratamento médico, reconstrução após desastre, apoio a famílias, proteção de animais, projetos sociais e pedidos individuais fazem parte da vida coletiva. A fraude não torna a compaixão um erro; ela tenta se aproveitar dela.

O desafio está em separar a história da destinação. Uma fotografia comovente pode ser verdadeira e estar sendo reutilizada fora do contexto. Um nome real pode aparecer em uma campanha criada por terceiros. Uma instituição existente pode ter sua marca copiada. A emoção despertada pela história não confirma quem receberá o dinheiro.

Por isso, antes de doar, a pergunta útil é: consigo confirmar a campanha fora da própria mensagem que me convenceu? Quando houver instituição, procure o site ou perfil oficial por iniciativa própria. Quando houver pessoa identificada, verifique se familiares, organização responsável ou outro canal confiável confirma a necessidade e a forma de contribuição.

Também é importante evitar o movimento oposto: transformar prudência em indiferença. A conclusão correta não é “pedidos de ajuda são suspeitos”. É “pedidos de ajuda também podem ser verificados”. A confirmação protege tanto quem doa quanto quem realmente precisa receber.

Golpistas podem ainda usar a urgência moral: “se você não ajudar agora, algo grave acontecerá”. Às vezes, a urgência é real. Mesmo assim, quem organiza uma campanha legítima tende a conseguir indicar destinatário, instituição, histórico e meios de confirmação. A necessidade de agir rápido não elimina a necessidade de saber para onde a ajuda está indo.

8.4 Medo, ameaça, vergonha e segredo

Em outras fraudes, o golpista não promete afeto nem pede solidariedade. Ele ameaça. A vítima é levada a acreditar que precisa pagar, obedecer ou fornecer algo para evitar prisão, exposição, prejuízo, constrangimento, perda profissional ou dano a alguém próximo.

O medo altera a prioridade. Em vez de perguntar se a história é verdadeira, a pessoa passa a pensar em como impedir a consequência anunciada. A ameaça ocupa toda a atenção. Se houver também prazo curto — “pague agora”, “não desligue”, “não conte a ninguém” — a possibilidade de comparação com uma fonte externa diminui.

O segredo tem função especial porque isola. Um terceiro pode perceber rapidamente uma incoerência que, sob pressão, a vítima não percebe. Por isso, ordens para não conversar com familiares, colegas, banco, advogado, polícia ou outras pessoas de confiança merecem atenção. O isolamento favorece o controle da narrativa.

Em situações íntimas, a ameaça de exposição pode ser particularmente poderosa. Campanhas oficiais brasileiras de enfrentamento à violência digital reconhecem a sextorsão como forma de chantagem ou ameaça de caráter sexual praticada por meios digitais.[33] Situações assim exigem linguagem cuidadosa: ter compartilhado conteúdo íntimo, conversado com alguém ou acreditado em determinada relação não transforma a pessoa ameaçada em responsável pela extorsão.

Vergonha também pode surgir em fraudes sem conteúdo sexual. A vítima pode temer o julgamento da família, dos colegas ou de si mesma. Esse sentimento pode impedir que ela peça uma segunda opinião justamente quando ainda seria possível interromper pagamentos, preservar provas ou reduzir danos.

Por isso, um princípio de proteção é trazer a situação de volta ao mundo compartilhado. Uma ameaça que só funciona enquanto permanece secreta perde parte de sua força quando é examinada por alguém confiável ou por uma instituição legítima. O procedimento

específico depois de uma ameaça ou de um prejuízo será tratado adiante; aqui importa perceber que o segredo imposto pelo golpista não deve comandar a decisão.

8.5 Por que é tão difícil admitir que fomos enganados

Descobrir um golpe não é apenas descobrir que uma informação era falsa. Pode significar reconhecer que dinheiro, tempo, confiança, afeto ou esperança foram investidos em uma história que não existia como parecia existir. Quanto maior esse investimento, mais dolorosa pode ser a mudança de interpretação.

Uma revisão sistemática publicada em 2026 sobre consequências psicológicas da vitimização por fraude encontrou, em diferentes modalidades, efeitos como sofrimento emocional, vergonha, ansiedade, redução de confiança e outros impactos psicossociais.[34] Esses resultados não significam que toda vítima desenvolverá os mesmos sintomas. Mostram, porém, que o dano pode ultrapassar a dimensão financeira e que reações intensas depois do golpe não são um detalhe irrelevante.

Nas fraudes amorosas, esse efeito pode ser ainda mais complexo porque interromper a fraude também pode significar perder uma relação na qual a pessoa acreditava. Estudos com vítimas descrevem dificuldade de cessação, sofrimento e necessidade de apoio, além do prejuízo material.[31] A pessoa pode estar tentando aceitar duas perdas ao mesmo tempo: o dinheiro e a história afetiva.

Existe também uma pressão produzida pelo que já foi investido. Depois de vários pagamentos, pode parecer que parar agora tornaria certa toda a perda anterior. O golpista pode explorar esse momento prometendo que falta apenas uma última taxa, um último documento, um último depósito para liberar o dinheiro, resolver o problema ou finalmente cumprir o encontro prometido. O novo pagamento passa a parecer uma maneira de salvar os anteriores.

Essa lógica merece ser interrompida. Dinheiro já enviado não se torna mais recuperável porque se envia mais. Tempo já investido não

torna a história verdadeira. Afeto já construído não confirma a identidade de quem o recebeu. Cada nova decisão precisa ser avaliada pelo que pode acontecer a partir daquele ponto, e não pela necessidade de justificar decisões anteriores.

A vergonha pode dificultar essa interrupção. Admitir a suspeita para outra pessoa pode parecer equivalente a admitir ingenuidade. Mas essa associação é falsa e contraproducente. Como vimos desde o início do livro, golpes funcionam porque combinam contexto, credibilidade, pressão e ação. Reconhecer que esse processo pode ter funcionado é uma etapa de proteção, não um julgamento sobre inteligência ou caráter.

Por isso, uma pergunta mais útil do que “como eu pude acreditar?” é: “o que ainda posso verificar e impedir agora?”. Essa mudança desloca a atenção do passado, que não pode ser desfeito, para as próximas decisões, que ainda podem ser controladas.

O aprendizado transferível deste capítulo é direto: quando uma situação produz emoção intensa e, ao mesmo tempo, exige decisão imediata, a necessidade de verificar aumenta, não diminui. Afeto, medo, compaixão e vergonha são experiências humanas legítimas. A proteção começa quando elas deixam de ser tratadas como prova da história que as provocou.

No próximo capítulo, essa distinção se torna ainda mais importante. Até aqui, vimos como sentimentos podem tornar uma narrativa convincente. A seguir, veremos como tecnologia pode tornar convincentes também imagens, vozes, mensagens e outros sinais que antes pareciam suficientes para confirmar o que vemos e ouvimos.

CAPÍTULO 9

QUANDO JÁ NÃO PODEMOS CONFIAR NO QUE VEMOS E OUVIMOS

9.1 A fraude no ambiente digital

O golpe não se tornou digital porque surgiu uma nova natureza humana. Tornou-se digital porque parte da nossa vida passou a acontecer em telas, aplicativos, contas e serviços conectados. O fraudador acompanha esse deslocamento. Em vez de precisar entregar um documento falso em mãos, pode enviar uma mensagem. Em vez de montar uma loja física, pode copiar a aparência de um site. Em vez de convencer uma pessoa a revelar uma senha numa conversa presencial, pode conduzi-la a uma página que parece legítima.

Phishing é um bom exemplo dessa adaptação. O nome descreve tentativas de induzir alguém a clicar, entrar, informar ou confirmar algo em um ambiente controlado pelo fraudador. A abordagem pode chegar por e-mail, SMS, aplicativo de mensagens, rede social, ligação ou QR Code. O Ministério das Comunicações lembra que essas campanhas podem buscar CPF, senhas, códigos de autenticação, dados bancários e números de cartão, usando urgência, promessa de benefício ou alerta sobre um suposto problema.[35] O mecanismo é antigo; o caminho tecnológico é que muda.

Um link, por exemplo, não é perigoso apenas porque “leva para a internet”. Ele é uma instrução de destino. Se o destino foi escolhido

pelo golpista, a vítima pode chegar a uma página que copia cores, logotipo, textos e até partes do endereço de uma instituição verdadeira. O problema não está na aparência da página, mas em quem controla aquele ambiente e no que será feito com as informações fornecidas ali.

O mesmo raciocínio vale para QR Codes. Eles não têm, por si mesmos, caráter seguro ou inseguro. Funcionam como uma forma rápida de transportar uma informação — muitas vezes um endereço eletrônico ou os dados de uma operação. O Ministério das Comunicações orienta conferir o endereço mostrado pelo aplicativo e, em pagamentos, o nome do destinatário e o valor antes de concluir a operação.[39] Um quadrado impresso em um boleto, cartaz, mesa ou embalagem continua exigindo atenção ao destino para o qual conduz.

Aplicativos também podem fazer parte do processo. A vítima pode ser orientada a instalar um programa apresentado como atualização, suporte, comprovante ou ferramenta necessária para resolver um problema. Em outros casos, o objetivo não é instalar nada, mas obter uma senha, um código temporário ou aprovação de login. Senhas e códigos de autenticação têm valor justamente porque permitem que um sistema trate quem os possui como usuário autorizado. Entregá-los a um terceiro pode significar entregar parte da própria capacidade de acesso.

Tomada de conta é diferente de perfil falso. No perfil falso, alguém cria outro canal e imita uma pessoa ou instituição. Na tomada de conta, o fraudador passa a controlar a conta verdadeira ou uma sessão válida. Essa diferença explica por que uma mensagem pode vir de um perfil realmente pertencente a um conhecido e ainda assim não ter sido escrita por ele. O sinal visual de autenticidade da conta continua existindo, mas quem está operando aquele acesso mudou.

Por isso, no ambiente digital, reconhecer a interface não basta. É preciso considerar também o caminho de acesso, a origem da mensagem, o endereço utilizado, a ação solicitada e a consequência daquela ação. A tecnologia pode reproduzir aparência com enorme precisão; a verificação precisa olhar além dela.

9.2 Redes sociais e exposição de informações

Redes sociais não são apenas vitrines públicas. Elas são também arquivos de contexto. Fotografias, comentários, marcações, viagens, aniversários, profissão, parentes, escola dos filhos, cidade, hábitos e eventos podem parecer informações banais quando vistas separadamente. Combinadas, podem ajudar alguém a construir uma abordagem muito mais convincente.

O CERT.br orienta os usuários a evitar exposição excessiva e lembra que informações compartilhadas em redes podem ser usadas de forma abusiva, inclusive para tentativas de personificação.[36] Isso não significa que publicar uma fotografia ou contar onde trabalha seja a causa de um golpe. A responsabilidade pela fraude permanece de quem a pratica. O ponto preventivo é outro: informações públicas podem reduzir o trabalho necessário para tornar uma história falsa plausível.

Imagine uma mensagem que menciona corretamente o nome de um irmão, uma viagem recente e a empresa em que você trabalha. Nenhum desses dados, isoladamente, prova a identidade do remetente. Mas a combinação pode produzir a sensação de que “essa pessoa sabe demais para ser falsa”. Esse efeito já apareceu no Capítulo 6. Aqui importa perceber uma das fontes possíveis dessa familiaridade: aquilo que nós mesmos, nossos contatos ou organizações publicam no ambiente digital.

A exposição também pode revelar momentos de oportunidade. Uma postagem informando que alguém está viajando, procurando emprego, vendendo um carro ou celebrando uma compra pode ajudar a escolher o tema de uma abordagem. O fraudador não precisa saber toda a vida da vítima; basta ter contexto suficiente para não parecer completamente aleatório.

Administrar exposição não significa desaparecer da internet. Significa escolher melhor o que precisa ser público, revisar quem pode ver determinadas informações e evitar publicar dados que aumentem desnecessariamente a capacidade de terceiros imitarem você ou responderem perguntas de segurança. Também significa lembrar que

a privacidade de uma pessoa depende parcialmente do que familiares, amigos e empresas publicam sobre ela.

Quanto mais informação um contato suspeito demonstra conhecer, maior pode ser a impressão de autenticidade. A resposta adequada não é entrar em pânico com a existência desses dados, mas voltar ao princípio já consolidado: informação correta prova que alguém conhece a informação; não prova quem é esse alguém.

9.3 Inteligência artificial e conteúdo sintético

A inteligência artificial generativa ampliou a capacidade de produzir texto, imagem, áudio e vídeo com aparência plausível. Isso não significa que todo conteúdo estranho seja artificial, nem que qualquer golpe moderno dependa de IA. Significa apenas que uma nova ferramenta passou a estar disponível para criar, adaptar e escalar materiais usados em histórias fraudulentas.

Em 2024, o FBI já alertava para o uso de inteligência artificial generativa em fraudes financeiras, incluindo textos, imagens, vídeos e áudios sintéticos.[5] No Brasil, em 2026, a Anatel passou a alertar especificamente para fraudes com vídeos, áudios e imagens manipuladas capazes de imitar rostos, vozes e comportamentos de pessoas conhecidas.[37] São registros de uso e risco documentados; não previsões sobre um futuro hipotético.

Deepfake é um termo frequentemente usado para conteúdos de áudio, imagem ou vídeo modificados ou gerados com técnicas de inteligência artificial de modo a produzir elevado realismo. A Agência Nacional de Proteção de Dados publicou, em 2026, um Radar Tecnológico dedicado ao tema, tratando dessas capacidades e dos riscos associados à proteção de dados e aos ambientes digitais.[38] A tecnologia pode ser usada para finalidades legítimas, criativas e educativas; o problema surge quando a aparência sintética é usada para enganar, personificar, constranger ou obter vantagem.

O texto sintético merece atenção pelo mesmo motivo. Uma mensagem bem escrita, coerente e personalizada já não exige necessariamente que alguém a tenha redigido palavra por palavra.

Ferramentas podem ajudar a corrigir idioma, adaptar tom, produzir variações e responder rapidamente. Isso reduz o valor preventivo de um antigo conselho: “golpes têm muitos erros de português”. Alguns ainda têm. Outros não.

Imagens sintéticas também podem funcionar como peças de credibilidade. Uma fotografia pode ser fabricada; uma imagem verdadeira pode ser alterada; um cenário pode ser criado; uma captura de tela pode ser montada. O leitor não precisa aprender técnicas de perícia digital para concluir algo mais simples: uma imagem, sozinha, mostra o que está na imagem, não necessariamente como ela foi produzida nem quem a enviou.

Com áudio, o efeito pode ser mais forte porque a voz carrega memória afetiva. Uma fala curta, com timbre e ritmo semelhantes aos de alguém conhecido, pode reduzir a vontade de conferir. Mas a existência de clonagem de voz não transforma toda ligação familiar em suspeita. Ela apenas retira da voz o status de prova final de identidade quando a conversa exige dinheiro, credenciais, segredo ou outra decisão relevante.

O ponto decisivo não é tentar adivinhar se determinado conteúdo “foi feito por IA”. Essa pergunta pode ser difícil até para especialistas e, em muitos casos, é desnecessária. Para a prevenção, basta reconhecer que conteúdo convincente pode ser produzido ou manipulado e que decisões importantes não devem depender exclusivamente dele.

9.4 A crise da evidência aparente

Fotografia, voz, vídeo, documento e site profissional continuam tendo valor. O erro seria concluir o contrário e transformar o mundo digital em um lugar onde nada merece confiança. A mudança é mais precisa: esses elementos nem sempre bastam, isoladamente, para encerrar uma verificação.

Por muito tempo, ver uma pessoa em vídeo podia parecer confirmação quase definitiva de que ela estava realmente ali. Ouvir uma voz conhecida parecia confirmar quem estava do outro lado. Receber uma fotografia de documento parecia aproximar a conversa

da formalidade. Encontrar um site bem construído parecia sinal de empresa consolidada. Cada um desses elementos ainda pode contribuir para a credibilidade. Mas todos podem ser copiados, manipulados, encenados ou retirados de contexto.

É útil separar conteúdo e origem. O conteúdo responde: “o que estou vendo ou ouvindo?”. A origem responde: “de onde isso veio e quem controla o canal pelo qual chegou até mim?”. Um documento pode ser verdadeiro e ter sido enviado por um impostor. Uma fotografia pode ser verdadeira e estar ligada a uma história falsa. Uma voz pode se parecer com a de um familiar sem que o canal de comunicação pertença a ele. Um site pode reproduzir perfeitamente uma marca sem ser controlado pela empresa imitada.

A confirmação mais forte costuma introduzir alguma independência. Se uma mensagem diz que há problema no banco, o leitor procura o banco por um canal que já conhecia. Se um vídeo pede uma transferência, confirma-se o pedido por outro meio. Se um QR Code promete levar a determinado serviço, observa-se o endereço e o destinatário antes de prosseguir. Se uma conta pede um código, vale perguntar por que aquele código está sendo solicitado e quem realmente deveria recebê-lo.

Essa mudança de raciocínio evita dois extremos. O primeiro é a credulidade automática: “se vi, ouvi ou recebi, então é verdadeiro”. O segundo é o ceticismo absoluto: “nada digital pode ser confiável”. O caminho útil fica entre os dois. Evidências aparentes continuam informando, mas seu peso precisa ser proporcional ao risco da decisão.

Quanto maior a consequência — dinheiro, acesso a contas, documentos, dados sensíveis, instalação de programas ou decisões difíceis de desfazer — mais importante se torna combinar sinais. A tecnologia não eliminou a possibilidade de saber o que é verdadeiro. Ela apenas elevou o custo de tratar aparência como confirmação suficiente.

9.5 Tecnologia também protege

A tecnologia que facilita a falsificação também cria barreiras contra ela. Sistemas podem exigir fatores adicionais de autenticação, alertar sobre acessos, limitar tentativas, identificar comportamentos anormais, atualizar falhas conhecidas e permitir recuperação de contas. Parte da proteção acontece antes de a pessoa perceber que existe um golpe.

Para o público geral, algumas medidas oferecem benefício alto sem transformar segurança em profissão. Uma delas é usar autenticação em duas etapas ou em múltiplos fatores quando o serviço oferecer o recurso. O Ministério das Comunicações inclui essa recomendação entre as medidas de prevenção contra phishing, juntamente com a manutenção de sistemas e aplicativos atualizados.[35] O objetivo é criar uma barreira adicional caso uma senha seja descoberta ou reutilizada por terceiros.

Senhas continuam importantes, mas não precisam carregar sozinhas toda a segurança. Senhas únicas para serviços relevantes reduzem o efeito de um vazamento em cadeia. Gerenciadores de senhas podem ajudar a criar e armazenar credenciais distintas. Atualizações de sistema e aplicativos corrigem falhas e mantêm mecanismos de proteção funcionando de acordo com versões mais recentes.

Controles de privacidade também têm função preventiva. Limitar a exposição pública não impede personificação, mas pode reduzir a quantidade de material disponível para personalização de abordagens. Alertas de login e notificações de segurança, quando oferecidos, ajudam a perceber acessos ou tentativas que não foram iniciados pelo usuário.

Há ainda uma regra simples sobre códigos de autenticação: eles devem ser tratados como credenciais, não como números neutros. Se um serviço envia um código para confirmar acesso, redefinir senha ou autorizar operação, o recebimento desse código não cria obrigação de repassá-lo a quem entrou em contato. Antes de usar ou compartilhar qualquer código, é preciso entender qual ação ele autoriza.

Nenhuma dessas medidas oferece imunidade. Autenticação adicional pode ser contornada em alguns cenários; sistemas podem falhar; usuários podem ser induzidos a aprovar ações. Ainda assim, a existência de limites não torna as proteções inúteis. Segurança prática costuma resultar de camadas: hábitos, controles técnicos e verificação independente trabalhando juntos.

Este capítulo não pede que o leitor desconfie de tudo o que vê ou ouve. Pede algo mais específico: que não confunda realismo com autenticidade. No ambiente contemporâneo, uma voz pode soar verdadeira, uma imagem pode parecer perfeita e uma página pode reproduzir cada detalhe visual de uma instituição. O que transforma aparência em confiança suficiente é a possibilidade de confirmar a origem e a ação por caminhos adequados.

Esse passo prepara o próximo capítulo. O leitor já possui as peças necessárias; agora elas serão organizadas em um método simples para decidir o que fazer diante de uma situação suspeita.

CAPÍTULO 10

PARE, CONFIRA, DEPOIS DECIDA

10.1 Reconheça a situação de risco

Depois de conhecer tantas formas de fraude, existe um risco curioso: imaginar que a proteção depende de reconhecer exatamente qual golpe está acontecendo. Não depende. Na maioria das situações, o leitor não precisa dar nome à fraude antes de perceber que alguma coisa exige cuidado. Precisa apenas notar que está diante de uma decisão com consequência relevante e que alguém está tentando conduzi-la com rapidez, pressão ou informação insuficiente.

Os sinais mais úteis são os que mudam a forma como devemos decidir. Um contato inesperado pede dinheiro, senha, código, documento, instalação de aplicativo ou acesso a uma conta. Uma pessoa conhecida aparece por um canal diferente. Um suposto funcionário afirma que é preciso agir imediatamente. Uma oportunidade exige pagamento antes de ser verificada. Um comprador envia comprovante e pressiona pela entrega. Um interlocutor pede segredo, ameaça prejuízo ou afirma que qualquer demora fará perder uma vantagem. Nenhum desses elementos prova, sozinho, que existe fraude. Todos justificam aumentar a verificação.

Também merece atenção a mudança de procedimento. A empresa que sempre recebia de uma forma passa a indicar outra conta. O banco que normalmente se comunica pelo aplicativo supostamente pede uma operação por telefone. O advogado que costumava falar de

determinado número passa a solicitar pagamento por outro canal. O parente que sempre ligava pede ajuda apenas por mensagem. Mudanças podem ser legítimas, mas o próprio fato de haver mudança retira parte das referências que tornavam a situação familiar.

O mesmo vale para pedidos que ampliam o poder de outra pessoa sobre você: compartilhar um código, fotografar um documento, permitir acesso remoto ao dispositivo, instalar um programa, autorizar uma operação, informar credenciais ou enviar dinheiro para um terceiro. A pergunta prática não é “isso parece golpe?”. É: “o que exatamente estão tentando me fazer fazer, e o que acontece se eu fizer?”.

Essa pergunta desloca a atenção da história para a ação. A narrativa pode envolver banco, emprego, prêmio, filho, processo judicial, compra, investimento ou emergência. O pedido concreto costuma ser mais simples: transferir, clicar, instalar, fornecer, autorizar, entregar ou permanecer em segredo. Quando a consequência é importante ou difícil de desfazer, a exigência de confirmação deve aumentar.

Reconhecer risco, portanto, não é concluir que o outro está mentindo. É admitir que ainda não há informação suficiente para agir com segurança. Essa distinção evita dois erros opostos: confiar automaticamente porque a história parece plausível e acusar automaticamente porque algum sinal parece estranho. O objetivo é criar espaço para conferir.

10.2 Interrompa o roteiro do golpista

Golpes funcionam melhor quando a vítima permanece dentro do roteiro criado pelo fraudador. Cada resposta leva à próxima instrução; cada instrução reduz o tempo disponível para pensar; cada nova informação parece confirmar a anterior. A primeira defesa, por isso, pode ser surpreendentemente simples: interromper a sequência.

Interromper não significa discutir, desafiar ou tentar desmascarar alguém. Muitas vezes significa apenas não executar a próxima ação. Não clicar agora. Não transferir agora. Não instalar agora. Não ditar o código agora. Não entregar o bem agora. Não confirmar a senha agora.

Quando for adequado, significa encerrar a ligação, fechar a conversa ou sair do ambiente para verificar por outro caminho.

Essa pausa tem valor porque devolve duas coisas que a pressão tenta retirar: tempo e escolha. Enquanto o interlocutor controla o ritmo, a pessoa reage a estímulos sucessivos. Quando a sequência é interrompida, a decisão volta a pertencer a quem sofrerá a consequência.

A urgência verdadeira pode existir. Uma conta pode ter problema real. Um familiar pode realmente precisar de ajuda. Um prazo pode ser curto. Uma compra pode depender de resposta rápida. Mas urgência legítima não transforma qualquer instrução recebida em obrigação de obedecer sem confirmação. Quanto maior a pressão para impedir conferência, maior a razão para criar distância antes de agir.

Também não é recomendável continuar uma conversa suspeita apenas para “ver até onde vai”. Além de prolongar a exposição, isso pode fornecer novas informações ao interlocutor, aumentar a persuasão e criar oportunidades para novos pedidos. Para o público geral, investigar o fraudador não é requisito de proteção. O objetivo é interromper a influência sobre a decisão e sair do canal controlado por quem está fazendo o pedido.

Uma frase mental ajuda: “eu não preciso resolver isso neste canal”. Se a situação for legítima, haverá alguma forma adequada de confirmar. Um banco continuará existindo quando a ligação terminar. Uma empresa poderá ser encontrada por seus meios oficiais. Um familiar poderá ser procurado pelo contato habitual. Um profissional verdadeiro poderá ser identificado por cadastro ou canal independente. A legitimidade não depende de manter você preso à mesma conversa.

10.3 Verifique fora da história que lhe contaram

A verificação independente é o centro deste capítulo. Significa confirmar uma afirmação por uma fonte que não dependa do próprio contato que está sendo verificado. Se uma mensagem diz que veio do banco, não basta ligar para o número indicado na mensagem. Se alguém diz representar uma empresa, não basta abrir o link que ele enviou. Se um perfil afirma ser de um familiar, não basta perguntar ao próprio perfil se ele é verdadeiro.

O caminho mais forte costuma começar em uma referência que você já possuía antes da abordagem: o aplicativo instalado anteriormente, o número salvo e conhecido, o endereço digitado por você, o site encontrado a partir de fonte confiável, o cadastro profissional, o contato presencial ou outra pessoa que possa confirmar o fato sem depender do interlocutor suspeito. O Banco Central, por exemplo, recomenda confirmar pedidos de transferência feitos por conhecidos e, em caso de dúvida, recorrer aos canais oficiais da instituição financeira.[28]

É importante separar quatro perguntas. A primeira: quem está falando comigo? A segunda: o fato narrado realmente aconteceu? A terceira: a ação que estão pedindo é realmente necessária? A quarta: o destinatário, a conta, o endereço ou o ambiente para o qual estou sendo conduzido é o correto? Uma confirmação pode responder apenas uma dessas perguntas. Saber que existe um processo judicial verdadeiro não confirma que o remetente seja o advogado. Saber que existe uma dívida não confirma aquele boleto. Saber que o parente está viajando não confirma o pedido de dinheiro.

A verificação deve acompanhar a consequência. Para uma informação sem impacto, uma confirmação simples pode bastar. Para enviar dinheiro, entregar documentos, permitir acesso a uma conta ou instalar software, é razoável exigir evidência mais forte. Quando duas confirmações independentes são fáceis de obter, combiná-las costuma ser melhor do que depender de um único sinal.

Pessoas de confiança também podem funcionar como segunda fonte. Em situações emocionalmente intensas, explicar a história a

alguém de fora ajuda a reconstruir o problema sem a pressão original. Isso não transfere a decisão para outra pessoa; amplia a informação disponível. O segredo exigido pelo interlocutor é especialmente perigoso quando serve para impedir exatamente esse tipo de conferência.

Verificar fora da história também significa desconfiar de confirmações que acontecem todas dentro do mesmo ambiente. Um site pode mostrar um telefone que pertence ao próprio fraudador. Um e-mail pode indicar outro endereço controlado pela mesma estrutura. Um falso atendente pode "transferir" a ligação para um segundo falso setor. Uma plataforma fraudulenta pode exibir documentos, avaliações e saldos produzidos para reforçar a narrativa. A independência da fonte importa tanto quanto a quantidade de sinais.

O objetivo não é encontrar certeza absoluta. Muitas decisões da vida são tomadas com informação incompleta. O que se busca é confirmação suficiente para o risco envolvido. Se a verificação falha, é contraditória ou só pode ser feita pelos meios oferecidos por quem deseja a ação, a decisão mais prudente pode ser não prosseguir até que exista uma fonte independente.

10.4 Proteja antes de precisar

A melhor hora para criar algumas barreiras é antes da emergência. Sob medo, pressa ou cansaço, depender apenas de atenção e memória é uma estratégia frágil. Controles simples podem reduzir o número de decisões que precisam ser improvisadas.

Contas importantes devem, quando possível, usar autenticação em duas etapas ou múltiplos fatores. Senhas relevantes devem ser diferentes entre serviços, e um gerenciador de senhas pode ajudar a manter essa separação. Sistemas e aplicativos precisam permanecer atualizados. O Ministério das Comunicações inclui autenticação adicional e atualização de dispositivos entre as medidas recomendadas contra phishing.[35] Essas medidas não impedem toda fraude, mas adicionam barreiras caso uma credencial seja descoberta, reutilizada ou capturada.

Códigos de autenticação merecem uma regra própria: trate-os como credenciais. O código recebido por SMS, aplicativo ou outro meio pode autorizar acesso, redefinição de senha ou operação. O fato de alguém saber que você recebeu um código não significa que essa pessoa deva recebê-lo. Antes de digitar ou compartilhar qualquer código, descubra qual ação ele está autorizando e em qual ambiente.

No celular e no computador, bloqueio de tela, atualizações, cuidado com aplicativos e atenção às permissões reduzem exposição. Em redes sociais, configurações de privacidade e limitação de dados desnecessariamente públicos reduzem material disponível para personalização de abordagens. O CERT.br recomenda, entre outras medidas, restringir informações públicas, proteger contas com verificação em duas etapas e revisar configurações de segurança e privacidade.[36]

Na vida financeira, limites compatíveis com a rotina podem reduzir a consequência de uma decisão equivocada. Alertas e notificações ajudam a perceber operações. Para pagamentos, vale desenvolver o hábito de conferir beneficiário, valor e contexto no ambiente em que a operação será concluída. Para compras e vendas, não substituir confirmação efetiva por comprovante enviado por outra pessoa.

Documentos pessoais também merecem parcimônia. Nem todo cadastro precisa de todos os dados. Quando for necessário enviar cópia, é útil saber para quem está sendo entregue, por qual motivo e em qual ambiente. A mesma lógica vale para fotografias do rosto, documentos e informações cadastrais: quanto maior o potencial de uso posterior, maior a importância de confirmar a finalidade e o destinatário.

Há ainda uma proteção que não depende de tecnologia: combinar procedimentos com pessoas próximas. Famílias podem estabelecer como confirmar pedidos urgentes. Empresas podem definir como validar mudança de conta bancária. Sócios podem exigir dupla confirmação para pagamentos incomuns. Pessoas idosas ou com menor familiaridade digital podem escolher alguém de confiança para consultar em situações fora do padrão, sem retirar sua autonomia.

Prevenção permanente e reação a incidente não são a mesma coisa. Este capítulo organiza hábitos e barreiras que devem existir antes do problema. Se já houve pagamento, invasão, compartilhamento de senha, perda de documento ou tomada de conta, a prioridade muda. O Capítulo 11 tratará dessas providências de emergência.

10.5 Um método para o golpe que ainda não existe

O valor de um método aparece quando a situação não se parece exatamente com nenhuma história conhecida. Imagine que, daqui a alguns meses, surja um novo serviço digital. Um contato afirma representar esse serviço, mostra documentos convincentes, conhece dados verdadeiros sobre você e diz que existe um benefício a liberar. Para receber, é necessário instalar uma ferramenta, autenticar com um código e confirmar uma pequena operação financeira.

Você talvez nunca tenha ouvido falar daquela modalidade. Ainda assim, não está desarmado. Primeiro, PARE. A sequência contém decisões relevantes e está sendo conduzida por alguém que controla a narrativa. Não é necessário descobrir imediatamente se o documento é falso, se a voz foi clonada ou se o serviço existe.

Depois, IDENTIFIQUE. O que está sendo pedido? Instalação, código e operação financeira. Em nome de quem? De um serviço que afirma ter relação com você. Qual a consequência? Entregar acesso e autorizar uma ação que pode ser difícil de reverter. Quais sinais elevam o risco? Contato inesperado, vantagem prometida, necessidade de agir dentro do canal oferecido e pedido de credenciais.

Em seguida, CONFIRA. Você sai do contato. Procura o serviço por caminho independente. Verifica se a empresa existe, se mantém relação com você e se realmente oferece aquela vantagem. Se houver conta, entra pelo aplicativo ou endereço que já conhece. Se houver dúvida, procura suporte oficial sem utilizar os links recebidos. Se o pedido envolver terceiro conhecido, confirma por outro meio.

Só então, DECIDA. Se a história for confirmada e a operação fizer sentido, você pode prosseguir pelo caminho oficial. Se houver contradição, ausência de confirmação ou pressão para retornar ao

canal inicial, você não executa a ação. A decisão deixa de depender da habilidade de reconhecer o golpe e passa a depender da qualidade da confirmação.

O mesmo método serve para uma mensagem de parente, uma cobrança, uma vaga de emprego, uma compra, um investimento, um profissional, uma emergência ou uma tecnologia que ainda não existe hoje. As histórias mudam; as perguntas essenciais permanecem.

PARE significa interromper a pressão e recuperar tempo. IDENTIFIQUE significa traduzir a narrativa em pedido concreto, identidade alegada e consequência. CONFIRA significa buscar evidência adequada por caminho independente. DECIDA significa agir apenas depois que a verificação for proporcional ao risco.

PARE IDENTIFIQUE CONFIRA DECIDA

Esse método não promete imunidade e não transforma qualquer situação incomum em fraude. Sua função é mais modesta e mais útil: impedir que aparência, pressão, emoção ou familiaridade sejam confundidas com confirmação. O leitor não precisa conhecer o próximo golpe. Precisa saber como recuperar o controle da decisão.

CAPÍTULO 11

CAÍ NO GOLPE. E AGORA?

11.1 Primeiro: interrompa o dano

Se você acabou de perceber que pode ter caído em um golpe, a prioridade não é descobrir todos os detalhes. É impedir que o prejuízo aumente. Não faça novos pagamentos, não envie outra “taxa”, não forneça mais códigos, não instale programas adicionais e não continue seguindo instruções de quem conduziu a situação. Se ainda houver contato com o possível golpista, interrompa a sequência.

A providência seguinte depende do que já aconteceu. Se houve transferência ou pagamento, acione imediatamente a instituição financeira pelos canais oficiais. Se você forneceu senha, código ou aprovou acesso, proteja as contas envolvidas. Se instalou aplicativo desconhecido ou permitiu acesso remoto, trate o dispositivo como potencialmente comprometido. Se entregou documento ou muitos dados pessoais, pense também no risco de uso da sua identidade. Se uma conta de rede social foi tomada, inicie o processo oficial de recuperação da própria plataforma.

Essa separação é importante porque “caí num golpe” descreve situações muito diferentes. Uma pessoa pode ter enviado dinheiro voluntariamente sob engano; outra pode descobrir transações que nunca autorizou; outra pode ter perdido o controle de uma conta; outra pode ter apenas fornecido documentos. Misturar tudo numa única resposta pode desperdiçar o tempo mais importante.

O Banco Central orienta vítimas de golpes financeiros a contatar o banco e registrar Boletim de Ocorrência, e recomenda rapidez nas providências.[40] A velocidade, porém, deve servir à contenção, não ao pânico. A vítima não precisa telefonar para todos os lugares ao mesmo tempo. Precisa identificar o que ainda está exposto e agir primeiro sobre aquilo que pode produzir novo dano.

Anote, em poucas linhas, o que ocorreu: quando começou, por qual canal, o que você fez, quais valores foram enviados, quais dados foram fornecidos, quais contas ou dispositivos podem ter sido afetados. Essa pequena cronologia ajuda a organizar as próximas decisões justamente quando memória, medo e pressa estão disputando atenção.

11.2 Proteja dinheiro, contas e dispositivos

Se houve movimentação financeira, procure a instituição envolvida por canal oficial: aplicativo que você já usava, telefone do cartão, site digitado por você ou atendimento presencial. Informe que se trata de suspeita de fraude, identifique as operações e siga o procedimento de contestação aplicável. Não volte ao número, link ou “atendente” que participou do golpe para pedir ajuda.

No Pix, existe o Mecanismo Especial de Devolução, o MED. Segundo as regras vigentes consultadas para esta edição, a vítima deve comunicar sua instituição e solicitar a devolução; o pedido pode ser registrado em até 80 dias da transação, mas o próprio Banco Central ressalta que agir rapidamente aumenta as chances de recuperação. O MED não garante devolução: o resultado depende da análise do caso e da existência de recursos que possam ser bloqueados e devolvidos.[15]

Para TED, cartão, boleto e outras formas de pagamento, não suponha que o procedimento seja o mesmo do Pix. Informe imediatamente o banco ou emissor, identifique a operação e peça orientação sobre contestação, bloqueio ou tentativa de recuperação adequada àquele meio. O importante é não perder tempo procurando um mecanismo que não se aplica ao caso.

Se você não reconhece transações ou suspeita que alguém entrou na sua conta, a orientação do Ministério da Justiça é contatar o banco por

canais oficiais, contestar as movimentações, trocar a senha, cancelar cartões virtuais comprometidos e verificar transações agendadas ou resgates.[41] Faça alterações de segurança a partir de um dispositivo que você considere confiável.

Se o dispositivo usado no golpe pode estar comprometido — por exemplo, após instalação de programa desconhecido, acesso remoto ou comportamento anormal — evite continuar usando esse mesmo aparelho para acessar serviços sensíveis até resolver o problema. O CERT.br recomenda, em caso de suspeita de malware, alterar as senhas em outro dispositivo considerado seguro ou somente depois de o equipamento afetado ter sido saneado.[46] A ideia é simples: trocar a senha num aparelho ainda controlado por terceiro pode expor a nova senha também.

Se uma conta de e-mail, rede social ou aplicativo foi invadida, use as ferramentas oficiais de recuperação do serviço, altere credenciais relacionadas e avise pessoas próximas caso o perfil possa estar sendo usado para abordá-las. O Ministério da Justiça também recomenda denunciar perfis falsos ou contas clonadas pelos canais da própria plataforma e não pagar “resgate” exigido por quem tomou a conta.[24]

Em perda, furto ou roubo do celular, há uma situação adicional: o aparelho pode conter sessões abertas, aplicativos bancários, mensagens e dados. O Programa Celular Seguro permite, para aparelhos cadastrados e situações abrangidas pelo serviço, emitir alerta e acionar medidas de bloqueio junto a parceiros.[43] Isso não substitui o contato com bancos, operadora e demais serviços que possam estar expostos; é mais uma camada de contenção.

Se documentos ou dados pessoais foram entregues e você teme abertura de contas em seu nome, o Banco Central mantém o BC PROTEGE+, serviço gratuito que permite comunicar ao sistema financeiro que você não deseja abertura de determinadas contas nem inclusão como titular ou representante enquanto a proteção estiver ativa.[44] O recurso cobre contas correntes, poupança e contas de pagamento pré-pagas nos limites informados pelo BC; não deve ser tratado como bloqueio universal de qualquer uso indevido do CPF. O

Registrato e o relatório de Contas e Relacionamentos também podem ajudar a observar vínculos bancários em seu nome.[23]

11.3 Preserve as provas

Depois de conter o que for urgente, preserve o que mostra como o fato aconteceu. Não apague a conversa por vergonha, raiva ou vontade de "encerrar o assunto". Mensagens, números de telefone, nomes de perfis, e-mails, endereços de páginas, anúncios, comprovantes, extratos, boletos, documentos recebidos, protocolos e registros de chamadas podem ser relevantes para bancos, plataformas, polícia e eventual medida jurídica.

Quando puder, guarde mais do que uma fotografia isolada. Preserve a conversa completa ou trechos suficientes para mostrar a sequência, a data e o contexto. Em e-mail, mantenha a mensagem original na caixa postal além de capturas de tela. Em páginas e anúncios, registre o endereço eletrônico e a aparência. Em transferências, conserve o comprovante e o extrato. Se houver nome, CPF ou CNPJ do destinatário visível na operação, guarde essa informação.

O Ministério da Justiça recomenda, em casos de conta invadida ou perfil clonado, salvar prints das mensagens e do perfil e incluir no registro policial dados como contato suspeito, número utilizado, data, horário, valores, destino da transferência e demais evidências disponíveis.[24] A mesma lógica vale para outras fraudes: organize aquilo que você já possui; não tente fabricar prova nem se exponha para conseguir informação adicional.

Faça uma cronologia curta. Algo como: "14h10 — recebi a ligação; 14h18 — instalei o aplicativo; 14h27 — fiz o Pix; 14h40 — percebi a fraude; 14h46 — contatei o banco". Esse encadeamento facilita explicar o caso várias vezes sem depender apenas da memória.

Guarde também protocolos de atendimento e respostas recebidas. Eles registram quando você comunicou o fato e o que foi solicitado. Não é necessário dominar técnicas de perícia digital. Para a maioria das pessoas, preservar os registros existentes, manter os arquivos

originais quando possível e organizá-los já melhora muito a capacidade de demonstrar o ocorrido.

11.4 Comunique e registre

Comunicar o golpe não é uma única ação. Há pelo menos três objetivos diferentes: interromper ou contestar operações; avisar a plataforma ou serviço cuja conta, perfil ou infraestrutura foi usada; e registrar o fato perante a autoridade policial. Um desses passos não substitui automaticamente os outros.

Se houve dinheiro, fale com a instituição financeira. Se houve perfil falso, conta invadida, anúncio fraudulento ou conteúdo malicioso, use os canais de denúncia e recuperação da plataforma. Se houve linha telefônica, dispositivo perdido ou tomado, acione os serviços correspondentes. Se uma empresa real foi personificada, avisá-la também pode ajudá-la a identificar e retirar canais falsos.

O Boletim de Ocorrência pode ser registrado presencialmente na Polícia Civil ou, quando a ocorrência estiver disponível no sistema do seu estado, pela delegacia virtual. As orientações federais consultadas remetem à delegacia virtual da unidade da Federação de residência da vítima.[41] Leve ou anexe a cronologia e as provas essenciais. Não espere o BO para acionar o banco quando houver operação financeira urgente.

Em outras palavras: o banco tenta lidar com a operação financeira; a plataforma lida com conta, perfil ou conteúdo dentro do serviço; a polícia registra e apura o fato conforme sua competência. Dependendo da situação, ainda pode ser necessário comunicar operadora, empresa personificada, marketplace ou outro intermediário. O objetivo é colocar cada problema diante de quem efetivamente pode agir sobre ele.

Se a resposta de uma instituição financeira não resolver o problema, o Banco Central informa que a vítima pode, conforme o caso, recorrer aos órgãos de defesa do consumidor, ao Poder Judiciário ou registrar reclamação no próprio BC.[40] A análise de direitos, responsabilidade e reparação ficará para o Capítulo 12; aqui o ponto é

não confundir o primeiro contato emergencial com o fim de todos os caminhos possíveis.

11.5 Tente recuperar o que ainda puder ser recuperado

Depois de interromper novos danos e comunicar o fato, tente recuperar o que for possível. A recuperação pode significar dinheiro, controle de uma conta, acesso a um perfil, bloqueio de um cartão, cancelamento de uma operação ainda pendente ou impedimento de uso posterior de dados. Não existe um procedimento único para todas essas situações.

No Pix, o MED é o mecanismo específico para fraude, golpe ou crime nas hipóteses previstas. A instituição analisa o caso e pode haver bloqueio e devolução integral ou parcial conforme os recursos localizados. O prazo para pedir não deve ser interpretado como motivo para esperar: quanto mais cedo a comunicação, maior a possibilidade de ainda existir saldo acessível.[15]

Se a fraude envolveu transferência por outro meio, boleto ou cartão, peça à instituição a providência aplicável àquela operação. Em um boleto falso, por exemplo, o Ministério da Justiça orienta comunicar tanto o banco utilizado no pagamento quanto o banco emissor do boleto e, se houver, a empresa ou marketplace envolvido.[42] A existência de contestação ou tentativa de bloqueio não significa que a recuperação será obtida.

Para contas digitais e redes sociais, a recuperação normalmente depende dos mecanismos oficiais do próprio serviço: redefinição de senha, verificação de identidade, encerramento de sessões, denúncia de perfil falso ou suporte. Para dispositivo comprometido, a prioridade é recuperar um ambiente seguro antes de retomar acessos sensíveis. Para uso indevido de identidade, monitorar vínculos e ativar proteções disponíveis pode reduzir danos futuros mesmo quando nada pode ser “devolvido” naquele momento.

O princípio mais importante é não transformar tentativa em promessa. Dinheiro pode já ter sido transferido para outras contas;

uma plataforma pode precisar verificar identidade; uma instituição pode concluir que determinado mecanismo não se aplica. Rapidez aumenta possibilidades, mas não cria certeza. Essa diferença protege a vítima também contra o próximo risco.

11.6 Não caia no segundo golpe

Quem acabou de sofrer uma fraude pode se tornar alvo de outra. O novo contato sabe exatamente o que a pessoa deseja ouvir: “localizamos seu dinheiro”, “seu valor está bloqueado”, “há uma decisão favorável”, “somos de um setor especial de recuperação” ou “basta pagar uma taxa para liberar a devolução”. A promessa de reparar a primeira perda passa a ser a isca da segunda fraude.

Esse risco não significa que empresas, advogados, bancos ou serviços de recuperação sejam todos suspeitos. Significa que a mesma regra de identidade e procedimento continua valendo. Confirme quem é o profissional ou instituição por fonte independente, verifique como ele obteve seus dados, entenda o serviço oferecido e não trate um documento, protocolo ou logotipo recebido pelo próprio contato como confirmação suficiente.

O Banco Central alerta especificamente para contatos e empresas que dizem atuar junto ao BC para reduzir dívidas ou recuperar valores pagos e orienta procurar diretamente a instituição financeira.[4] Uma abordagem pode usar termos oficiais, números de protocolo e conhecimento real sobre a perda. Nada disso transforma o interlocutor em representante legítimo.

Desconfie especialmente quando a “recuperação” exige novo pagamento urgente, envio de senha ou código, instalação de programa, acesso remoto ou transferência para conta de terceiro. Se a pessoa afirma agir em nome de banco, órgão público ou profissional, saia do contato e localize a instituição ou o profissional por caminho próprio.

A vítima recente costuma estar cansada, frustrada e com forte desejo de desfazer o que aconteceu. É justamente por isso que a recuperação deve ser tratada como uma nova decisão, e não como

continuação automática do caso anterior. Perder dinheiro uma vez não cria obrigação de arriscar mais para tentar recuperá-lo.

11.7 Protocolo imediato

Se você chegou a este capítulo logo depois de descobrir um golpe, use a sequência abaixo como ponto de partida.

1. INTERROMPA — pare pagamentos, transferências, compartilhamento de códigos, instalações e contato com quem conduziu a fraude.

2. DINHEIRO — se houve operação financeira, contate imediatamente o banco ou emissor pelo canal oficial e peça o procedimento de contestação, bloqueio ou recuperação aplicável. Se foi Pix, informe que se trata de suspeita de fraude e solicite o MED.

3. ACESSOS — se forneceu senha, código ou perdeu controle de conta, altere credenciais e encerre acessos suspeitos a partir de dispositivo confiável. Recupere contas pelos mecanismos oficiais.

4. DISPOSITIVO — se instalou programa suspeito ou permitiu acesso remoto, pare de usar o equipamento para operações sensíveis até saneá-lo. Se o celular foi perdido, furtado ou roubado, acione os bloqueios e serviços disponíveis.

5. IDENTIDADE — se documentos ou muitos dados pessoais foram expostos, monitore vínculos em seu nome e avalie proteções específicas, como BC PROTEGE+ para as contas abrangidas pelo serviço.

6. PROVAS — salve conversas, perfis, e-mails, links, comprovantes, extratos, documentos, horários e protocolos. Monte uma cronologia simples.

7. REGISTRE — faça o Boletim de Ocorrência e comunique plataformas, empresas ou serviços envolvidos conforme a natureza do caso.

> 8. ACOMPANHE — monitore contas, cartões, perfis e vínculos relacionados. Responda a novas movimentações rapidamente.

> 9. DESCONFIE DA "RECUPERAÇÃO GARANTIDA" — não faça novo pagamento nem entregue credenciais a quem promete recuperar o prejuízo. Confirme qualquer profissional ou instituição por caminho independente.

A ordem pode variar se houver risco imediato diferente. O princípio permanece: primeiro contenha o que ainda pode piorar; depois preserve, comunique e acompanhe. Se você já tomou uma dessas providências, passe à próxima. O objetivo não é executar tudo perfeitamente. É reduzir o dano enquanto ainda existe algo que pode ser protegido.

CAPÍTULO 12

DEPOIS DO GOLPE: DIREITOS, RESPONSABILIDADES E CAMINHOS

12.1 Ser vítima de um golpe não encerra a história

Depois das providências urgentes, começa uma segunda etapa. O dinheiro talvez não tenha voltado, uma conta pode continuar bloqueada, um empréstimo desconhecido pode aparecer, dados pessoais podem ter sido usados, uma compra pode gerar cobrança ou uma instituição pode negar responsabilidade. O golpe termina para o fraudador quando ele obtém vantagem; para a vítima, as consequências podem continuar por muito mais tempo.

Por isso, reação e reparação são coisas diferentes. O Capítulo 11 tratou de conter o dano: interromper pagamentos, proteger acessos, preservar provas e comunicar o fato. Agora a pergunta muda. O que ainda precisa ser corrigido, cancelado, recuperado ou discutido? E quem, além do próprio fraudador, pode ter alguma responsabilidade jurídica pelo prejuízo?

Nem toda consequência é apenas financeira. Um documento pode ter sido usado para abrir relacionamento em nome da vítima. Uma conta pode ter sido movimentada sem autorização. Uma empresa pode continuar cobrando obrigação que nasceu da fraude. Um perfil falso pode permanecer ativo. Um cadastro pode conter informação incorreta. Em cada situação, o primeiro passo é identificar qual

relação ficou afetada e qual providência concreta se pretende: cancelar, corrigir, restituir, indenizar, bloquear, retirar conteúdo, reconhecer inexistência de obrigação ou simplesmente obter uma resposta formal.

Ter sido vítima é um fato relevante, mas não responde sozinho a todas as questões jurídicas. É preciso reconstruir a sequência: como a fraude ocorreu, quais serviços participaram, que operações foram realizadas, quais mecanismos de segurança existiam, quando as instituições foram avisadas e que providências tomaram. Documentos e protocolos preservados no capítulo anterior passam a ter aqui outra função: permitir que cada responsabilidade seja examinada com base em fatos, e não apenas na sensação de injustiça.

Essa perspectiva evita duas frustrações. A primeira é acreditar que toda perda será automaticamente ressarcida. A segunda é concluir, cedo demais, que nada pode ser feito porque a vítima praticou alguma ação durante o golpe. Entre esses extremos existe a análise concreta, que pode envolver regras de consumo, responsabilidade civil, contratos, proteção de dados, serviços financeiros e outras áreas conforme o caso.

12.2 Quem pode responder pelo prejuízo

O autor direto da fraude é o primeiro responsável pelo próprio ato. Na prática, porém, ele pode ser desconhecido, usar identidade falsa, atuar por contas de terceiros ou estar fora do alcance imediato da vítima. Por isso, muitos conflitos posteriores discutem também a atuação de bancos, instituições de pagamento, empresas, marketplaces, plataformas, fornecedores ou profissionais que participaram da relação de alguma forma.

Participar do caminho do golpe não significa, por si só, ter obrigação de indenizar. A pergunta jurídica costuma ser mais precisa: havia um dever de segurança, informação, controle ou cuidado aplicável àquele participante? Houve falha desse dever? Essa falha contribuiu para o dano? Existe alguma causa que afaste ou limite a

responsabilidade? As respostas dependem do tipo de serviço e dos fatos comprovados.

[illegible]

O raciocínio também ajuda a compreender o papel das plataformas. Uma plataforma pode apenas ter sido usada como cenário por um terceiro, ou pode ter exercido funções que criam deveres específicos dentro daquela relação. Uma empresa pode ter sido apenas personificada, sem qualquer participação no golpe, ou pode ter falhado em procedimento que estava sob seu controle. A presença do nome, logotipo ou infraestrutura de alguém na história não basta para resolver a responsabilidade.

Por isso, casos visualmente parecidos podem terminar de forma diferente. Duas pessoas podem receber a mesma falsa mensagem, mas uma fraude depender apenas da persuasão do criminoso e outra ser acompanhada de falha concreta de segurança de um serviço. O resultado jurídico acompanha as circunstâncias demonstradas, não o nome popular do golpe.

12.3 Relações bancárias, financeiras e de consumo

Nas relações bancárias, existe um ponto de partida importante: o Superior Tribunal de Justiça consolidou que o Código de Defesa do Consumidor se aplica às instituições financeiras.[48] Também consolidou, na Súmula 479, que instituições financeiras respondem objetivamente por danos decorrentes de fraudes e delitos de terceiros quando o evento configura fortuito interno, isto é, risco ligado à própria atividade bancária.[49]

Essas regras são relevantes, mas não autorizam concluir que qualquer golpe gera ressarcimento pelo banco. Em julho de 2026, por exemplo, a Terceira Turma do STJ manteve decisão que afastou a responsabilidade de instituição financeira em um caso de falsa central porque, segundo as premissas fixadas no processo, não foram demonstradas transações incompatíveis com o perfil da cliente, insuficiência dos mecanismos de segurança ou outra falha que ligasse a fraude ao risco da atividade bancária.[50] Em outros julgados, quando a prova aponta falha na segurança e operações atípicas não contidas, a responsabilidade pode ser reconhecida.

O ponto prático é abandonar duas frases fáceis: “o banco sempre paga” e “se a vítima confirmou a operação, o banco nunca responde”. Nenhuma delas descreve adequadamente o direito. É necessário observar como a fraude se relacionou com o serviço, quais operações foram realizadas, se eram compatíveis com o perfil, que autenticações foram exigidas, que alertas existiram, como a instituição reagiu e quais fatos podem ser provados.

A mesma cautela vale para instituições de pagamento e participantes de arranjos de pagamento. Em 2026, o STJ reafirmou que o dever de processar transações com segurança alcança instituições de pagamento e que a discussão sobre responsabilidade também passa pela existência de defeito do serviço e pelas causas legais de exclusão.[51] O nome técnico da instituição importa menos ao consumidor do que compreender que o regime aplicável precisa ser identificado antes de afirmar quem deve ressarcir.

Fora do setor financeiro, relações de consumo podem envolver lojas, serviços digitais, marketplaces, empresas de telefonia, transportadoras e outros fornecedores. O princípio continua semelhante: descobrir qual serviço foi contratado ou utilizado, qual dever incidia sobre o fornecedor e se houve falha relacionada ao dano. Quando o problema nasce exclusivamente da personificação de uma empresa por um terceiro, a simples utilização indevida da marca não transforma automaticamente a empresa imitada em responsável.

Por outro lado, se o golpe deixou contrato, conta, dívida ou cobrança em nome da vítima, pode ser necessário contestar

formalmente a origem daquela obrigação e pedir correção dos registros. Nessas situações, não basta dizer “foi golpe”; é útil apresentar a cronologia, o boletim de ocorrência quando existente, os protocolos, comprovantes e demais elementos que permitam distinguir a contratação legítima da operação fraudulenta.

12.4 Caminhos extrajudiciais e judiciais

Nem todo conflito precisa começar no Judiciário. Em muitos casos, o caminho mais rápido é formular uma reclamação clara diretamente à instituição ou empresa: descrever o fato, indicar a operação contestada, dizer o que se pretende e anexar os documentos essenciais. Protocolos de atendimento são importantes porque registram quando o problema foi comunicado e qual resposta foi dada.

No setor financeiro, o Banco Central orienta primeiro procurar a agência ou o Serviço de Atendimento ao Consumidor e, depois, a ouvidoria da instituição. Se o problema continuar, o próprio BC indica Procon e Consumidor.gov.br como caminhos possíveis e também permite registrar reclamação contra instituições supervisionadas.[52] A reclamação ao regulador não deve ser confundida com garantia de ressarcimento: ela integra um sistema de supervisão e resposta, enquanto a solução individual pode depender de outros canais.

O Consumidor.gov.br é um serviço público de interlocução direta entre consumidores e empresas participantes. Em 2026, o Ministério da Justiça reafirmou que o serviço é gratuito e digital. A empresa cadastrada recebe a reclamação e tem prazo para responder dentro da plataforma.[53] O serviço não substitui Procons, Defensorias, Juizados ou outros órgãos; se a empresa não participa ou se a solução não for alcançada, esses caminhos permanecem disponíveis.

O Procon pode orientar, registrar reclamação e atuar dentro de suas competências de defesa do consumidor. Defensorias Públicas podem prestar assistência jurídica a quem preencher os requisitos aplicáveis. Dependendo do caso, a via judicial pode ser necessária para discutir inexistência de dívida, restituição, indenização, obrigação de fazer, retirada de restrição, recuperação de conta ou medida urgente. A

escolha depende do problema concreto, do valor envolvido, da prova disponível e da urgência.

Entrar em juízo também não transforma a controvérsia em resultado certo. A outra parte poderá apresentar sua versão, documentos e fundamentos; o juiz examinará fatos, provas e normas. Por isso, uma demanda bem organizada começa antes da petição: cronologia coerente, documentos legíveis, protocolos, identificação das operações e definição clara do que ainda precisa ser resolvido.

Evite tratar a quantidade de reclamações como substituto de qualidade. Abrir vários protocolos iguais em canais diferentes pode gerar confusão se a narrativa muda ou se os documentos ficam dispersos. É mais útil manter um arquivo simples com datas, números de protocolo, respostas e anexos. Assim, cada novo canal recebe a mesma história factual e é possível demonstrar o que já foi tentado.

12.5 Quando procurar orientação jurídica

Orientação jurídica individualizada torna-se especialmente útil quando a situação já ultrapassou a resposta administrativa simples. Isso ocorre, por exemplo, quando há valor relevante, dívida ou contrato que a vítima não reconhece, negativação, bloqueio de recursos, múltiplas instituições envolvidas, recusa formal de ressarcimento, necessidade de medida urgente, conflito sobre autenticidade de contratação ou dúvida sobre quem deve responder.

Também é prudente buscar avaliação profissional quando existem prazos potencialmente importantes, risco de perda de prova, consequências empresariais, exposição de dados sensíveis, uso indevido de identidade ou repercussões que se prolongam apesar das primeiras providências. Nessas situações, a pergunta deixa de ser apenas “qual canal devo procurar?” e passa a envolver estratégia, prova e escolha de medida adequada.

Levar uma pasta organizada ajuda muito mais do que levar apenas a conclusão “fui vítima de golpe”. Reúna uma cronologia de uma página, extratos e comprovantes, conversas essenciais, documentos recebidos, boletim de ocorrência, protocolos e respostas. Se houver

operação que você não reconhece, identifique-a por data, valor e destinatário. Se o problema for uma conta ou dívida criada em seu nome, indique quando descobriu e quais tentativas de correção já foram feitas.

Desconfie de quem promete vitória, devolução integral ou indenização garantida antes de analisar documentos. O mesmo cuidado usado contra o segundo golpe do capítulo anterior vale aqui: confirme a identidade e a habilitação do profissional por fonte independente, compreenda o serviço contratado e leia as condições antes de pagar. Orientação jurídica séria trabalha com possibilidades, riscos e evidências; não com certezas fabricadas.

Este livro oferece informação geral, não substitui análise de um caso concreto. Seu objetivo é permitir que o leitor chegue à etapa jurídica em posição melhor: dano contido, fatos organizados, documentos preservados, pedidos registrados e expectativas realistas. Depois de um golpe, direitos existem, caminhos existem e responsabilidades podem existir. Descobrir quais se aplicam exige método — o mesmo princípio que orientou todo o livro até aqui.

CAPÍTULO 13

PROTEÇÃO TAMBÉM SE COMPARTILHA

13.1 Pessoas diferentes, riscos diferentes

Depois de percorrer este livro, pode surgir uma tentação compreensível: ensinar tudo a todos. Repassar listas, alertas, vídeos, notícias e exemplos para familiares, colegas e amigos. Informação ajuda, mas proteção compartilhada começa de outro modo. Começa reconhecendo que pessoas diferentes vivem rotinas diferentes e, por isso, encontram situações de risco diferentes.

Quem compra e vende pela internet pode receber abordagens de falsos compradores, falsas lojas ou comprovantes fabricados. Quem administra pagamentos de uma empresa pode enfrentar pedidos de alteração de conta, cobranças e mensagens atribuídas a fornecedores ou superiores. Quem usa pouco serviços digitais talvez encontre dificuldade justamente quando precisa resolver alguma coisa fora da rotina. Quem está procurando trabalho pode estar mais exposto a falsas vagas. Quem inicia um relacionamento a distância pode enfrentar riscos que não aparecem na rotina de quem nunca usa aplicativos de relacionamento. Nenhuma dessas situações cria, por si só, um “tipo de vítima”. Elas apenas mudam a forma de exposição.

Essa distinção retoma a ideia de vulnerabilidade circunstancial apresentada no Capítulo 2. A pergunta útil não é “quem é vulnerável?”, como se houvesse um grupo permanentemente incapaz. É “em que situações esta pessoa precisa tomar decisões importantes, com quais

informações e sob quais pressões?". O mesmo indivíduo pode ser extremamente cuidadoso no trabalho e agir com menos referências diante de uma emergência familiar. Pode conhecer tecnologia e desconhecer procedimentos bancários. Pode dominar finanças e não reconhecer uma falsa identidade profissional.

Idade, profissão ou familiaridade digital também não devem ser transformadas em explicações automáticas. Uma pessoa idosa pode ter longa experiência com bancos e compras, enquanto um jovem muito conectado pode responder rapidamente a uma falsa oportunidade porque ela aparece no mesmo ambiente em que ele normalmente estuda, trabalha ou se diverte. Um empresário experiente pode conhecer profundamente seu negócio e ainda assim depender de um funcionário para confirmar uma alteração de dados bancários. A prevenção melhora quando parte da rotina real, não de estereótipos.

Compartilhar proteção, portanto, não significa escolher alguém para vigiar os outros. Significa identificar decisões que merecem uma segunda fonte. Em uma família, talvez sejam pedidos urgentes de dinheiro. Em outra, compras de alto valor. Em uma empresa, mudança de conta de fornecedor. Para uma pessoa que usa muitos serviços digitais, pode ser recuperação de senha ou autenticação. O procedimento precisa acompanhar a vida da pessoa, e não obrigá-la a viver sob suspeita permanente.

Há também uma diferença importante entre apoio e substituição de autonomia. Ajudar alguém a confirmar uma situação não significa decidir tudo por ela. Um familiar pode oferecer segunda opinião, localizar o canal oficial ou ajudar a organizar informações sem assumir controle da conta, do celular ou do dinheiro. Quanto mais a proteção puder ser incorporada como escolha da própria pessoa, maior a chance de ser usada quando realmente fizer diferença.

13.2 Como conversar sobre golpes sem humilhar

Uma boa rede de proteção depende de uma condição simples: as pessoas precisam poder contar o que aconteceu. Isso parece óbvio, mas muitas fraudes prosperam durante algum tempo porque a vítima teme parecer distraída, ingênua ou imprudente. Quando o ambiente familiar ou profissional reage com ironia e julgamento, o primeiro efeito pode ser o silêncio.

A revisão sistemática sobre consequências psicológicas e psicossociais da vitimização por fraude discutida no Capítulo 8 mostra que vergonha, autorrecriminação e sofrimento podem acompanhar esse tipo de experiência.[34] Não é necessário transformar a conversa familiar em atendimento psicológico para tirar uma conclusão prática: humilhar alguém depois de uma suspeita de golpe pode atrasar exatamente as informações necessárias para interromper o dano.

Compare duas reações. Na primeira, alguém diz: “como você acreditou nisso?”. Na segunda: “me conte desde o começo; o que você fez e o que ainda está acontecendo?”. A primeira frase procura explicar a pessoa. A segunda procura entender o problema. Para prevenção e reação, a segunda costuma ser muito mais útil.

O mesmo vale antes de qualquer golpe. Alertas podem ser compartilhados sem transformar toda mensagem em sermão. Em vez de encaminhar diariamente uma sucessão de notícias assustadoras, uma família pode conversar sobre poucos princípios duráveis: pedido urgente de dinheiro merece confirmação; mudança inesperada de número não confirma identidade; banco não deve ser validado pelo telefone fornecido na própria ligação; oportunidade vantajosa continua precisando ser verificada; dúvida pode ser compartilhada antes da decisão.

É importante também permitir que alguém pergunte sem precisar se justificar. Uma frase como “recebi isso e quero uma segunda opinião” deveria ser suficiente. Se cada dúvida vier acompanhada de bronca, a pessoa aprende a resolver sozinha justamente as situações em que uma segunda fonte seria mais valiosa.

Conversar bem não significa concordar com tudo. Se houver risco, é possível ser firme: “não faça outro pagamento agora”, “vamos confirmar fora dessa conversa”, “não envie o código”, “vamos ligar para o banco pelo aplicativo”. A diferença está em dirigir a firmeza para a ação de risco, não para a dignidade de quem está pedindo ajuda.

Também ajuda separar prevenção de retrospectiva. Depois que algo deu errado, é fácil enxergar sinais que antes estavam misturados a elementos plausíveis. O objetivo da conversa não deveria ser demonstrar que “era óbvio”, mas descobrir qual regra simples poderia funcionar numa próxima situação. Assim, o episódio deixa de ser apenas motivo de constrangimento e se transforma em aprendizado compartilhado.

13.3 Protocolos familiares simples

Famílias não precisam criar sistemas complexos. Um protocolo que ninguém lembra sob pressão não é proteção; é decoração. As melhores combinações são poucas, claras e adequadas às situações que realmente acontecem naquele grupo.

A primeira combinação pode ser esta: pedido inesperado de dinheiro deve ser confirmado por outro canal. Se o pedido chega por mensagem, ligue para um número conhecido. Se a ligação parece estranha, procure outra pessoa da família. Se alguém disser que não pode desligar, que tudo deve permanecer em segredo ou que a ajuda precisa ser enviada antes de qualquer confirmação, isso aumenta — e não diminui — a necessidade de interromper a sequência.

Uma segunda regra útil envolve mudança de contato. Número novo, perfil novo ou conta nova não deve ganhar automaticamente a confiança construída com a pessoa antiga. A confirmação pode ser simples: falar pelo contato anterior, fazer uma chamada iniciada por você, confirmar com alguém próximo ou combinar previamente como mudanças serão comunicadas. O objetivo não é criar uma “senha secreta” infalível. É impedir que a própria mensagem suspeita seja a única prova da identidade.

Uma terceira combinação pode tratar de decisões de maior valor. Acima de determinado patamar escolhido pela própria família, a pessoa espera alguns minutos, confere beneficiário e finalidade e, se a situação estiver fora da rotina, conversa com alguém. O valor não precisa ser igual para todos. Para uma pessoa, cem reais podem ser relevantes; para outra, a preocupação maior pode estar em documentos, acesso a contas ou contratação de crédito.

Também pode existir um contato de confiança para situações incomuns. Esse contato não precisa conhecer senhas nem controlar contas. Precisa apenas estar disponível para ajudar a localizar um canal oficial, comparar informações e reconstruir a história fora da pressão original. O Capítulo 10 já mostrou por que uma segunda fonte pode melhorar a decisão; aqui a diferença é combinar essa ajuda antes da emergência.

Famílias com crianças e adolescentes podem adaptar o princípio à autonomia de cada idade. Em vez de tentar ensinar todos os tipos de fraude, é possível estabelecer regras adequadas: não enviar documentos ou códigos sem conversar com responsável; não fazer pagamento inesperado; mostrar quando um desconhecido pede segredo, dinheiro ou material íntimo; procurar ajuda rapidamente se algo der errado. A regra precisa ser compreensível e compatível com a realidade daquela pessoa.

O protocolo não deve exigir que alguém prove permanentemente que merece confiança. Ele serve para situações excepcionais, não para transformar relações familiares em fiscalização. A proteção cresce quando todos sabem que certas decisões terão uma etapa adicional de confirmação — e que essa etapa vale inclusive para quem normalmente “entende mais” de tecnologia, dinheiro ou negócios.

13.4 Quando alguém próximo caiu em um golpe

Quando alguém próximo percebe que caiu em um golpe, quem está ao lado pode fazer grande diferença. Não por substituir banco, polícia, plataforma ou profissional especializado, mas por ajudar a pessoa a sair da sequência de pressão e organizar as próximas ações.

A primeira tarefa é descobrir se o golpe ainda está acontecendo. Há novo pagamento sendo pedido? O fraudador continua em ligação? Existe acesso remoto ativo? Alguma conta ainda está sob controle de terceiro? Há promessa de recuperação mediante taxa? Se houver risco em curso, a ajuda deve se concentrar em interromper novas ações e localizar os canais oficiais correspondentes. Os detalhes do protocolo emergencial estão no Capítulo 11; aqui importa a posição de quem acompanha.

Essa pessoa pode ajudar a transformar uma história confusa em cronologia: quando começou, quem entrou em contato, o que foi pedido, o que foi enviado, quais contas ou dispositivos foram usados e quais providências já foram tomadas. Pode ajudar a reunir comprovantes, localizar números oficiais e anotar protocolos. Muitas vezes, ter alguém escrevendo enquanto a vítima fala já reduz a desorganização produzida pela urgência.

O que costuma ajudar menos é iniciar uma investigação familiar para descobrir “como foi possível”. Esse debate pode ter lugar mais tarde, se for útil. Durante a contenção, ele desvia atenção do que ainda pode ser protegido. Também pode incentivar omissões: se a pessoa teme nova repreensão a cada informação, talvez demore a contar que fez um segundo pagamento, enviou documento ou instalou um aplicativo.

Também é importante observar o risco de segundo golpe. A vítima pode receber contato de supostos recuperadores, advogados, policiais, funcionários de banco ou empresas que afirmam já conhecer o caso. Quem está ajudando pode exercer exatamente a função da segunda fonte: “vamos confirmar quem é antes de responder”. A necessidade de recuperar o prejuízo não transforma o novo interlocutor em pessoa confiável.

Apoiar não significa assumir todas as decisões. Depois de interrompido o risco imediato, procure devolver à pessoa o controle possível sobre o processo: explicar opções, organizar documentos, acompanhar uma ligação se ela desejar, mas evitar tomar posse de contas, senhas ou decisões sem necessidade. Uma rede de proteção forte aumenta a capacidade da pessoa; não troca uma dependência por outra.

Se houver sofrimento intenso, ameaça, exposição íntima, medo persistente ou dificuldade de retomar atividades, a necessidade pode ultrapassar providências financeiras e digitais. Nesse caso, apoio familiar pode incluir procurar serviço profissional adequado. O livro não transforma esse sofrimento em diagnóstico; apenas reconhece que golpes podem produzir consequências que não cabem numa planilha de prejuízo.

13.5 Empresas também precisam de protocolos

O mesmo princípio vale no ambiente de trabalho. Uma empresa não deve depender de que cada funcionário identifique sozinho todo golpe novo. Quanto mais relevante a operação, mais útil é existir um procedimento que continue funcionando mesmo quando a mensagem parece convincente.

Mudança de dados bancários de fornecedor é um bom exemplo. O e-mail pode estar perfeitamente escrito, usar assinatura conhecida e mencionar uma fatura verdadeira. Ainda assim, a alteração pode depender de confirmação por canal previamente cadastrado. A regra não acusa o fornecedor de fraude; apenas separa pedido recebido de dado confirmado.

Solicitações atribuídas a superiores merecem lógica semelhante. Hierarquia pode pressionar alguém a agir rápido: “o diretor pediu”, “o presidente está em reunião”, “é confidencial”. Um protocolo saudável permite que o funcionário confirme uma ordem extraordinária sem parecer insubordinado. Quando a própria organização autoriza a conferência, o fraudador perde parte da vantagem de explorar autoridade e urgência.

Para pagamentos fora da rotina, dupla verificação pode reduzir dependência de uma única pessoa. Isso não precisa significar burocracia para toda despesa. A empresa pode definir quais alterações, valores ou destinatários exigem confirmação adicional. O ponto é criar fricção onde o erro teria consequência relevante.

Dados cadastrais também precisam de procedimento. Alteração de e-mail de cobrança, telefone de contato, conta bancária, usuário

administrador ou endereço de entrega pode parecer uma pequena mudança administrativa, mas às vezes modifica quem receberá dinheiro, informação ou acesso. Mudanças sensíveis merecem registro e confirmação compatíveis com sua consequência.

Empresas pequenas podem aplicar os mesmos princípios sem criar um departamento de compliance. Uma planilha de fornecedores confirmados, dois responsáveis para pagamentos incomuns, retorno por telefone conhecido antes de alterar conta e regra clara para solicitações urgentes já transformam segurança em processo. O objetivo não é importar estruturas de grandes corporações, mas impedir que decisões críticas dependam apenas da impressão momentânea de quem recebeu a mensagem.

Há ainda um benefício cultural. Quando a organização deixa claro que é permitido parar e confirmar, funcionários tendem a esconder menos as próprias dúvidas. Um erro ou suspeita comunicados cedo podem ser contidos. Um ambiente em que a pessoa teme ser ridicularizada por quase ter caído num golpe pode empurrar o problema para o silêncio — exatamente como ocorre nas famílias.

Proteção compartilhada, portanto, não é distribuir medo. É distribuir procedimentos. Uma pessoa aprende a confirmar um pedido. Uma família combina como reagir a uma emergência. Uma equipe estabelece como validar uma alteração. Um colega se torna segunda fonte para outro. O conhecimento deixa de existir apenas na cabeça de quem leu este livro e passa a aparecer nas decisões concretas de um grupo.

Informação individual reduz um risco. Informação compartilhada pode impedir que o mesmo mecanismo funcione repetidamente contra pessoas diferentes. E essa é a ponte para o último capítulo: quando a próxima fraude surgir com outro nome, outra tecnologia e outra história, o que permanecerá útil não será a memória de um catálogo, mas a capacidade de reconhecer quando é hora de parar, confirmar e decidir com autonomia.

CAPÍTULO 14

O PRÓXIMO GOLPE

14.1 O golpe que ainda não tem nome

Em algum momento, depois de fechar este livro, você poderá receber uma mensagem que não se parece com nenhuma das situações descritas aqui. Talvez chegue por um serviço que hoje ainda não existe. Talvez use um meio de pagamento novo, uma forma diferente de confirmar identidade ou uma tecnologia que, neste momento, parece distante. O nome do golpe poderá ser desconhecido. A história, convincente. A aparência, inédita.

Esse é justamente o teste final da proposta deste livro. Se a proteção dependesse de reconhecer apenas golpes já batizados, ela começaria a envelhecer no dia seguinte à publicação. A realidade muda rápido demais para que uma lista permaneça completa. Novas plataformas surgem, hábitos de comunicação se transformam, empresas alteram seus procedimentos e tecnologias que hoje exigem conhecimento especializado passam a caber em aplicativos de uso cotidiano.

Isso não significa que seja possível prever qual será a próxima fraude. Previsões específicas costumam confundir possibilidade com certeza. O que se pode afirmar com prudência é outra coisa: sempre que surgem novos ambientes de confiança, novas formas de movimentar valor, novas maneiras de provar identidade ou novos canais de comunicação, também surgem oportunidades para uso enganoso desses recursos. A superfície muda. O problema do engano continua.

O ponto mais importante é que uma fraude nova não precisa ser reconhecida pelo nome para poder ser questionada. Mesmo diante de uma situação inédita, ainda é possível perguntar: quem está falando comigo? O que querem que eu faça? Por que preciso fazer isso agora? Para quem vai o dinheiro, o dado, o acesso ou a autorização? O que consigo confirmar fora desta própria conversa? Essas perguntas não dependem da modalidade estar em uma cartilha.

Imagine uma ferramenta futura capaz de combinar voz, imagem, documentos, contexto pessoal e comunicação em tempo real com muito mais naturalidade do que hoje. A aparência poderá se tornar ainda mais convincente. Mas a decisão continuará tendo consequências concretas. Alguém pedirá uma transferência, um código, uma autorização, um documento, uma instalação, uma assinatura, um acesso ou alguma outra ação. Quanto mais sofisticada for a aparência, mais valiosa se tornará a capacidade de separar apresentação de confirmação.

O golpe que ainda não tem nome, portanto, não deve ser tratado como um monstro invisível contra o qual nada funciona. Ele será desconhecido em alguns detalhes, não em todos. Continuará existindo algum caminho entre a aproximação e a vantagem pretendida. Nesse caminho haverá decisões. E decisões criam pontos em que a verificação pode entrar.

14.2 Por que listas envelhecem

Listas de golpes são úteis. Elas ajudam a reconhecer modalidades frequentes, dão nome a problemas e permitem que alertas circulem rapidamente. O risco começa quando a lista parece um mapa completo. Nesse momento, tudo o que não está nela tende a parecer menos perigoso — justamente onde a fraude pode mudar de roupa.

Ao longo deste livro, apareceram falsos bancos, falsos familiares, falsos profissionais, falsas lojas, falsas oportunidades, falsas cobranças, falsos relacionamentos e outras situações. Vistos de longe, parecem golpes diferentes. Vistos pelo mecanismo, muitos compartilham estruturas: alguém precisa ganhar credibilidade, provocar uma

interpretação da situação, reduzir espaço para conferência e induzir uma ação que produz vantagem para o fraudador.

O falso banco pode amanhã assumir a aparência de uma instituição ainda inexistente. O pedido atribuído a um familiar pode migrar para outro aplicativo. Uma falsa oportunidade pode usar uma atividade econômica nova. Um golpe baseado em imagem pode incorporar recursos que hoje ainda não estão disponíveis ao público. Nada disso exige abandonar o que foi aprendido; exige aplicá-lo sem ficar preso ao exemplo antigo.

É por isso que decorar sinais isolados costuma ser menos durável do que compreender relações. Um erro de português pode aparecer em uma fraude e desaparecer na seguinte. Um site rudimentar pode ser substituído por uma página impecável. Um número desconhecido pode ser usado hoje; amanhã, uma conta legítima pode estar comprometida. Um vídeo convincente pode ser verdadeiro e ainda assim estar sendo apresentado fora de contexto. Quando um sinal muda, o mecanismo pode permanecer.

A pergunta mais forte não é 'qual é o nome deste golpe?'. É 'o que precisa ser verdadeiro para que eu faça o que estão me pedindo?'. Essa mudança de foco transforma o leitor de colecionador de alertas em alguém capaz de testar uma situação.

Conhecer modalidades continua sendo útil. O problema é confundir memória com método. A memória reconhece aquilo que já viu. O método permite lidar com aquilo que ainda não viu.

14.3 O que provavelmente continuará sendo explorado

Não sabemos quais plataformas dominarão a comunicação daqui a alguns anos nem quais instrumentos financeiros serão mais comuns. Também não sabemos que tecnologias serão incorporadas à rotina de empresas, governos e famílias. Mas sabemos que relações humanas continuarão dependendo de confiança, autoridade, expectativa, medo, afeto, cooperação, oportunidade e necessidade de decidir.

Esses elementos não são defeitos a serem eliminados. Confiar permite contratar, comprar, delegar e conviver. A autoridade organiza instituições. A urgência existe em emergências verdadeiras. O afeto sustenta relações. A solidariedade permite ajudar. A expectativa de ganho move escolhas econômicas. O medo pode proteger diante de um perigo real. O problema surge quando alguém fabrica ou distorce o contexto para colocar esses elementos a serviço de uma decisão que beneficia o enganador.

Por isso, o futuro provavelmente não exigirá seres humanos completamente diferentes para produzir novos golpes. Bastará combinar recursos novos com situações humanas conhecidas. Uma tecnologia pode tornar uma voz mais realista; ainda assim, a voz estará tentando convencer alguém de alguma coisa. Um sistema pode automatizar mensagens em grande escala; ainda assim, algumas delas buscarão criar credibilidade. Um novo meio de pagamento pode reduzir etapas; ainda assim, haverá um destinatário, uma autorização e uma consequência.

A tecnologia pode aumentar velocidade, alcance, personalização e realismo. Pode reduzir o custo de abordar muitas pessoas. Pode tornar mais difícil perceber, apenas pela aparência, se algo foi produzido ou alterado. Mas ela não transforma toda comunicação em mentira, nem elimina a possibilidade de conferir. Ao contrário: quanto menos confiáveis se tornam certos sinais visuais ou sonoros isolados, maior a importância de usar canais independentes, contexto, procedimentos e confirmação proporcional ao risco.

Também continuarão existindo situações em que o fraudador tenta encurtar o tempo entre acreditar e agir. Às vezes pela ameaça de uma perda; às vezes pela promessa de uma oportunidade; às vezes pela preocupação com alguém; às vezes pela vergonha de revelar o que aconteceu. A forma muda, mas a pressão possui uma característica recorrente: ela tenta transformar decisão em reação.

Foi por isso que criar tempo apareceu repetidamente neste livro. Tempo, sozinho, não prova nada. Mas alguns minutos podem permitir sair da narrativa apresentada, consultar outra fonte, perceber uma inconsistência, telefonar para alguém, abrir o aplicativo correto ou

simplesmente perguntar se aquela ação faz sentido. Em muitas fraudes, a pausa não derrota uma tecnologia. Ela interrompe o ritmo que favorecia o engano.

Há ainda outro elemento que provavelmente continuará valioso para quem engana: a aparência de legitimidade. Documentos, marcas, linguagem técnica, dados verdadeiros, perfis, avaliações, comprovantes, vídeos, protocolos e referências reais podem ser combinados a uma história falsa. O leitor não precisa aprender a desprezar esses elementos. Precisa lembrar que eles respondem apenas às perguntas que realmente conseguem provar.

Uma informação verdadeira pode provar que determinado processo existe e não provar quem enviou a mensagem. Uma voz parecida pode sugerir identidade e não confirmá-la. Um comprovante pode demonstrar que uma operação foi realizada e não que o dinheiro entrou. Uma empresa real pode existir e o contato ser falso. Uma oportunidade pode ser possível e a proposta concreta ainda precisar de verificação. Essa disciplina de separar uma afirmação da evidência que a sustenta continuará útil mesmo quando os objetos mudarem.

14.4 O que realmente precisa permanecer depois deste livro

O livro começou olhando para trás. Moedas, mercadorias, documentos, correspondências e outras formas antigas de engano lembraram que a fraude não nasceu com a internet. Depois, aproximamos o problema do presente: vimos por que ninguém possui imunidade absoluta, como a credibilidade pode ser construída, como o golpe pode ganhar escala e como os mesmos mecanismos aparecem em dinheiro, identidade, oportunidades, sentimentos e tecnologia.

Em seguida, a compreensão virou procedimento. Você não precisava identificar cada modalidade. Precisava aprender a interromper a sequência e perguntar o que estava acontecendo. O método foi resumido em quatro movimentos: PARE IDENTIFIQUE CONFIRA DECIDA.

Pare não significa viver desconfiado. Significa perceber quando a pressão está tomando o lugar da decisão. Identifique não significa investigar o mundo inteiro. Significa descobrir qual ação concreta está sendo solicitada e quais afirmações precisam ser verdadeiras para justificá-la. Confira não significa exigir certeza absoluta. Significa buscar confirmação adequada ao risco e, sempre que necessário, independente do próprio contato. Decida significa recuperar o controle da ação.

Depois, o livro mudou novamente de posição. Partiu do pressuposto de que a fraude já havia acontecido. Nesse momento, o objetivo deixou de ser evitar e passou a ser conter: interromper novos danos, proteger dinheiro, acessos, dispositivos e identidade, preservar provas, comunicar o fato e desconfiar de promessas de recuperação garantida. Em seguida, vieram os direitos e os caminhos possíveis — com uma diferença importante entre existir uma possibilidade jurídica e existir um resultado certo.

Por fim, a proteção deixou de ser apenas individual. Família, colegas e empresas podem criar ambientes em que perguntar não seja motivo de vergonha e em que decisões relevantes suportem uma segunda fonte. Isso reduz a dependência da atenção perfeita de uma única pessoa. Ninguém precisa acertar sozinho o tempo todo.

Se alguma coisa deve permanecer depois destas páginas, não é uma sensação de que o mundo se tornou impossível de confiar. Essa conclusão seria tão inútil quanto perigosa. A vida cotidiana exige confiança. Você continuará recebendo mensagens verdadeiras, fazendo pagamentos legítimos, conhecendo pessoas, aceitando oportunidades, ajudando quem precisa e utilizando tecnologias que tornam a vida melhor.

O que deve mudar é outra coisa: a confiança deixa de ser tratada como autorização automática quando a consequência é relevante. Em certas situações, confiar pode ser o começo da decisão, mas não precisa ser o fim da verificação.

Quando algo pedir dinheiro, acesso, segredo, código, documento, assinatura ou uma decisão difícil de desfazer, você pode criar uma

pequena distância entre a história recebida e a ação. Essa distância pode durar um minuto ou uma noite. Pode ser uma ligação para um número conhecido, uma consulta ao aplicativo oficial, uma conversa com alguém de confiança ou uma pergunta simples: o que eu consigo confirmar independentemente?

Isso não elimina o risco. Nenhum livro elimina. Fraudadores aprendem, tecnologias evoluem, procedimentos falham e pessoas tomam decisões sob condições imperfeitas. O objetivo sempre foi mais realista: aumentar sua capacidade de perceber risco, recuperar tempo, buscar confirmação e agir melhor.

Também é importante guardar uma atitude para depois do erro. Se você cair em um golpe, o conhecimento deste livro não se torna inútil. Ele muda de função. Serve para interromper a perda, organizar a reação, buscar os canais adequados e evitar que vergonha ou desespero ampliem o dano. Se outra pessoa cair, serve para ajudá-la sem transformar o acontecimento em julgamento de caráter.

O próximo golpe pode aparecer amanhã ou daqui a anos. Pode usar uma tecnologia sofisticada ou apenas uma conversa bem construída. Pode chegar em uma tela, em uma ligação, em um documento, em uma relação de confiança ou em um ambiente que ainda não existe. Talvez você nunca tenha ouvido falar dele.

Mas ele ainda terá de convencer alguém de alguma coisa. Ainda terá de produzir uma realidade suficientemente plausível para provocar uma ação. Ainda haverá um momento em que aparência e confirmação podem ser separadas. É ali que todo o percurso deste livro encontra sua utilidade.

Começamos com golpes antigos para mostrar que o engano muda de forma. Terminamos diante de golpes que ainda não foram inventados para mostrar que você não precisa conhecer todas as formas futuras para conservar aquilo que é mais importante.

Compreender como o engano funciona. Reconhecer quando uma situação merece atenção. Conferir antes de entregar à aparência o peso de uma prova. Evitar o que puder ser evitado. Reagir com rapidez e método quando algo acontecer.

COMPREENDER RECONHECER CONFERIR EVITAR REAGIR

Os golpes continuarão mudando. Essa sequência é o que deve permanecer.

Messias Costa

Março a outubro de 2026

REFERÊNCIAS

REFERÊNCIAS BIBLIOGRÁFICAS

1. BRITISH MUSEUM. Coin; forgery (ancient). Londres: British Museum, [s. d.]. Catálogo da coleção, objeto R.4755. Disponível em: https://www.britishmuseum.org/collection/object/C_R-4755. Acesso em: 11 set. 2026.

2. BRITISH MUSEUM. Tablet. Londres: British Museum, [s. d.]. Catálogo da coleção, objeto 1953,0411.71. Carta de Nanni a Ea-nasir. Disponível em: https://www.britishmuseum.org/collection/object/W_1953-0411-71. Acesso em: 11 set. 2026.

3. PLÍNIO, O VELHO. The Natural History. Livro XXXVII: The natural history of precious stones. Tradução de John Bostock e H. T. Riley. Londres: Taylor and Francis, 1855. Edição digital: Perseus Digital Library, Tufts University. Disponível em: https://www.perseus.tufts.edu/hopper/text?doc=Perseus%3Atext%3A1999.02.0137%3Abook%3D37. Acesso em: 11 set. 2026.

4. UNITED STATES. Federal Bureau of Investigation. Enduring lure of Ponzi schemes. [S. l.]: FBI, 12 mar. 2007. Disponível em: https://archives.fbi.gov/archives/news/stories/2007/march/ponzi_031207. Acesso em: 11 set. 2026.

5. UNITED STATES. Federal Bureau of Investigation. Criminals use generative artificial intelligence to facilitate financial fraud. [S. l.]: Internet Crime Complaint Center, 3 dez. 2024. Alerta I-120324-PSA. Disponível em: https://www.ic3.gov/PSA/2024/PSA241203. Acesso em: 11 set. 2026.

6. NORRIS, Gareth; BROOKES, Alexandra; DOWELL, David. The psychology of internet fraud victimisation: a systematic review. Journal of Police and Criminal Psychology, v. 34, p. 231–245, 2019. DOI: https://doi.org/10.1007/s11896-019-09334-5. Disponível em: https://link.springer.com/article/10.1007/s11896-019-09334-5. Acesso em: 11 set. 2026.

7. UNITED STATES. Federal Trade Commission. FTC issues annual report to Congress on agency's actions to protect older adults. [S. l.]: FTC, dez. 2025. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults. Acesso em: 11 set. 2026.
UNITED STATES. Federal Trade Commission. FTC testifies before the Joint Economic Committee on agency's efforts to combat fraud. Washington, DC: FTC, mar. 2026. Disponível em: https://search.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud. Acesso em: 13 out. 2026.

8. DELIEMA, Marti et al. Exposed to scams: what separates victims from non-victims? [S. l.]: FINRA Investor Education Foundation; BBB Institute for Marketplace Trust;

Stanford Center on Longevity, set. 2019. Disponível em: https://www.finrafoundation.org/exposed-to-scams. Acesso em: 11 set. 2026.

9. AUTON, Jaime Claire; STURMAN, Daniel. Persuasion under pressure: the influence of persuasion principles and time constraints on phishing email susceptibility. Information and Computer Security, v. 33, n. 5, p. 845–859, 2025. DOI: https://doi.org/10.1108/ICS-07-2024-0163. Disponível em: https://digital.library.adelaide.edu.au/items/3c118ff1-97c0-4d77-b316-a20dd26c8ca2. Acesso em: 11 set. 2026.

10. CERT.br. Phishing e outros golpes. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, dez. 2022. Fascículo da Cartilha de Segurança para Internet. Disponível em: https://cartilha.cert.br/guardiao/fasciculo-phishing-golpes-alta-egc.pdf. Acesso em: 11 set. 2026.

11. BANCO CENTRAL DO BRASIL. Segurança no Pix. Brasília, DF: Banco Central do Brasil, [s. d.]. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/pix-seguranca. Acesso em: 11 set. 2026.

12. BRASIL. Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (ENCCLA). Ação 1/2025 — Produto 1: diagnóstico sobre o golpe da falsa central. Brasília, DF: Ministério da Justiça e Segurança Pública, 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/enccla/acoes-enccla/arquivos-enccla-2025/e2025a01-acao-1-enccla-2025-produto-1.pdf. Acesso em: 11 set. 2026.

13. INTERPOL. Global Financial Fraud Assessment. Lyon: INTERPOL, mar. 2024. Disponível em: https://www.interpol.int/content/download/21077/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03%20v2.pdf. Acesso em: 11 set. 2026.

14. INTERPOL. Global Financial Fraud Threat Assessment. Lyon: INTERPOL, mar. 2026. Disponível em: https://www.interpol.int/content/download/24291/420870?version=2. Acesso em: 11 set. 2026.

15. BANCO CENTRAL DO BRASIL. Vítima fez um Pix e caiu em um golpe. Brasília, DF: Banco Central do Brasil, atualizado em 7 ago. 2026. FAQ — Golpes. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/vitima-fez-um-pix-e-caiu-em-um-golpe. Acesso em: 11 set. 2026.

16. BANCO CENTRAL DO BRASIL. Medidas para evitar golpes envolvendo empréstimo. Brasília, DF: Banco Central do Brasil, atualizado em 28 mar. 2024. FAQ — Golpes. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/medidas-para-evitar-golpes-envolvendo-emprestimo. Acesso em: 11 set. 2026.

17. BRASIL. Receita Federal. Golpe via SMS. Brasília, DF: Receita Federal do Brasil, publicado em 3 maio 2024, atualizado em 11 dez. 2025. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/remessas-postal-e-expressa/e-golpe/golpe-por-carta/golpe-por-carta. Acesso em: 11 set. 2026.

18. BRASIL. Comissão de Valores Mobiliários. Ofertas / Atuações irregulares. Rio de Janeiro: CVM, publicado em 16 nov. 2020, atualizado em 8 ago. 2025. Disponível em: https://www.gov.br/cvm/pt-br/assuntos/protecao/alertas/ofertas-atuacoes-irregulares. Acesso em: 11 set. 2026.

19. BRASIL. Comissão de Valores Mobiliários. Relatório de pesquisa: fraudes financeiras. Rio de Janeiro: CVM, 2020. Disponível em: https://www.gov.br/investidor/pt-br/educacional/publicacoes-educacionais/pesquisas/relatorio-pesquisa-fraudes-financeiras-2020.pdf. Acesso em: 11 set. 2026.

20. BRASIL. Agência Nacional de Telecomunicações. Golpe do WhatsApp Falso: veja as orientações da Anatel para denunciar e se proteger. Brasília, DF: Anatel, 24 out. 2025. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/golpe-do-whatsapp-falso-veja-as-orientacoes-da-anatel-para-denunciar-e-se-proteger. Acesso em: 11 set. 2026.

21. BRASIL. Centro Integrado de Segurança Cibernética do Governo Digital. Golpistas enviam mensagens no WhatsApp se passando por entidades do governo. Brasília, DF: CISC, 13 fev. 2026, modificado em 9 abr. 2026. Disponível em: https://www.gov.br/cisc/pt-br/alertas-de-golpes-digitais/golpistas-enviam-mensagens-no-whatsapp-se-passando-por-entidades-do-governo. Acesso em: 11 set. 2026.

22. ORDEM DOS ADVOGADOS DO BRASIL. Plataforma ConfirmADV completa um ano com mais de 32 mil verificações contra falsos advogados. Brasília, DF: Conselho Federal da OAB, 29 abr. 2026. Disponível em: https://www.oab.org.br/noticia/64127/plataforma-confirmadv-completa-um-ano-com-mais-de-32-mil-verificacoes-contra-falsos-advogados. Acesso em: 11 set. 2026.

23. BANCO CENTRAL DO BRASIL. Relatório de Contas e Relacionamentos (CCS). Brasília, DF: Banco Central do Brasil, atualizado em 9 mar. 2026. Disponível em: https://www.bcb.gov.br/meubc/faqs/s/relatorio-de-contas-e-relacionamentos-em-bancos-ccs1. Acesso em: 11 set. 2026.

24. BRASIL. Ministério da Justiça e Segurança Pública. Invadiram ou clonaram minha rede social. Brasília, DF: Ministério da Justiça e Segurança Pública, [s. d.]. Programa “Sofri um golpe, e agora?”. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/sofri-um-golpe-e-agora/minha-conta-em-redes-socias-foi-invadida-ou-clonada. Acesso em: 11 set. 2026.

25. BRASIL. Receita Federal. Compras em sites falsos ou redes sociais. Brasília, DF: Receita Federal do Brasil, publicado em 9 jul. 2024, atualizado em 10 dez. 2025. Disponível em: https://www.gov.br/receitafederal/pt-br/assuntos/aduana-e-comercio-exterior/manuais/remessas-postal-e-expressa/e-golpe/compras-em-redes-sociais/compras-em-redes-sociais. Acesso em: 11 set. 2026.

26. MATO GROSSO DO SUL. Fundação do Trabalho de Mato Grosso do Sul. Funtrab alerta sobre anúncio falso de cursos e vagas de emprego nas redes sociais. Campo Grande: Funtrab, 12 jan. 2026. Disponível em: https://www.funtrab.ms.gov.br/funtrab-

alerta-sobre-anuncio-falso-de-cursos-e-vagas-de-emprego-nas-redes-sociais/. Acesso em: 11 set. 2026.

27. CONSELHO REGIONAL DE CORRETORES DE IMÓVEIS DE MATO GROSSO DO SUL. Atenção! Proteja-se de golpes na locação de imóveis. Campo Grande: CRECI-MS, 12 fev. 2025. Disponível em: https://crecims.gov.br/noticia.php?id=1630. Acesso em: 11 set. 2026.

28. BANCO CENTRAL DO BRASIL. Golpes: dicas gerais para evitar golpes. Brasília, DF: Banco Central do Brasil, atualizado em 22 jul. 2025. Disponível em: https://www.bcb.gov.br/meubc/faqs/s/golpes. Acesso em: 11 set. 2026.

29. BANCO CENTRAL DO BRASIL. Vítima do golpe do “presente”. Brasília, DF: Banco Central do Brasil, atualizado em 22 jul. 2025. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/vitima-do-golpe-do-presente. Acesso em: 11 set. 2026.

30. LAZARUS, Suleman; WHITTAKER, Jack M.; MCGUIRE, Michael R.; PLATT, Lucinda. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). Journal of Economic Criminology, v. 2, 100013, 2023. DOI: https://doi.org/10.1016/j.jeconc.2023.100013. Acesso em: 11 set. 2026.

31. DREW, Jacqueline M.; WEBSTER, Julianne. The victimology of online fraud: a focus on romance fraud victimisation. Journal of Economic Criminology, v. 3, 100053, 2024. DOI: https://doi.org/10.1016/j.jeconc.2024.100053. Acesso em: 11 set. 2026.

32. PARANÁ. Polícia Civil do Paraná. PCPR e PMPR localizam criança vítima de golpe do falso sequestro em Mamborê. Curitiba: PCPR, 25 jun. 2026. Disponível em: https://www.policiacivil.pr.gov.br/Noticia/PCPR-e-PMPR-localizam-crianca-vitima-de-golpe-do-falso-sequestro-em-Mambore. Acesso em: 11 set. 2026.

33. BRASIL. Ministério das Mulheres. O Digital é Nosso Lugar. Brasília, DF: Ministério das Mulheres, publicado em 22 jun. 2026, modificado em 3 jul. 2026. Disponível em: https://www.gov.br/mulheres/pt-br/central-de-conteudos/campanhas/2026/o-digital-e-nosso-lugar. Acesso em: 11 set. 2026.

34. BAI, Jie; HO, Mei-Hsin; SUNG, Hsiang-Te; HUNG, Chuan-Sheng; TSAI, Jui-Hsiu. Mental health and psychosocial sequelae of fraud victimization: a systematic review. Frontiers in Psychology, v. 17, 1805536, 2026. DOI: https://doi.org/10.3389/fpsyg.2026.1805536. Acesso em: 11 set. 2026.

35. BRASIL. Ministério das Comunicações. Ataque Phishing: como identificar tentativas de fraude na internet. Brasília, DF: Ministério das Comunicações, 14 jul. 2026. Disponível em: https://www.gov.br/mcom/pt-br/noticias/noticias_alt/2026/julho/ataque-phishing-como-identificar-tentativas-de-fraude-na-internet. Acesso em: 11 set. 2026.

36. CERT.br. Redes Sociais. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, fev. 2023. Fascículo da Cartilha de Segurança para Internet. Disponível em: https://cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais.pdf. Acesso em: 11 set. 2026.

37. BRASIL. Agência Nacional de Telecomunicações. Parece real, mas pode ser golpe. Brasília, DF: Anatel, 17 mar. 2026. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/parece-real-mas-pode-ser-golpe. Acesso em: 11 set. 2026.

38. BRASIL. Agência Nacional de Proteção de Dados. ANPD publica Radar Tecnológico sobre deepfakes. Brasília, DF: ANPD, 29 jul. 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-radar-tecnologico-sobre-deepfakes. Acesso em: 11 set. 2026.

39. BRASIL. Ministério das Comunicações. QR Code: um atalho entre o mundo físico e o digital. Brasília, DF: Ministério das Comunicações, 6 ago. 2026. Disponível em: https://www.gov.br/mcom/pt-br/noticias/noticias_alt/2026/agosto/qr-code-um-atalho-entre-o-mundo-fisico-e-o-digital. Acesso em: 11 set. 2026.

40. BANCO CENTRAL DO BRASIL. Dicas gerais de como proceder após sofrer um golpe. Brasília, DF: Banco Central do Brasil, atualizado em 2 jun. 2026. FAQ — Golpes. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/dicas-gerais-de-como-proceder-apos-sofrer-um-golpe. Acesso em: 11 set. 2026.

41. BRASIL. Ministério da Justiça e Segurança Pública. Invadiram minha conta e fizeram transações. Brasília, DF: Ministério da Justiça e Segurança Pública, [s. d.]. Programa “Sofri um golpe, e agora?”. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/sofri-um-golpe-e-agora/invadiram-minha-conta. Acesso em: 11 set. 2026.

42. BRASIL. Ministério da Justiça e Segurança Pública. Recebi boletos ou ofertas falsos. Brasília, DF: Ministério da Justiça e Segurança Pública, [s. d.]. Programa “Sofri um golpe, e agora?”. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/sofri-um-golpe-e-agora/paguei-boletos-ou-ofertas-que-se-mostraram-falsos/. Acesso em: 11 set. 2026.

43. BRASIL. Ministério das Comunicações. Celular Seguro: veja como cadastrar seu aparelho e emitir alertas em caso de roubo, furto ou perda. Brasília, DF: Ministério das Comunicações, 7 ago. 2026. Disponível em: https://www.gov.br/mcom/pt-br/noticias/noticias_alt/2026/agosto/celular-seguro-veja-como-cadastrar-seu-aparelho-e-emitir-alertas-em-caso-de-roubo-furto-ou-perda. Acesso em: 11 set. 2026.

44. BANCO CENTRAL DO BRASIL. BC PROTEGE+. Brasília, DF: Banco Central do Brasil, atualizado em 17 ago. 2026. FAQ — BC PROTEGE+ e Golpes. Disponível em: https://www.bcb.gov.br/meubc/faqs/s/bc-protege. Acesso em: 11 set. 2026.

45. BANCO CENTRAL DO BRASIL. Golpes envolvendo o nome do Banco Central. Brasília, DF: Banco Central do Brasil, atualizado em 2 jul. 2026. FAQ — Golpes. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/golpes-envolvendo-o-nome-do-banco-central. Acesso em: 11 set. 2026.

46. CERT.br. Computadores. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2026. Fascículo da Cartilha de Segurança para Internet. Disponível em:

https://cartilha.cert.br/guardiao/fasciculo-computadores-alta-egc.pdf. Acesso em: 11 set. 2026.

47. BRASIL. Câmara dos Deputados. Lei nº 8.078, de 11 de setembro de 1990 — Código de Defesa do Consumidor. Texto atualizado. Brasília, DF: Câmara dos Deputados. Disponível em: https://www2.camara.leg.br/legin/fed/lei/1990/lei-8078-11-setembro-1990-365086-normaatualizada-pl.html. Acesso em: 11 set. 2026.

48. SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula 297. O Código de Defesa do Consumidor é aplicável às instituições financeiras. Brasília, DF: STJ, Segunda Seção, julgado em 12 maio 2004, DJ 8 set. 2004. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=297.num. Acesso em: 11 set. 2026.

49. SUPERIOR TRIBUNAL DE JUSTIÇA. Súmula 479. As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias. Brasília, DF: STJ, Segunda Seção, julgado em 27 jun. 2012, DJe 1 ago. 2012. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=479.num. Acesso em: 11 set. 2026.

50. SUPERIOR TRIBUNAL DE JUSTIÇA. Sem transações incompatíveis com perfil de cliente, banco não responde por golpe da falsa central. Brasília, DF: STJ, 15 jul. 2026. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2026/15072026-Sem-transacoes-incompativeis-com-perfil-de-cliente--banco-nao-responde-por-golpe-da-falsa-central.aspx. Acesso em: 11 set. 2026.

51. SUPERIOR TRIBUNAL DE JUSTIÇA. Informativo de Jurisprudência n. 892. Responsabilidade de instituições de pagamento por fraudes e delitos de terceiros no âmbito das operações. Brasília, DF: STJ, 16 jun. 2026. Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/. Acesso em: 11 set. 2026.

52. BANCO CENTRAL DO BRASIL. Reclamar contra bancos e outras instituições. Brasília, DF: Banco Central do Brasil, atualizado em 10 abr. 2026. FAQ — Atendimento ao cidadão. Disponível em: https://www.bcb.gov.br/meubc/faqs/p/reclamarcontrabancoseoutrasinstituicoes. Acesso em: 11 set. 2026.

53. BRASIL. Ministério da Justiça e Segurança Pública. Consumidor.gov.br: saiba como registrar uma reclamação pela plataforma. Brasília, DF: MJSP, 10 jul. 2026. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias-1/consumidor-gov-br-saiba-como-registrar-uma-reclamacao-pela-plataforma. Acesso em: 11 set. 2026.