



Oi, mãe! Troquei de número.  
Salva esse aqui.

Me faz um Pix urgente? !

# NÃO CAIA NESSA

Como proteger você, sua família e seu  
negócio dos golpes digitais da era da IA

FELIPE PINTO GOMES

# Não Caia Nessa

Como proteger você, sua família e seu negócio dos golpes digitais da era da IA

Felipe Pinto Gomes

## Introdução: por que qualquer pessoa pode cair em um golpe

Se você já caiu em um golpe, ou quase caiu, saiba de uma coisa logo de início: você não é ingênuo. Você foi alvo de profissionais.

Golpistas digitais estudam o comportamento humano, testam mensagens, ajustam o roteiro e repetem o que funciona. Eles trabalham em equipe, têm metas e usam tecnologia de ponta. Do outro lado está você, no meio de um dia corrido, com o celular na mão e mil coisas na cabeça.

Não é uma disputa justa. Mas dá para virar o jogo.

### A história de Dona Lúcia

*Caso ilustrativo.* Dona Lúcia tem 67 anos, é professora aposentada e usa o WhatsApp todos os dias para falar com os netos. Numa terça-feira, recebeu uma mensagem de um número desconhecido:

"Oi mãe, troquei de número. Salva esse aqui. O outro deu problema."

A foto do perfil era do filho dela, Marcos. O jeito de escrever parecia o dele. Meia hora depois, veio o pedido: Marcos precisava pagar um fornecedor urgente, mas o aplicativo do banco estava bloqueado. Ele devolveria o dinheiro no dia seguinte.

Dona Lúcia fez dois Pix, somando R\$ 4.800. Só descobriu a verdade à noite, quando ligou para o número antigo do filho para saber se estava tudo bem.

Dona Lúcia é uma mulher inteligente, cuidadosa e experiente. Mesmo assim, caiu. Por quê? Porque o golpe foi desenhado para funcionar exatamente com pessoas como ela: que amam a família e querem ajudar.

### O golpe não ataca sua inteligência, ataca suas emoções

Todo golpe bem feito explora algo bom ou humano em nós: o amor pela família, a vontade de ajudar, o medo de perder dinheiro, a esperança de uma oportunidade. Quando a emoção sobe, o raciocínio desce.

Por isso, médicos, advogados, engenheiros e até profissionais de tecnologia caem em golpes todos os dias. Inteligência não protege ninguém. O que protege é **conhecimento e hábito**.

## Por que agora ficou mais perigoso

Três mudanças recentes tornaram os golpes mais frequentes e mais convincentes:

| Mudança                 | O que mudou para o golpista                                                              |
|-------------------------|------------------------------------------------------------------------------------------|
| Pix e bancos digitais   | O dinheiro sai em segundos e é transferido para outras contas antes que a vítima perceba |
| Vazamento de dados      | Golpistas já sabem seu nome, CPF, endereço e até nomes de parentes                       |
| Inteligência artificial | Mensagens sem erros, vozes clonadas e vídeos falsos que parecem reais                    |

O resultado é que o golpe de hoje não tem mais erros de português gritantes nem histórias absurdas. Ele chega com seu nome, com a foto de alguém que você conhece e, às vezes, com a voz dessa pessoa.

## O que você vai encontrar neste livro

Este livro é um guia prático. Não é preciso saber nada de tecnologia para entender e aplicar o que está aqui.

| Parte                     | O que você vai aprender                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------|
| 1. Entendendo o inimigo   | Como os golpistas pensam, se organizam e usam a IA                                      |
| 2. Os golpes mais comuns  | Como funcionam os golpes de WhatsApp, Pix, compras, emprego, investimento, amor e dados |
| 3. Proteção na prática    | Como blindar seu celular, sua família e seu negócio                                     |
| 4. Quando o pior acontece | O que fazer nas primeiras horas depois de um golpe                                      |

Cada capítulo começa com uma história, explica como o golpe funciona, mostra os sinais de alerta e termina com um quadro **Na prática**, com um checklist que você pode aplicar no mesmo dia.

As histórias marcadas como ilustrativas foram criadas para representar situações comuns. Elas não se referem a pessoas reais, mas são baseadas em golpes que acontecem todos os dias no Brasil.

## Uma regra para levar desde já

Se você não lembrar de mais nada deste livro, lembre desta regra:

**Pressa e segredo são as duas marcas do golpe.** Sempre que alguém pedir que você aja rápido e não conte para ninguém, pare. Respire. Confirme por outro caminho.

Agora, vamos conhecer o inimigo.

## Capítulo 1: A indústria do golpe

O golpista que manda mensagem para você raramente é uma pessoa sozinha. Na maioria dos casos, ele faz parte de uma estrutura organizada, que funciona como uma empresa: tem funções, metas, fornecedores e até treinamento.

Entender isso muda a forma como você enxerga o problema. Você não está lidando com um amador. Está lidando com uma indústria.

### A história de Rafael

*Caso ilustrativo.* Rafael, 34 anos, analista de sistemas, recebeu uma ligação às 9h da manhã. A pessoa se apresentou como funcionária da central de segurança do banco dele. Sabia seu nome completo, os quatro últimos números do cartão e o valor da última compra.

Ela informou que havia uma compra suspeita de R\$ 2.390 em uma loja de eletrônicos e perguntou se ele reconhecia. Rafael disse que não. A atendente, muito educada, explicou que precisaria transferi-lo para o setor de contestação.

No fundo, dava para ouvir o barulho de uma central de atendimento: outras vozes, teclados, até música de espera. Tudo parecia real. Quarenta minutos depois, Rafael havia instalado um aplicativo "de segurança" no celular e perdido acesso à própria conta.

Rafael trabalha com tecnologia. Mesmo assim, caiu. O motivo é simples: ele estava diante de uma operação profissional.

## Como uma quadrilha digital se organiza

As investigações policiais no Brasil mostram que muitas quadrilhas dividem o trabalho em funções especializadas. Cada pessoa faz uma parte, o que torna o golpe mais eficiente e dificulta a investigação.

| Função              | O que faz                                                                   | Comparação com uma empresa       |
|---------------------|-----------------------------------------------------------------------------|----------------------------------|
| Fornecedor de dados | Compra ou obtém listas com nomes, CPFs, telefones e dados bancários vazados | Setor de inteligência de mercado |
| Roteirista          | Cria e testa as histórias e mensagens que mais convencem                    | Marketing                        |
| Operador            | Faz as ligações e conversa com as vítimas                                   | Atendimento e vendas             |
| Técnico             | Clona números, cria sites falsos, desenvolve aplicativos maliciosos         | Tecnologia                       |
| Laranja             | Empresta ou vende a própria conta bancária para receber o dinheiro          | Tesouraria                       |
| Lavador             | Espalha o dinheiro por várias contas e o transforma em bens ou criptomoedas | Financeiro                       |

Repare que muitas dessas pessoas nunca falam com a vítima. O laranja, por exemplo, pode ser alguém que vendeu o acesso à própria conta por algumas centenas de reais, sem saber direito para que seria usada.

## O golpe é um negócio de volume

Golpistas sabem que a maioria das pessoas não vai cair. Eles não precisam enganar todo mundo. Precisam enganar apenas uma pequena parte.

Imagine uma quadrilha que envia 10 mil mensagens por dia. Se apenas uma em cada mil pessoas cair, são 10 vítimas por dia. Se cada vítima perder em média R\$ 2.000, a quadrilha fatura R\$ 20 mil por dia. Os números são ilustrativos, mas mostram a lógica: o golpe é um jogo de quantidade.

Isso explica algo importante. **Você não foi escolhido por ser fraco. Você foi sorteado em uma lista.** O golpista testa milhares de pessoas e trabalha com quem responde.

## O funil do golpe

Quase todo golpe passa pelas mesmas etapas, como um funil de vendas:

1. **Abordagem em massa:** mensagens, ligações ou anúncios enviados para milhares de pessoas.
2. **Filtro:** quem responde, clica ou atende mostra que é um possível alvo.
3. **Construção de confiança:** o golpista usa dados pessoais, cria intimidade ou finge ser uma instituição.
4. **Gatilho emocional:** cria urgência, medo ou oportunidade irresistível.
5. **Pedido:** dinheiro, senha, código, instalação de aplicativo ou dados.
6. **Desaparecimento:** bloqueia a vítima, apaga o perfil e transfere o dinheiro.

A boa notícia é que você pode interromper o golpe em qualquer uma dessas etapas. Quanto mais cedo, melhor. E a etapa mais fácil de quebrar é a terceira: quando você desconfia da confiança que alguém está tentando criar.

## De onde vêm os seus dados

Uma das coisas que mais assusta as vítimas é perceber que o golpista sabia muito sobre elas. Esses dados geralmente vêm de quatro fontes:

| Fonte                   | Exemplos                                                                     |
|-------------------------|------------------------------------------------------------------------------|
| Vazamentos de empresas  | Bases de lojas, operadoras, aplicativos e órgãos que sofreram ataques        |
| Redes sociais           | Fotos, nomes de familiares, onde você trabalha, onde estuda, onde viaja      |
| Golpes anteriores       | Formulários falsos e sites de phishing que coletaram dados de outras pessoas |
| Funcionários desonestos | Pessoas com acesso a sistemas que vendem informações                         |

Esses dados são vendidos em grupos fechados e mercados clandestinos na internet. Por isso, saber seu nome, CPF ou endereço **não prova** que alguém é do seu banco ou de uma empresa séria. Hoje, esses dados estão nas mãos de muita gente.

## Por que é tão difícil prender e recuperar

Vítimas frequentemente perguntam por que a polícia não resolve rapidamente. Há algumas razões:

- O dinheiro passa por várias contas de laranjas em minutos.
- Os golpistas usam chips e contas em nome de terceiros.
- Muitas quadrilhas operam de outros estados ou até de outros países.
- Cada vítima perde um valor que, isoladamente, parece pequeno para uma grande investigação.

Isso não significa que nada pode ser feito. O Brasil endureceu as punições para fraudes eletrônicas com a Lei 14.155, de 2021, e o Banco Central criou mecanismos de devolução para o Pix. Falaremos disso no Capítulo 13. Mas a verdade é que **prevenir é muito mais eficaz do que tentar recuperar**.

## O que o golpista mais teme

Se o golpe é um negócio, o golpista quer o máximo de resultado com o mínimo de esforço e risco. Ele foge de três coisas:

1. **Pessoas que desconfiam e confirmam.** Uma ligação para o número oficial do banco destrói o golpe.
2. **Pessoas que demoram.** O golpe depende de pressa. Tempo é o maior inimigo do golpista.
3. **Pessoas que conversam com outras.** Quando você conta para alguém, outra cabeça percebe o que a emoção escondeu.

Guarde essas três atitudes: **confirmar, esperar e conversar**. Elas aparecerão em quase todos os capítulos deste livro.

## Na prática

- ☐ Aceite que saber seus dados não prova a identidade de ninguém.
- ☐ Lembre que golpistas trabalham com volume: você foi sorteado, não escolhido.
- ☐ Sempre que receber um contato inesperado sobre dinheiro, desligue e ligue você mesmo para o número oficial.
- ☐ Ganhe tempo: nenhuma decisão financeira séria precisa ser tomada em cinco minutos.
- ☐ Converse com alguém de confiança antes de transferir dinheiro em situações incomuns.
- ☐ Nunca empreste ou venda sua conta bancária para terceiros. Laranjas também respondem criminalmente.

## Capítulo 2: A mente do golpista, os gatilhos emocionais

Golpes mudam de forma o tempo todo. Um dia é o falso parente, no outro é a falsa central do banco, depois é a vaga de emprego dos sonhos. Mas por trás de todos eles há um conjunto pequeno de truques psicológicos que se repetem.

Quem aprende a reconhecer esses truques fica protegido até contra golpes que ainda nem foram inventados.

### A história de Juliana

*Caso ilustrativo.* Juliana, 29 anos, estava saindo do trabalho quando recebeu um SMS: "Seu CPF será bloqueado hoje às 23h59 por pendência na Receita Federal. Regularize agora para evitar multa e restrições." Havia um link.

Ela estava cansada, com fome e preocupada com uma viagem marcada para a semana seguinte. Pensou: "E se meu CPF for bloqueado e eu não conseguir embarcar?". Clicou, preencheu os dados e pagou uma "taxa de regularização" de R\$ 197,40.

No dia seguinte, mais calma, percebeu que a Receita Federal não manda SMS com links de pagamento. O golpe funcionou porque juntou três ingredientes: **autoridade, medo e pressa.**

### Por que a emoção vence a razão

Nosso cérebro funciona em dois modos. Um é rápido, automático e emocional. O outro é lento, cuidadoso e racional. No dia a dia, usamos muito o modo rápido, porque ele economiza energia.

O golpista quer que você fique no modo rápido. Para isso, ele cria situações que disparam emoções fortes. Quando você está com medo, ansioso ou empolgado, o modo racional praticamente desliga.

A defesa, portanto, é simples de entender e difícil de praticar: **ganhar tempo para o modo racional voltar a funcionar.**

### Os sete gatilhos do golpe

Quase todo golpe usa um ou mais destes sete gatilhos:

| Gatilho  | Como aparece               | Exemplo de frase                        |
|----------|----------------------------|-----------------------------------------|
| Urgência | Prazo curtíssimo para agir | "Você tem 10 minutos antes do bloqueio" |

| Gatilho      | Como aparece                                 | Exemplo de frase                                  |
|--------------|----------------------------------------------|---------------------------------------------------|
| Medo         | Ameaça de perda, punição ou dano             | "Sua conta foi invadida", "Seu filho foi preso"   |
| Autoridade   | Finge ser banco, governo, polícia ou empresa | "Aqui é da central de segurança"                  |
| Afeto        | Usa o amor por familiares e amigos           | "Mãe, preciso de ajuda, não conta pro pai"        |
| Ganância     | Promete ganho fácil ou fora do comum         | "Renda de R\$ 500 por dia curtindo vídeos"        |
| Escassez     | Oferta limitada ou exclusiva                 | "Últimas 3 unidades com 80% de desconto"          |
| Prova social | Mostra que outros já aproveitaram            | Depoimentos falsos, grupos cheios de "ganhadores" |

Repare que muitos golpes combinam vários gatilhos ao mesmo tempo. O golpe do falso parente, por exemplo, usa afeto, urgência e segredo. O golpe da falsa central usa autoridade, medo e urgência.

### O segredo: o gatilho escondido

Existe um oitavo elemento que aparece em quase todos os golpes, mesmo quando não é dito diretamente: o **isolamento**.

O golpista quer que você decida sozinho. Ele diz "não desliga", "não conta para ninguém", "é confidencial", "não fala com o gerente porque ele pode estar envolvido". Tudo isso tem um objetivo: impedir que outra pessoa olhe a situação com calma e diga "isso é golpe".

Sempre que alguém pedir segredo em uma situação que envolve dinheiro, trate isso como um alarme vermelho.

### Os golpistas se aproveitam do momento

Golpistas também escolhem a hora certa. Algumas situações deixam todos nós mais vulneráveis:

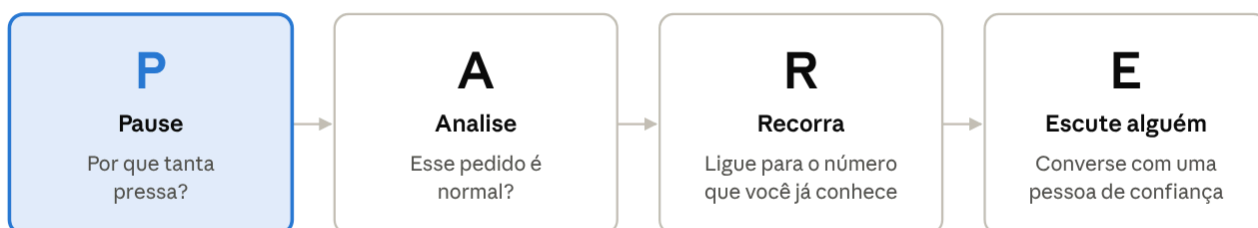
- **Cansaço:** fim do dia, madrugada, depois de um plantão.
- **Pressa:** saindo de casa, no trânsito, no meio de uma reunião.
- **Momentos de fragilidade:** luto, doença, separação, desemprego.
- **Datas especiais:** Black Friday, Natal, declaração do Imposto de Renda, volta às aulas.
- **Notícias em alta:** benefícios do governo, catástrofes, eventos esportivos.

Não é coincidência que muitos golpes cheguem em horários incômodos. O golpista sabe que você vai pensar menos.

## O método PARE

Para colocar tudo isso em prática, use um método simples, fácil de lembrar em qualquer situação. Chame de **PARE**:

**Parar antes de agir já quebra a maior parte dos golpes**



Método PARE · 4 passos

O PARE funciona porque ataca exatamente o que o golpista precisa: pressa, emoção e isolamento. Se você aplicar só a letra P, já terá evitado a maior parte dos golpes.

## Desconfiar não é ser grosseiro

Muitas pessoas caem em golpes por educação. Não querem desligar na cara de alguém, não querem parecer desconfiadas, não querem ofender um parente.

É importante tirar essa culpa. Empresas sérias **nunca** se ofendem quando você diz: "Vou desligar e ligar para o número oficial". Familiares de verdade **nunca** se ofendem quando você liga para confirmar. Só o golpista fica irritado com a confirmação.

Na verdade, a irritação é mais um sinal de alerta. Se a pessoa do outro lado insiste, pressiona ou fica agressiva quando você quer confirmar, você já tem sua resposta.

## Frases que devem acender o alerta

Algumas frases aparecem tanto em golpes que valem como um detector rápido:

- "Não desliga, senão o processo é cancelado."
- "Não conta para ninguém."
- "Só hoje" ou "últimas horas".
- "Faz um Pix de teste" ou "um Pix para validar".
- "Instala esse aplicativo para eu te ajudar."
- "Me passa o código que chegou no seu celular."
- "Seu nome está envolvido em uma investigação."

- "Você foi selecionado" ou "você ganhou".
- "Te devolvo amanhã sem falta."

Se ouvir ou ler qualquer uma delas, aplique o PARE imediatamente.

## Na prática

- ☐ Decore o método PARE: pause, analise, recorra a outro canal, escute alguém.
- ☐ Desconfie de qualquer pedido que junte pressa e dinheiro.
- ☐ Trate pedidos de segredo como alarme vermelho.
- ☐ Evite decisões financeiras quando estiver cansado, com pressa ou abalado.
- ☐ Não tenha vergonha de desligar e confirmar. Quem é sério entende.
- ☐ Combine com sua família: "Antes de qualquer transferência fora do comum, a gente liga um para o outro".

## Capítulo 3: A IA mudou o jogo

Durante anos, uma das melhores dicas contra golpes era: "repare nos erros de português". Essa dica envelheceu. Com a inteligência artificial, o golpista escreve melhor, fala com a voz de quem você ama e aparece em vídeo com o rosto de pessoas famosas.

Este capítulo explica, sem complicação, o que mudou e como se proteger.

### Um caso real que chocou o mundo

Em 2024, um funcionário do setor financeiro de uma multinacional em Hong Kong participou de uma videoconferência com quem parecia ser o diretor financeiro da empresa e outros colegas. Todos estavam na tela, conversando normalmente.

O diretor pediu uma série de transferências urgentes e confidenciais. O funcionário obedeceu e transferiu o equivalente a cerca de US\$ 25 milhões. Depois, descobriu que todas as pessoas da reunião, exceto ele, eram imagens e vozes falsas criadas com inteligência artificial.

Se isso aconteceu em uma grande empresa, com profissionais treinados, pode acontecer em qualquer lugar. Inclusive no grupo da família.

### O que é essa tal de IA

Inteligência artificial é um tipo de programa de computador que aprende com exemplos. Se você mostrar a ela muitas fotos de uma pessoa, ela aprende a criar novas imagens dessa pessoa. Se mostrar alguns segundos de uma voz, ela aprende a imitar essa voz.

Hoje, muitas dessas ferramentas são baratas ou gratuitas e fáceis de usar. Não é preciso ser um gênio da computação. Por isso, os golpistas adotaram a IA rapidamente.

## As quatro armas da IA nas mãos dos golpistas

| Arma                   | O que faz                                                          | Como aparece nos golpes                                                             |
|------------------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Texto perfeito         | Escreve mensagens sem erros, no tom certo, em segundos             | E-mails e mensagens de bancos, empresas e órgãos públicos idênticos aos verdadeiros |
| Voz clonada            | Imita a voz de uma pessoa a partir de poucos segundos de áudio     | Áudio de WhatsApp ou ligação de um "filho" pedindo dinheiro                         |
| Vídeo falso (deepfake) | Cria vídeos de pessoas falando coisas que nunca disseram           | Famosos recomendando investimentos, "chefe" em videochamada                         |
| Robôs de conversa      | Conversam com centenas de vítimas ao mesmo tempo, 24 horas por dia | Perfis falsos de namoro, atendimento falso, grupos de investimento                  |

## Deepfake: quando ver não é mais acreditar

**Deepfake** é o nome dado a vídeos, fotos ou áudios falsos criados por IA para imitar uma pessoa real.

No Brasil, tornaram-se comuns anúncios em redes sociais com vídeos de apresentadores, médicos, empresários e políticos famosos recomendando investimentos milagrosos, remédios ou jogos de aposta. Essas pessoas nunca gravaram aqueles vídeos.

A regra é clara: **um vídeo de uma pessoa famosa recomendando um produto ou investimento não prova nada**. Se a oferta parece boa demais, o vídeo provavelmente é falso.

## Voz clonada: o golpe mais perigoso para famílias

Para clonar uma voz, o golpista precisa de poucos segundos de áudio. Ele pode conseguir isso em:

- Vídeos publicados em redes sociais.
- Áudios enviados em grupos de WhatsApp.
- Uma ligação rápida em que a pessoa diz "alô, quem fala?".

Com a voz clonada, o golpista envia um áudio ou faz uma ligação curta, geralmente em tom de desespero: "Mãe, sofri um acidente", "Pai, fui assaltado, preciso de dinheiro". O áudio costuma ser curto e cheio de emoção, justamente para não dar tempo de você perceber detalhes estranhos.

## Como identificar conteúdo falso

A tecnologia está melhorando rápido, então os sinais visuais vão ficando mais difíceis de perceber. Ainda assim, vale observar:

| Tipo     | Sinais de alerta                                                                                                                |
|----------|---------------------------------------------------------------------------------------------------------------------------------|
| Vídeo    | Boca que não acompanha bem as palavras, piscadas estranhas, rosto que "derrete" em movimentos rápidos, iluminação inconsistente |
| Voz      | Tom monótono ou robótico, respiração ausente, ruídos estranhos, frases curtas e genéricas                                       |
| Texto    | Linguagem perfeita mas impessoal, ausência de detalhes que só a pessoa saberia                                                  |
| Contexto | Pedido incomum, urgência, segredo, oferta boa demais                                                                            |

O sinal mais confiável, porém, não é técnico. É o **contexto**. Mesmo que a voz seja perfeita, o pedido continua estranho: dinheiro, urgência e segredo.

## A melhor defesa: a palavra-código

Contra voz e vídeo falsos, a proteção mais eficaz é antiga e simples: **uma palavra-código combinada com a família**.

Funciona assim: você e seus familiares escolhem uma palavra ou pergunta que só vocês conhecem. Em qualquer pedido de dinheiro urgente, por telefone, áudio ou vídeo, quem recebe pede a palavra-código. O golpista não terá a resposta.

Dicas para escolher:

- Não use datas de nascimento, nomes de pets ou informações que aparecem nas redes sociais.
- Prefira algo inusitado, como "abacate azul" ou o nome de um lugar de uma viagem antiga.
- Combine pessoalmente, nunca por mensagem.
- Troque a palavra se ela for usada ou se desconfiar que vazou.

No Capítulo 11, você encontrará um modelo completo de combinação familiar.

## Confirme por outro canal

A segunda grande defesa é a confirmação por outro canal. Se o pedido veio por áudio no WhatsApp, ligue para o número que você já tinha salvo. Se veio por videochamada, mande mensagem para outro número ou fale com outra pessoa da família.

Uma pergunta simples também ajuda: faça algo que só a pessoa real saberia responder. "Qual foi o nome do restaurante onde comemoramos seu aniversário?". Golpistas, mesmo com IA, não têm acesso às suas memórias.

## Cuidado com o que você publica

Não é preciso abandonar as redes sociais, mas vale reduzir a matéria-prima dos golpistas:

- Deixe perfis com informações pessoais restritos a amigos.
- Evite publicar vídeos longos falando diretamente para a câmera em perfis abertos.
- Não informe em tempo real onde você está ou que viajou.
- Ensine crianças e idosos da família a fazer o mesmo.

## A IA também protege

Nem tudo é ameaça. Bancos e empresas de tecnologia também usam inteligência artificial para detectar transações suspeitas, bloquear mensagens fraudulentas e identificar sites falsos. Por isso, mantenha aplicativos atualizados e não ignore alertas do seu banco.

## Na prática

- ☐ Combine uma palavra-código com sua família ainda esta semana.
- ☐ Desconfie de áudios e vídeos com pedidos de dinheiro, mesmo com voz e rosto conhecidos.
- ☐ Confirme sempre por outro canal, usando contatos que você já tinha salvos.
- ☐ Não acredite em vídeos de famosos recomendando investimentos ou produtos milagrosos.
- ☐ Restrinja quem pode ver seus vídeos e fotos nas redes sociais.
- ☐ Ao atender números desconhecidos, espere a pessoa falar primeiro.

## Capítulo 4: WhatsApp e redes sociais

O WhatsApp é o aplicativo mais usado pelos brasileiros para conversar com a família, com amigos e até com empresas. Por isso mesmo, é um dos principais palcos dos golpes digitais. O mesmo vale para Instagram, Facebook e outras redes.

A boa notícia é que a maior parte desses golpes segue poucos roteiros. Conhecendo os roteiros, fica muito mais fácil reconhecer o golpe.

### A história de Carlos

*Caso ilustrativo.* Carlos, 52 anos, dono de uma pequena oficina, recebeu uma mensagem de um número desconhecido com a foto do seu cunhado, Paulo. "Fala, Carlos! Esse é meu número novo. Tô numa correria aqui, depois te explico."

Horas depois, "Paulo" pediu ajuda: precisava pagar um boleto de R\$ 1.850 que vencia naquele dia, mas o limite do Pix tinha estourado. Pediu para Carlos pagar e prometeu devolver no dia seguinte.

Carlos desconfiou do português um pouco diferente e ligou para o número antigo do cunhado. Paulo atendeu, surpreso: não tinha trocado de número. Carlos não perdeu nada porque fez a coisa certa: **confirmou por outro canal**.

### Os golpes mais comuns no WhatsApp

| Golpe                              | Como funciona                                                      | Sinal de alerta                                        |
|------------------------------------|--------------------------------------------------------------------|--------------------------------------------------------|
| Falso parente ou amigo             | Usa foto de alguém conhecido em um número novo e pede dinheiro     | "Troquei de número" seguido de pedido de Pix           |
| Clonagem de WhatsApp               | Pede o código de seis dígitos que chega por SMS e assume sua conta | Qualquer pedido para informar um código recebido       |
| Falsa empresa                      | Finge ser loja, banco, operadora ou serviço de entrega             | Contato não solicitado com link ou pedido de pagamento |
| Falso sorteio ou brinde            | Avisa que você ganhou um prêmio e cobra uma taxa para liberar      | Você não participou de nenhum sorteio                  |
| Falso link de pesquisa ou cadastro | Pede para preencher um formulário com dados pessoais               | Promessa de prêmio por responder perguntas             |

| Golpe                 | Como funciona                                                | Sinal de alerta                          |
|-----------------------|--------------------------------------------------------------|------------------------------------------|
| Grupo de investimento | Adiciona você a grupos com "especialistas" e supostos lucros | Promessas de ganhos rápidos e garantidos |

## Clonagem x número falso: qual a diferença?

Muitas pessoas confundem os dois golpes mais comuns:

- **Número falso:** o golpista cria uma conta nova, com outro número, e coloca a foto de alguém que você conhece. A conta verdadeira da pessoa continua funcionando normalmente.
- **Clonagem:** o golpista assume a conta verdadeira da pessoa, com o mesmo número. Para isso, ele precisa do código de verificação de seis dígitos que o WhatsApp envia por SMS.

O golpe de clonagem geralmente começa com uma desculpa: "Sou do restaurante onde você fez o pedido, vou te mandar um código de confirmação", "Sou do site de vendas, preciso confirmar seu anúncio". O código, na verdade, é o que permite ao golpista entrar no seu WhatsApp.

**Regra de ouro:** o código de verificação do WhatsApp é como a chave da sua casa. Nunca passe para ninguém, por nenhum motivo.

## Como ativar a verificação em duas etapas

A verificação em duas etapas cria uma senha de seis dígitos que você escolhe. Mesmo que alguém consiga o código do SMS, não conseguirá entrar na sua conta sem essa senha.

O caminho no aplicativo costuma ser:

1. Abra o WhatsApp e vá em **Configurações**.
2. Toque em **Conta**.
3. Toque em **Confirmação em duas etapas** e depois em **Ativar**.
4. Crie um PIN de seis dígitos fácil de lembrar e difícil de adivinhar.
5. Cadastre um e-mail para recuperar o PIN caso esqueça.

Os nomes dos menus podem mudar um pouco conforme a versão do aplicativo, mas a opção sempre fica dentro das configurações da conta.

## Golpes nas redes sociais

Instagram, Facebook e TikTok também são usados para golpes, com algumas variações:

| Golpe                         | Como funciona                                                                        |
|-------------------------------|--------------------------------------------------------------------------------------|
| Perfil invadido               | O golpista invade a conta de um amigo e oferece produtos ou pede dinheiro emprestado |
| Venda de móveis e eletrônicos | Perfil de amigo invadido anuncia itens baratos porque "está de mudança"              |
| Anúncio patrocinado falso     | Anúncios com vídeos falsos de famosos levam para sites fraudulentos                  |
| Falso suporte da plataforma   | Mensagem dizendo que sua conta será desativada se você não clicar em um link         |
| Perfil falso de empresa       | Copia o perfil de uma loja verdadeira e vende produtos que nunca chegam              |

Um golpe muito comum é o do **amigo vendendo coisas de mudança**. Você vê nos Stories um amigo anunciando uma geladeira ou um sofá por preço baixíssimo. Na verdade, a conta dele foi invadida. O pagamento antecipado por Pix nunca volta.

### Sinais de que um perfil foi invadido

- Publicações fora do estilo habitual da pessoa.
- Ofertas de produtos muito baratos ou de investimentos.
- Pedidos de empréstimo ou de ajuda financeira por mensagem.
- Linguagem diferente da que a pessoa costuma usar.
- Pressa para fechar o negócio.

Se perceber algo assim, avise o amigo por outro meio, como uma ligação, e denuncie o perfil na própria plataforma.

### O que fazer se receber uma mensagem suspeita

1. **Não responda e não clique em links.**
2. **Confirme por outro canal:** ligue para o número antigo ou fale com alguém próximo da pessoa.
3. **Faça uma pergunta pessoal** que só a pessoa verdadeira saberia responder.
4. **Bloqueie e denuncie** o número no próprio WhatsApp.
5. **Avise a família e os amigos**, porque o golpista provavelmente está mandando mensagens para outros contatos.

## O que fazer se seu WhatsApp for clonado

- Reinstale o WhatsApp e confirme seu número para recuperar a conta.
- Avise imediatamente seus contatos, por outros meios, que sua conta foi invadida.
- Escreva para o suporte do WhatsApp pelo e-mail ou formulário indicado no aplicativo.
- Registre um boletim de ocorrência, que pode ser feito pela internet na maioria dos estados.
- Ative a verificação em duas etapas assim que recuperar o acesso.

## Na prática

- ☐ Ative hoje a verificação em duas etapas do WhatsApp.
- ☐ Nunca informe códigos recebidos por SMS para ninguém.
- ☐ Desconfie de qualquer "número novo" que pede dinheiro, mesmo com foto conhecida.
- ☐ Confirme pedidos de dinheiro ligando para o número antigo da pessoa.
- ☐ Em Configurações de Privacidade, limite quem pode ver sua foto de perfil e quem pode adicionar você a grupos.
- ☐ Desconfie de vendas e empréstimos anunciados por amigos nas redes sociais.

## Capítulo 5: Pix, bancos e cartões

O Pix trouxe uma enorme praticidade para a vida dos brasileiros. Com poucos toques, o dinheiro chega em segundos, a qualquer hora. Essa mesma rapidez, porém, é o que torna o Pix tão atraente para golpistas: quando a vítima percebe o erro, o dinheiro já passou por várias contas.

O Pix em si é seguro. O que os golpistas fazem é enganar as pessoas para que elas mesmas façam a transferência ou entreguem o acesso às suas contas.

### A história de Seu Antônio

*Caso ilustrativo.* Seu Antônio, 71 anos, recebeu uma ligação de um número parecido com o do seu banco. A atendente disse que haviam detectado uma tentativa de empréstimo de R\$ 15 mil em seu nome e que, para cancelar, ele precisaria seguir algumas instruções.

Primeiro, pediu que ele baixasse um aplicativo para "proteger o celular". Depois, pediu que ele abrisse o aplicativo do banco para "conferir o saldo". Enquanto isso, do outro lado, golpistas controlavam a tela do celular dele à distância.

Em poucos minutos, foram feitos três Pix e um empréstimo pré-aprovado foi contratado. Seu Antônio viu tudo acontecer na tela sem entender. Esse é o golpe conhecido como **mão fantasma**.

## Os golpes bancários mais comuns

| Golpe                             | Como funciona                                                                                | O que o banco de verdade nunca faz                       |
|-----------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Falsa central de atendimento      | Ligação ou mensagem de alguém se passando pelo banco, avisando de compra suspeita            | Pedir senha, código ou transferência para "conta segura" |
| Mão fantasma                      | Golpista convence a vítima a instalar app de acesso remoto e controla o celular              | Pedir para instalar aplicativos por telefone             |
| Conta segura                      | Pede para você transferir o dinheiro para uma conta "protegida" enquanto resolve um problema | Pedir que você transfira dinheiro para resolver fraude   |
| Golpe do motoboy                  | Diz que seu cartão foi clonado e envia alguém para buscá-lo                                  | Mandar alguém buscar cartão na sua casa                  |
| Boleto falso                      | Boleto adulterado com dados de pagamento do golpista                                         | Enviar boleto por canais não oficiais com urgência       |
| Pix agendado ou comprovante falso | Golpista mostra comprovante falso ou agendado para receber produto                           | Considerar agendamento como pagamento feito              |
| Pix errado                        | Alguém diz que fez um Pix por engano e pede devolução para outra conta                       | Exigir devolução por fora do sistema                     |

### A regra mais importante deste capítulo

**Banco nenhum liga para você pedindo senha, código, transferência, instalação de aplicativo ou entrega de cartão.** Se isso acontecer, é golpe. Desligue e ligue você para o número que está no verso do seu cartão ou no aplicativo oficial.

Golpistas conseguem fazer aparecer no seu celular um número parecido ou até igual ao do banco. Por isso, **não confie no número que aparece na tela**. A única forma segura é desligar e ligar você mesmo, de preferência de outro telefone ou esperando alguns minutos.

## O golpe do Pix devolvido

Uma variação curiosa funciona assim: você recebe um Pix de valor baixo, de alguém desconhecido. Logo depois, chega uma mensagem: "Desculpa, fiz um Pix errado para você, pode me devolver?". O golpista pede que você devolva para outra chave.

O problema é que o Pix original pode ter vindo de uma conta de outra vítima, ou o golpista pode pedir a devolução pelo sistema oficial depois, recebendo o valor duas vezes. Se receber um Pix por engano, **use a opção de devolução do próprio aplicativo do banco**, que devolve para a conta de origem. Nunca transfira para outra chave.

## Antes de confirmar um Pix, confira

A tela de confirmação do Pix mostra o nome de quem vai receber e parte do CPF ou CNPJ. Esse é o momento de salvar o seu dinheiro.

| Confira              | Pergunta                                                     |
|----------------------|--------------------------------------------------------------|
| Nome do destinatário | É mesmo a pessoa ou empresa que eu queria pagar?             |
| Tipo de destinatário | Uma loja grande recebendo em CPF de pessoa física? Desconfie |
| Valor                | Está correto, sem dígitos a mais?                            |
| Instituição          | Faz sentido o banco do destinatário?                         |

Se o nome não bater, cancele. Uma loja que pede Pix para o CPF de uma pessoa desconhecida, ou um parente cujo Pix vai para o nome de outra pessoa, é sinal claro de golpe.

## Cartões de crédito e débito

Alguns cuidados simples reduzem muito os riscos com cartões:

- Prefira o **cartão virtual** nas compras pela internet. Ele pode ser gerado no aplicativo do banco e cancelado facilmente.
- Ative as **notificações** de todas as compras no aplicativo do banco.
- Nunca entregue seu cartão a ninguém que vá até sua casa "buscar", mesmo que diga ser do banco.
- Ao pagar em maquininhas, confira o valor no visor antes de digitar a senha.
- Se o cartão for clonado, bloqueie pelo aplicativo e conteste as compras imediatamente.

## Ferramentas de proteção que você já tem

Os bancos oferecem recursos de segurança que muita gente não usa. Vale conhecer:

| Recurso                         | Para que serve                                                                                                                          |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Limite de Pix noturno           | Desde 2021, o Banco Central estabeleceu um limite padrão menor para Pix entre 20h e 6h para pessoas físicas, que você pode manter baixo |
| Ajuste de limites               | Você pode reduzir os limites diários de Pix e transferências; aumentos costumam levar um tempo para entrar em vigor                     |
| Cadastro de contatos confiáveis | Alguns bancos permitem limites maiores só para pessoas cadastradas previamente                                                          |
| Notificações                    | Avisam na hora sobre qualquer transação                                                                                                 |
| Biometria e senha               | Dificultam o uso do aplicativo por terceiros                                                                                            |

Uma dica valiosa: **mantenha os limites de Pix baixos no dia a dia** e aumente apenas quando precisar. Se um golpista conseguir acesso, o prejuízo será menor.

## Cuidado com os aplicativos de acesso remoto

Aplicativos que permitem controlar o celular à distância são ferramentas legítimas, usadas por equipes de suporte técnico. Nas mãos de golpistas, viram a principal arma da mão fantasma.

Nunca instale aplicativos a pedido de alguém que ligou para você. Se o seu celular pedir permissão de "acessibilidade" ou "compartilhamento de tela" para um aplicativo que você não conhece, negue.

## Na prática

- ☐ Salve o número oficial do seu banco e só ligue para ele.
- ☐ Desligue sempre que alguém do "banco" pedir senha, código, transferência ou instalação de aplicativo.
- ☐ Confira o nome do destinatário antes de confirmar qualquer Pix.
- ☐ Reduza seus limites de Pix e mantenha o limite noturno baixo.
- ☐ Use cartão virtual nas compras pela internet.
- ☐ Ative notificações de todas as transações.
- ☐ Se receber um Pix por engano, devolva apenas pelo botão de devolução do próprio aplicativo.

## Capítulo 6: Compras e ofertas falsas

Comprar pela internet é prático, barato e, na maioria das vezes, seguro. Mas os golpistas sabem que todo mundo gosta de uma boa oferta. Por isso, criam lojas falsas, anúncios enganosos e promoções que parecem imperdíveis.

Neste capítulo, você vai aprender a separar a oferta boa da armadilha.

### A história de Fernanda

*Caso ilustrativo.* Fernanda, 38 anos, queria comprar uma air fryer para a mãe. Rolando o Instagram, viu um anúncio de uma loja com um modelo de marca conhecida por R\$ 159, quando em outras lojas custava mais de R\$ 500. A página tinha logotipo bonito, fotos profissionais e muitos comentários positivos.

O site aceitava apenas Pix, com "10% de desconto adicional". Fernanda pagou. O código de rastreio nunca funcionou, o WhatsApp de atendimento parou de responder e, uma semana depois, o site tinha sumido.

Os comentários eram falsos, as fotos foram copiadas de lojas reais e o domínio do site tinha sido criado dias antes. Fernanda caiu no golpe da **loja falsa**.

### Os golpes de compra mais comuns

| Golpe                       | Como funciona                                                       | Sinal de alerta                                                    |
|-----------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------|
| Loja falsa                  | Site bonito, com produtos de marca muito abaixo do preço de mercado | Desconto exagerado e pagamento só por Pix                          |
| Cópia de loja famosa        | Site imita uma loja conhecida, com endereço parecido                | Endereço do site com letras trocadas ou terminações estranhas      |
| Anúncio patrocinado         | Anúncio em rede social leva para site fraudulento                   | Oferta "relâmpago" com contador regressivo                         |
| Falso leilão                | Leilões de carros e imóveis com preços muito baixos                 | Pedido de depósito antecipado para "garantir o lance"              |
| Marketplace e classificados | Vendedor pede pagamento por fora da plataforma                      | "Me paga por Pix que te dou desconto"                              |
| Falsa taxa de entrega       | Mensagem dizendo que sua encomenda está retida e precisa pagar taxa | Você não estava esperando nenhuma entrega, ou o link não é oficial |

| Golpe           | Como funciona                                       | Sinal de alerta                                                |
|-----------------|-----------------------------------------------------|----------------------------------------------------------------|
| Falso comprador | Golpista "compra" seu produto com comprovante falso | Comprovante enviado por imagem e pressa para retirar o produto |

## O golpe da taxa de entrega

Esse merece atenção especial, porque atinge milhões de pessoas. Chega um SMS, e-mail ou WhatsApp: "Sua encomenda está retida. Pague a taxa de R\$ 9,90 para liberar a entrega". Há um link para um site idêntico ao dos Correios ou de transportadoras.

O valor pequeno faz a pessoa pagar sem pensar. Mas o objetivo pode ser outro: roubar dados do cartão de crédito digitados no site falso, que depois serão usados em compras maiores.

Sempre que receber aviso de encomenda retida, **não clique no link**. Abra você mesmo o site ou aplicativo oficial da transportadora e consulte pelo código de rastreio da sua compra.

## Como verificar se uma loja é confiável

Antes de comprar em uma loja que você não conhece, faça uma checagem rápida:

| Verificação         | Como fazer                                                                                             |
|---------------------|--------------------------------------------------------------------------------------------------------|
| Endereço do site    | Confira se o nome está escrito corretamente e se começa com "https"                                    |
| CNPJ                | Procure o CNPJ no rodapé do site e confira se a empresa existe e está ativa no site da Receita Federal |
| Reputação           | Pesquise o nome da loja em sites de reclamação e veja se responde aos clientes                         |
| Tempo de existência | Desconfie de lojas que ninguém conhece e que surgiram há poucos dias                                   |
| Formas de pagamento | Lojas sérias oferecem várias opções, como cartão e boleto                                              |
| Contato             | Verifique se há telefone, endereço físico e canais de atendimento reais                                |

| Verificação   | Como fazer                                                                                  |
|---------------|---------------------------------------------------------------------------------------------|
| Redes sociais | Perfis com poucas publicações, comentários bloqueados ou seguidores comprados são suspeitos |

O cadeado ao lado do endereço do site significa apenas que a conexão é criptografada. **Ele não garante que a loja é honesta.** Sites falsos também têm cadeado.

## Por que o golpista prefere o Pix

Lojas falsas quase sempre oferecem desconto para pagamento via Pix ou aceitam somente Pix. Isso acontece porque o Pix é instantâneo e mais difícil de contestar do que o cartão de crédito.

No cartão de crédito, você pode contestar uma compra não entregue junto ao banco emissor. No Pix, a devolução depende de mecanismos específicos e nem sempre o dinheiro é recuperado.

Por isso, ao comprar em lojas desconhecidas, **prefira o cartão de crédito, de preferência virtual.** O desconto do Pix não compensa o risco.

## Comprando e vendendo em classificados

Sites e aplicativos de classificados são muito usados para comprar e vender produtos usados. Alguns cuidados ajudam:

### Se você está comprando:

- Prefira negociar e pagar dentro da própria plataforma, quando ela oferece pagamento protegido.
- Desconfie de vendedores que pedem para continuar a conversa só pelo WhatsApp.
- Para itens de valor alto, como celulares e carros, veja o produto pessoalmente, em local público e movimentado.

### Se você está vendendo:

- Só entregue o produto depois de confirmar no aplicativo do seu banco que o dinheiro entrou.
- Não confie em comprovantes enviados por imagem. Eles podem ser falsos ou de Pix agendado.
- Nunca clique em links enviados pelo comprador para "receber o pagamento".

## Datas de risco

Golpes de compra aumentam muito em algumas épocas do ano:

- Black Friday e Cyber Monday.
- Dia das Mães, Dia dos Namorados e Natal.
- Lançamentos de celulares e videogames.
- Volta às aulas.

Nessas datas, redobre a atenção com anúncios em redes sociais e promoções que chegam por mensagem.

## Na prática

- ☐ Desconfie de preços muito abaixo do mercado, especialmente de marcas famosas.
- ☐ Confira endereço do site, CNPJ e reputação antes de comprar em lojas desconhecidas.
- ☐ Prefira cartão de crédito virtual em vez de Pix em lojas novas.
- ☐ Nunca clique em links de "taxa de entrega". Consulte o rastreio pelo site oficial.
- ☐ Ao vender, só entregue o produto após confirmar o dinheiro no aplicativo do banco.
- ☐ Lembre: cadeado no site não significa loja honesta.

## Capítulo 7: Emprego, investimento e renda extra

Quem precisa de dinheiro, quer mudar de vida ou sonha com uma renda extra é um alvo especialmente procurado pelos golpistas. Eles oferecem exatamente o que a pessoa deseja: um emprego, uma oportunidade, um investimento que vai multiplicar o dinheiro.

Esses golpes são cruéis porque atingem quem já está em um momento difícil. E, muitas vezes, levam a vítima a perder mais do que tinha, porque ela pega empréstimos ou envolve amigos e familiares.

### A história de Bruno

*Caso ilustrativo.* Bruno, 24 anos, estava desempregado havia seis meses. Recebeu uma mensagem no WhatsApp: "Olá! Vimos seu perfil e temos uma vaga de meio período, trabalhando de casa, com ganhos de R\$ 200 a R\$ 800 por dia. Basta curtir vídeos e avaliar produtos".

No primeiro dia, ele curtiu alguns vídeos e recebeu R\$ 30 por Pix. No segundo, recebeu R\$ 50. Então, foi colocado em um grupo onde as "tarefas premium" exigiam um depósito para liberar ganhos maiores. Bruno depositou R\$ 300 e ganhou R\$ 420 de volta. Depositou R\$ 1.500. Depois R\$ 4.000, emprestados da irmã.

Quando tentou sacar, o sistema pediu uma "taxa de liberação". Ele percebeu, tarde demais, que estava em um golpe. Os pequenos pagamentos iniciais existiam apenas para conquistar sua confiança.

## Golpes de emprego

| Golpe                        | Como funciona                                                   | Sinal de alerta                                                |
|------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|
| Trabalhe curtindo vídeos     | Paga pequenas quantias no início e depois exige depósitos       | Ganho alto para tarefas simples                                |
| Taxa de contratação          | Cobra por uniforme, curso, exame ou cadastro antes de começar   | Empresa séria não cobra para contratar                         |
| Falsa vaga de empresa famosa | Usa nome de grandes empresas para coletar dados ou cobrar taxas | Contato por WhatsApp sem processo seletivo formal              |
| Revenda de kits              | Pede para comprar um kit inicial para revender                  | Lucro depende de recrutar outras pessoas                       |
| Coleta de documentos         | Pede RG, CPF, selfie e comprovantes para "contratação"          | Documentos usados depois para abrir contas e fazer empréstimos |

**Regra simples:** emprego de verdade paga você. Se pedirem que você pague para trabalhar, é golpe.

## Golpes de investimento

Os golpes de investimento costumam envolver valores maiores e prometer retornos fora da realidade. Os mais comuns são:

- **Pirâmide financeira:** os "lucros" dos participantes antigos são pagos com o dinheiro dos novos. Quando param de entrar pessoas, o esquema desaba.
- **Falso investimento em criptomoedas:** plataformas que mostram ganhos incríveis na tela, mas não permitem saque.
- **Robô de investimento:** promessa de um programa que opera sozinho e garante lucro todos os dias.
- **Falso consórcio ou empréstimo:** cobra uma taxa antecipada para liberar crédito que nunca chega.

- **Grupos com "mentores":** grupos de WhatsApp ou Telegram com supostos especialistas e participantes que comemoram ganhos falsos.

## Como reconhecer um golpe de investimento

| Sinal                             | Por que é suspeito                                              |
|-----------------------------------|-----------------------------------------------------------------|
| Rendimento garantido e muito alto | Nenhum investimento sério garante ganhos muito acima do mercado |
| Pressa para entrar                | "Vagas limitadas" e "só hoje" são gatilhos de escassez          |
| Bônus por indicar amigos          | Típico de pirâmides, que dependem de novos participantes        |
| Dificuldade para sacar            | Taxas e desculpas para não liberar o dinheiro                   |
| Empresa sem registro              | Ofertas públicas de investimento precisam de autorização da CVM |
| Vídeos de famosos                 | Deepfakes de celebridades são muito usados nesses golpes        |

## A armadilha dos primeiros ganhos

Um detalhe importante: muitos golpes pagam no início. Essa é uma estratégia deliberada. O golpista devolve pequenas quantias para provar que "funciona" e conquistar sua confiança.

Depois, a vítima investe valores maiores, convence amigos e familiares a entrar e, quando tenta sacar, descobre que não há como. **Ter recebido no começo não prova que o negócio é legítimo.**

## Como verificar antes de investir

1. **Consulte a CVM** (Comissão de Valores Mobiliários), que mantém alertas sobre empresas não autorizadas a oferecer investimentos.
2. **Consulte o Banco Central**, que informa quais instituições são autorizadas a funcionar no país.
3. **Pesquise o nome da empresa** acompanhado das palavras "golpe" ou "reclamação".
4. **Desconfie de qualquer pressa.** Investimento sério espera você pensar.
5. **Converse com alguém de confiança** que entenda de finanças antes de colocar dinheiro.

## A comparação que ajuda

Uma forma simples de se proteger é comparar a promessa com investimentos conhecidos e regulados, como a poupança, o Tesouro Direto ou o CDB de grandes bancos. Se a oferta promete render muitas vezes mais, com garantia e sem risco, ela está mentindo.

No mundo real, rendimento alto vem sempre acompanhado de risco alto. Quando alguém promete os dois ao mesmo tempo, rendimento alto e risco zero, você está diante de um golpe.

## Quando o golpe envolve amigos

Pirâmides e falsos investimentos se espalham principalmente por indicação. Muitas vezes, quem convida é um amigo ou parente sincero, que também foi enganado e acredita estar ajudando.

Isso torna difícil dizer não. Uma resposta educada e firme ajuda: "Obrigado por pensar em mim, mas eu só invisto depois de consultar a CVM e o meu banco". Se o negócio for sério, ele resistirá à verificação.

## Na prática

- ☐ Nunca pague para conseguir um emprego.
- ☐ Desconfie de ganhos altos para tarefas simples, como curtir vídeos.
- ☐ Não envie documentos e selfies para "contratações" feitas só por WhatsApp.
- ☐ Consulte a CVM e o Banco Central antes de investir em qualquer empresa desconhecida.
- ☐ Lembre que ter recebido pequenos ganhos no início não prova nada.
- ☐ Fuja de qualquer investimento que pague bônus por indicar novas pessoas.

## Capítulo 8: Golpes amorosos e contra idosos

Alguns golpes atingem o bolso. Outros atingem o coração. Os golpes amorosos e os golpes contra idosos estão entre os mais cruéis, porque exploram a solidão, o carinho e a confiança.

Além do prejuízo financeiro, que costuma ser alto, as vítimas sofrem com vergonha, culpa e tristeza. Por isso, este capítulo pede um cuidado especial: **acolher, e não julgar**.

## A história de Marta

*Caso ilustrativo.* Marta, 58 anos, viúva havia três anos, conheceu "Richard" em uma rede social. Ele dizia ser um engenheiro americano trabalhando em uma plataforma de petróleo. Mandava mensagens carinhosas todos os dias, fotos bonitas e áudios com sotaque.

Depois de dois meses de conversa, Richard disse que queria vir ao Brasil para conhecê-la. Mas havia um problema: um pacote com presentes e documentos estava retido na alfândega e precisava de uma taxa. Depois veio outra taxa. Depois uma emergência médica. Depois um advogado.

Em seis meses, Marta enviou mais de R\$ 60 mil, incluindo um empréstimo consignado. Richard nunca existiu. As fotos eram de outra pessoa e as mensagens eram escritas por uma quadrilha.

## Como funciona o golpe do amor

O golpe amoroso, também chamado de **golpe do falso romance**, segue um roteiro muito conhecido:

| Etapa          | O que acontece                                                                                     |
|----------------|----------------------------------------------------------------------------------------------------|
| 1. Aproximação | Perfil atraente faz contato em rede social, aplicativo de namoro ou até em jogos online            |
| 2. Conquista   | Mensagens frequentes, elogios, declarações rápidas de amor e planos para o futuro                  |
| 3. Distância   | O golpista sempre tem um motivo para não se encontrar: trabalha no exterior, em navio, no exército |
| 4. Problema    | Surge uma emergência: alfândega, doença, viagem, documento, conta bloqueada                        |
| 5. Pedido      | Pede dinheiro, sempre com promessa de devolver                                                     |
| 6. Repetição   | Novos problemas aparecem, e os pedidos aumentam                                                    |

O golpista investe tempo. Às vezes, conversa por semanas ou meses antes de pedir dinheiro. Quando o pedido chega, a vítima já está emocionalmente envolvida.

## Sinais de alerta no golpe do amor

- A pessoa declara amor muito rápido, sem nunca ter encontrado você.

- Sempre há um motivo para não fazer videochamada ou para a câmera "não funcionar".
- A profissão é sempre longe e difícil de verificar: militar, engenheiro offshore, médico em missão humanitária.
- A história tem muitas tragédias e emergências.
- Pede segredo sobre o relacionamento ou sobre o dinheiro.
- Pede dinheiro, presentes, cartões ou dados bancários.

Uma verificação simples: use a busca reversa de imagens do Google ou de outro buscador para ver se as fotos da pessoa aparecem na internet com outros nomes. Muitas vezes, aparecem.

## Por que os idosos são alvos frequentes

Idosos não são menos inteligentes. Mas algumas condições os tornam alvos preferenciais:

- Costumam ter economias, aposentadoria e crédito consignado disponível.
- Muitos aprenderam a usar a tecnologia mais tarde e conhecem menos os truques digitais.
- Foram educados em uma época em que se confiava mais em ligações e autoridades.
- Podem viver sozinhos e ter menos pessoas para consultar no dia a dia.
- Têm medo de incomodar os filhos ou de parecer incapazes.

## Os golpes mais comuns contra idosos

| Golpe                     | Como funciona                                                                        |
|---------------------------|--------------------------------------------------------------------------------------|
| Falso parente             | Mensagem ou ligação de "filho" ou "neto" pedindo dinheiro urgente                    |
| Falsa central do banco    | Ligação dizendo que há fraude na conta e pedindo transferência ou cartão             |
| Falso INSS                | Promessa de revisão de aposentadoria, liberação de valores ou cobrança de pendências |
| Empréstimo não solicitado | Crédito consignado contratado sem autorização, com cobrança de "devolução"           |
| Falso sequestro           | Ligação com gritos e ameaças dizendo que um familiar foi sequestrado                 |
| Falso técnico             | Visita ou ligação de alguém que diz ser de empresa de luz, água ou internet          |

| Golpe                     | Como funciona                                                               |
|---------------------------|-----------------------------------------------------------------------------|
| Golpe do bilhete premiado | Pessoa simpática na rua pede ajuda para sacar um prêmio e exige um depósito |

O **INSS não liga** pedindo dados ou pagamentos e não manda pessoas na sua casa. Serviços do INSS podem ser consultados pelo aplicativo ou site oficial Meu INSS e pelo telefone 135.

## Como conversar sem humilhar

Muitos idosos escondem que caíram em golpes por vergonha. Isso faz o prejuízo crescer, porque o golpista volta a atacar. A forma como a família conversa faz toda a diferença.

| Evite dizer                           | Prefira dizer                                             |
|---------------------------------------|-----------------------------------------------------------|
| "Como você caiu nisso?"               | "Isso acontece com muita gente, inclusive com gente nova" |
| "Eu te avisei"                        | "Que bom que você me contou, vamos resolver juntos"       |
| "Você não pode mais mexer no celular" | "Vamos combinar algumas regras para ficar mais seguro"    |
| "Você é muito ingênuo"                | "Esses criminosos são profissionais, é difícil perceber"  |

O objetivo é que a pessoa se sinta segura para pedir ajuda **antes** de transferir dinheiro, e não depois.

## Como proteger quem você ama

- Combine uma regra simples: "antes de qualquer transferência fora do comum, ligue para mim".
- Configure limites baixos de Pix no aplicativo do banco.
- Peça ao banco o bloqueio de novos empréstimos consignados, quando disponível.
- Salve na agenda os números oficiais do banco e do INSS.
- Ensine o método PARE e a palavra-código da família.
- Mantenha contato frequente. Solidão é uma porta de entrada para golpistas.

## Na prática

- ☐ Desconfie de quem declara amor rápido e nunca aparece em videochamada.
- ☐ Faça busca reversa das fotos de perfis suspeitos.
- ☐ Nunca envie dinheiro para alguém que você não conheceu pessoalmente.
- ☐ Converse com os idosos da família sobre os golpes mais comuns, sem julgamento.
- ☐ Configure limites de Pix e verifique a possibilidade de bloquear consignados não solicitados.
- ☐ Lembre que o INSS e os bancos não ligam pedindo dados, pagamentos ou transferências.

## Capítulo 9: Vazamento de dados e uso do seu nome

Nem todo golpe tira dinheiro da sua conta. Alguns usam o seu nome para tirar dinheiro de outras pessoas ou de empresas. O golpista abre contas, faz compras, pega empréstimos e contrata serviços como se fosse você. Quem fica com a dívida e a dor de cabeça é a vítima.

Esse tipo de golpe é silencioso. Muitas pessoas só descobrem meses depois, quando recebem uma cobrança, têm o nome negativado ou têm um crédito negado.

### A história de Patrícia

*Caso ilustrativo.* Patrícia, 41 anos, tentou financiar um carro e teve o crédito negado. Ao consultar seu CPF, descobriu três contas em bancos digitais que ela nunca abriu, um empréstimo de R\$ 8.000 e duas linhas de celular em seu nome.

Um ano antes, ela havia enviado foto do documento e uma selfie para um suposto processo de emprego pelo WhatsApp. A vaga não existia. Os golpistas usaram os documentos para se passar por ela.

Patrícia levou meses para limpar o nome. Não perdeu dinheiro diretamente, mas perdeu tempo, tranquilidade e oportunidades.

### O que é vazamento de dados

Vazamento de dados acontece quando informações pessoais saem do controle de quem deveria protegê-las. Isso pode ocorrer porque uma empresa foi invadida, porque um funcionário vendeu informações ou porque a própria pessoa entregou os dados em um site falso.

No Brasil, a Lei Geral de Proteção de Dados, a LGPD, obriga empresas a proteger seus dados e a comunicar incidentes graves. Mesmo assim, vazamentos continuam acontecendo, e muitas bases de dados circulam livremente entre criminosos.

## Quais dados valem ouro para o golpista

| Dado                             | Para que o golpista usa                                                     |
|----------------------------------|-----------------------------------------------------------------------------|
| Nome completo e CPF              | Criar cadastros, ligar se passando por empresas, dar credibilidade ao golpe |
| Data de nascimento e nome da mãe | Responder perguntas de segurança em atendimentos                            |
| Endereço e telefone              | Golpes por ligação, por correspondência e entregas falsas                   |
| Foto de documento                | Abrir contas e fazer cadastros em seu nome                                  |
| Selfie segurando documento       | Burlar verificações de identidade de bancos e aplicativos                   |
| Dados do cartão                  | Fazer compras online                                                        |
| Senhas                           | Acessar e-mails, redes sociais e outras contas                              |

Repare que a **selfie com documento** é um dos dados mais valiosos. Ela é usada justamente para provar que "você é você". Nunca envie esse tipo de imagem fora dos aplicativos oficiais das instituições.

## Golpes que usam seu nome

- **Abertura de contas:** usadas para receber dinheiro de outros golpes, o que pode colocar você sob suspeita.
- **Empréstimos e crediários:** dívidas contratadas em seu nome.
- **Linhas de celular:** usadas para aplicar golpes e clonar contas.
- **Compras parceladas:** carnês e boletos em lojas.
- **Abertura de empresas:** CNPJs registrados em seu nome para fraudes fiscais.
- **Chaves Pix:** cadastradas em contas que você não controla.

## Como descobrir se estão usando seu nome

Existem ferramentas oficiais e gratuitas que todo brasileiro deveria conhecer:

| Ferramenta                   | O que mostra                                                                      |
|------------------------------|-----------------------------------------------------------------------------------|
| Registrato, do Banco Central | Contas bancárias, chaves Pix, empréstimos e financiamentos registrados no seu CPF |

| Ferramenta                                     | O que mostra                                                                        |
|------------------------------------------------|-------------------------------------------------------------------------------------|
| Gov.br                                         | Acesso a serviços públicos e a consultas sobre sua situação junto a órgãos federais |
| Birôs de crédito, como Serasa, SPC e Boa Vista | Dívidas, consultas ao seu CPF e alertas de uso do documento                         |
| Consulta de linhas telefônicas                 | Muitas operadoras e a Anatel oferecem formas de verificar linhas em seu nome        |

O **Registrato** merece destaque. Ele é gratuito, oficial e mostra, em um só lugar, os relacionamentos que você tem com instituições financeiras. Vale consultar pelo menos duas vezes por ano.

### Como diminuir a exposição dos seus dados

- Não envie fotos de documentos e selfies por WhatsApp ou e-mail para desconhecidos.
- Desconfie de formulários que pedem muitos dados em troca de prêmios ou vagas.
- Não publique fotos de documentos, cartões de embarque ou comprovantes nas redes sociais.
- Ao jogar papéis fora, rasgue documentos, faturas e cartas com dados pessoais.
- Use senhas diferentes para cada serviço importante.
- Ative a verificação em duas etapas no e-mail, que é a chave para recuperar quase todas as suas contas.

### Senhas vazadas

Quando uma empresa sofre vazamento, sua senha daquele serviço pode cair nas mãos de criminosos. Se você usa a mesma senha em vários lugares, todos ficam vulneráveis.

Existem sites reconhecidos internacionalmente que permitem verificar se seu e-mail apareceu em vazamentos conhecidos. Se aparecer, troque as senhas imediatamente, começando pelo e-mail e pelos bancos.

### O que fazer se usarem seu nome

1. **Registre um boletim de ocorrência**, descrevendo o uso indevido dos seus dados.
2. **Entre em contato com cada empresa** onde a conta, compra ou empréstimo foi feito, informe a fraude e peça o cancelamento, anexando o boletim.
3. **Conteste negativas indevidas** nos birôs de crédito.
4. **Consulte o Registrato** e peça o encerramento de contas que você não abriu.
5. **Guarde todos os protocolos**, e-mails e documentos.

**6. Procure o Procon ou a Justiça** se as empresas não resolverem. Empresas respondem por falhas na verificação de identidade.

## Na prática

- ☐ Consulte o Registrato do Banco Central ainda este mês.
- ☐ Ative alertas de uso do CPF em um birô de crédito, quando disponível.
- ☐ Nunca envie selfie com documento fora dos aplicativos oficiais.
- ☐ Use senhas diferentes para e-mail, bancos e redes sociais.
- ☐ Ative a verificação em duas etapas no seu e-mail principal.
- ☐ Se descobrir uso do seu nome, registre boletim de ocorrência e guarde todos os protocolos.

## Capítulo 10: Blindando sua vida digital

Até aqui, você aprendeu a reconhecer os golpes. Agora é hora de fechar as portas. Este capítulo reúne as medidas práticas que tornam sua vida digital muito mais segura, mesmo que você não entenda nada de tecnologia.

A boa notícia: a maioria dessas medidas leva poucos minutos e só precisa ser feita uma vez.

### A história de Renata

*Caso ilustrativo.* Renata, 45 anos, recebeu um e-mail dizendo que sua conta de e-mail seria desativada por falta de espaço. Clicou no link e digitou a senha. Pronto: o golpista entrou no e-mail dela.

A partir do e-mail, ele pediu a troca de senha das redes sociais, do aplicativo de compras e até de uma conta de investimentos. Em um único dia, Renata perdeu o controle de quase toda a sua vida digital.

Se ela tivesse ativado a verificação em duas etapas no e-mail, o golpista teria a senha, mas não conseguiria entrar. Uma configuração de dois minutos teria evitado todo o problema.

### As cinco camadas de proteção

Pense na sua segurança digital como uma casa com várias camadas de proteção. Se uma falhar, as outras seguram.

| Camada     | O que protege               | Medida principal                |
|------------|-----------------------------|---------------------------------|
| 1. Celular | Tudo o que está no aparelho | Bloqueio de tela e atualizações |

| Camada             | O que protege                                 | Medida principal                          |
|--------------------|-----------------------------------------------|-------------------------------------------|
| 2. E-mail          | A chave para recuperar todas as outras contas | Senha forte e verificação em duas etapas  |
| 3. Contas e senhas | Bancos, redes sociais, lojas                  | Senhas diferentes e gerenciador de senhas |
| 4. Aplicativos     | O que roda no seu celular                     | Baixar só das lojas oficiais              |
| 5. Comportamento   | Você                                          | Método PARE e confirmação por outro canal |

## Camada 1: o celular

Seu celular guarda banco, conversas, fotos e senhas. Proteja-o como protege sua carteira.

- **Use bloqueio de tela** com senha, biometria ou reconhecimento facial. Evite padrões simples como 1234 ou datas de nascimento.
- **Mantenha o sistema atualizado.** As atualizações corrigem falhas de segurança.
- **Ative a localização e o bloqueio remoto** do aparelho, disponíveis nos sistemas Android e iPhone, para apagar os dados se ele for roubado.
- **Coloque senha no chip** (PIN do SIM). Isso impede que um ladrão use seu chip em outro aparelho para receber códigos por SMS.
- **Não deixe senhas de bancos anotadas** em blocos de notas ou fotos no celular.

## Camada 2: o e-mail

O e-mail é a conta mais importante que você tem, porque é por ele que se recuperam quase todas as outras senhas. Se o golpista controla seu e-mail, controla sua vida digital.

- Use uma senha longa e única, que você não usa em nenhum outro lugar.
- Ative a verificação em duas etapas.
- Cadastre um telefone e um e-mail de recuperação atualizados.
- Desconfie de mensagens dizendo que sua conta será bloqueada ou desativada.

## Camada 3: senhas fortes e diferentes

O maior erro em segurança digital é usar a mesma senha em todos os lugares. Quando um site vaza, todas as suas contas ficam expostas.

| Senha fraca               | Por quê                                 | Alternativa forte                           |
|---------------------------|-----------------------------------------|---------------------------------------------|
| 123456                    | Uma das mais usadas do mundo            | Frase longa com palavras aleatórias         |
| Nome + data de nascimento | Fácil de descobrir pelas redes sociais  | Combinação sem relação com sua vida pública |
| Mesma senha em tudo       | Um vazamento compromete todas as contas | Uma senha diferente para cada serviço       |

Uma técnica fácil é usar **frases-senha**: quatro ou cinco palavras sem relação entre si, como "cadeira laranja voa lentamente". São fáceis de lembrar e difíceis de adivinhar.

Como é impossível decorar dezenas de senhas diferentes, vale usar um **gerenciador de senhas**, um aplicativo que guarda todas elas protegidas por uma senha principal. Os próprios sistemas Android e iPhone já oferecem gerenciadores gratuitos.

## A verificação em duas etapas

A verificação em duas etapas exige, além da senha, uma segunda confirmação: um código no celular, uma notificação no aplicativo ou a sua biometria. Mesmo que alguém descubra sua senha, não consegue entrar.

Ative essa proteção, nesta ordem de prioridade:

1. E-mail principal.
2. WhatsApp.
3. Aplicativos de banco e investimento, quando oferecerem.
4. Redes sociais.
5. Lojas online com cartão salvo.

Lembre: o código da verificação em duas etapas é **só seu**. Se alguém pedir esse código, por qualquer motivo, é golpe.

## Camada 4: aplicativos

- Baixe aplicativos apenas da Google Play ou da App Store.
- Nunca instale aplicativos a pedido de alguém que ligou para você.
- Desconfie de aplicativos que pedem permissões exageradas, como uma lanterna que quer acessar seus contatos.
- Revise de tempos em tempos os aplicativos instalados e apague os que não usa.

- Negue permissões de "acessibilidade" e "compartilhamento de tela" para aplicativos desconhecidos.

## Camada 5: comportamento

A tecnologia ajuda, mas a última camada é você. Revise os hábitos que aprendeu nos capítulos anteriores:

| Hábito                            | Por que importa                                             |
|-----------------------------------|-------------------------------------------------------------|
| Aplicar o método PARE             | Quebra a pressa e a emoção que o golpe precisa              |
| Confirmar por outro canal         | Desmonta golpes de falso parente, falso banco e falso chefe |
| Não clicar em links recebidos     | Evita sites falsos e roubo de senhas                        |
| Desconfiar de ofertas boas demais | Protege contra lojas falsas e investimentos fraudulentos    |
| Conversar antes de transferir     | Traz outra cabeça para avaliar a situação                   |

## Redes Wi-Fi públicas

Redes Wi-Fi de aeroportos, cafés e shoppings são práticas, mas nem sempre seguras. Evite acessar bancos ou fazer compras nessas redes. Se precisar, prefira usar os dados móveis do seu celular.

## Na prática: checklist de 30 minutos

Reserve meia hora e faça tudo isto de uma vez:

- ☐ Ative o bloqueio de tela do celular com senha forte ou biometria.
- ☐ Atualize o sistema e os aplicativos do celular.
- ☐ Ative a localização e o bloqueio remoto do aparelho.
- ☐ Coloque PIN no chip do celular.
- ☐ Troque a senha do e-mail principal por uma frase-senha única.
- ☐ Ative a verificação em duas etapas no e-mail e no WhatsApp.
- ☐ Ative um gerenciador de senhas e comece pelas contas mais importantes.
- ☐ Apague aplicativos que você não usa mais.

## Capítulo 11: Protegendo a família

Você pode estar muito bem protegido e, ainda assim, ver alguém que você ama cair em um golpe. Pais, avós, filhos adolescentes, tios e sogros são alvos diários. Por isso, segurança digital é um assunto de família.

Este capítulo mostra como transformar o que você aprendeu em um plano simples, que toda a família consegue seguir.

### A história da família Souza

*Caso ilustrativo.* Depois que a avó perdeu R\$ 3.000 no golpe do falso neto, a família Souza resolveu fazer uma reunião em um almoço de domingo. Sem broncas, cada um contou um golpe que já tinha recebido. O neto adolescente contou do falso sorteio no jogo online. A tia, da loja falsa. O pai, da falsa central do banco.

No fim, combinaram três regras: uma palavra-código, uma ligação antes de qualquer transferência fora do comum e um grupo da família para avisar sobre golpes novos.

Três meses depois, a avó recebeu um áudio com a voz do neto pedindo dinheiro. Ela pediu a palavra-código. Do outro lado, silêncio. Depois, o número bloqueou ela. A família tinha vencido o golpe.

### O plano familiar antigolpe

Um bom plano familiar tem cinco partes:

| Parte                   | O que é                                                  | Como fazer                                     |
|-------------------------|----------------------------------------------------------|------------------------------------------------|
| 1. Palavra-código       | Senha verbal para confirmar pedidos de dinheiro          | Combinar pessoalmente e trocar se vazar        |
| 2. Regra da ligação     | Ninguém transfere dinheiro fora do comum sem ligar antes | Vale para todos, inclusive os mais jovens      |
| 3. Contatos oficiais    | Números do banco, do INSS e de emergência salvos         | Salvar na agenda de cada celular               |
| 4. Grupo de alerta      | Canal para avisar sobre golpes que estão circulando      | Grupo de mensagens só da família               |
| 5. Pessoa de referência | Alguém de confiança para tirar dúvidas                   | Um filho, neto ou amigo que entende do assunto |

## Como criar a palavra-código

A palavra-código é a defesa mais eficaz contra os golpes do falso parente e da voz clonada. Siga este modelo:

### Modelo de combinação familiar

1. Reúna a família pessoalmente ou em uma ligação de vídeo que você mesmo iniciou.
2. Escolham juntos uma palavra ou frase inusitada, sem relação com informações públicas.
3. Combinem a regra: "Sempre que alguém pedir dinheiro de forma urgente, por mensagem, áudio, ligação ou vídeo, quem recebe pede a palavra-código".
4. Combinem também que ninguém se ofende ao ser questionado.
5. Não escrevam a palavra em mensagens, redes sociais ou notas no celular.
6. Troquem a palavra uma vez por ano ou sempre que houver suspeita de que vazou.

Uma variação útil é a **pergunta-código**: uma pergunta cuja resposta só a família sabe, como "qual era o nome do cachorro do vizinho na casa antiga?".

## Conversando com idosos

Os idosos merecem atenção especial, como vimos no Capítulo 8. Algumas dicas ajudam a conversa:

- Use exemplos reais e recentes, que eles reconheçam.
- Mostre mensagens de golpe verdadeiras e explique onde está o truque.
- Repita as regras com carinho. Uma conversa só não basta.
- Configure o celular junto com eles, sem tirar a autonomia.
- Deixe claro que podem ligar a qualquer hora, sem medo de incomodar.

Uma ideia prática é colar um cartão perto do telefone ou na capa do celular com as regras principais e os números oficiais.

### Modelo de cartão de bolso

|                                                       |
|-------------------------------------------------------|
| Antes de transferir dinheiro, lembre                  |
| Banco não pede senha, código, transferência ou cartão |
| INSS não liga pedindo pagamento                       |
| Pedido de dinheiro urgente? Peça a palavra-código     |

|                                                                  |
|------------------------------------------------------------------|
| Antes de transferir dinheiro, lembre                             |
| Na dúvida, ligue para: (nome e telefone da pessoa de referência) |
| Banco: (número oficial)                                          |

## Conversando com crianças e adolescentes

Crianças e adolescentes passam muito tempo online e também são alvos. Os golpes mais comuns para essa faixa etária incluem:

| Golpe                   | Como funciona                                                       |
|-------------------------|---------------------------------------------------------------------|
| Itens grátis em jogos   | Promessa de moedas, skins ou prêmios em troca de login e senha      |
| Falso influenciador     | Perfil que oferece sorteios ou parcerias e pede dados ou dinheiro   |
| Compras não autorizadas | Uso do cartão dos pais salvo em lojas de aplicativos e jogos        |
| Chantagem com fotos     | Criminosos conquistam a confiança e depois ameaçam divulgar imagens |

Algumas medidas ajudam:

- Ative o controle parental nos celulares, consoles e lojas de aplicativos.
- Exija senha ou aprovação para compras dentro de jogos e aplicativos.
- Ensine que senhas não se compartilham, nem com amigos.
- Converse sobre os perigos de enviar fotos e informações pessoais para desconhecidos.
- Deixe claro que eles podem contar qualquer coisa estranha sem medo de castigo.

Este último ponto é fundamental. Criminosos que chantageiam jovens contam com o medo de os pais descobrirem. Uma criança que sabe que pode falar com os pais está muito mais protegida.

## O grupo de alerta da família

Criar um grupo de mensagens só para a família trocar alertas sobre golpes funciona muito bem. Sempre que alguém receber uma mensagem suspeita, compartilha um print com o aviso "golpe circulando". Isso transforma cada tentativa de golpe em aprendizado para

todos.

Só tome um cuidado: nunca clique nos links compartilhados nesses prints.

## Na prática

- ☐ Marque uma conversa com a família ainda este mês para falar sobre golpes.
- ☐ Combine pessoalmente uma palavra-código ou pergunta-código.
- ☐ Combine a regra da ligação antes de transferências fora do comum.
- ☐ Salve os números oficiais do banco e do INSS no celular dos familiares.
- ☐ Prepare o cartão de bolso para os idosos da família.
- ☐ Ative o controle parental nos aparelhos das crianças.
- ☐ Crie um grupo de alerta familiar sobre golpes.

## Capítulo 12: Pequenos negócios na mira

Muita gente acha que golpistas só miram grandes empresas. É o contrário. Pequenos negócios são alvos preferidos porque movimentam dinheiro todos os dias, mas raramente têm equipe de tecnologia, processos formais ou alguém dedicado à segurança.

Um único golpe pode comprometer o caixa do mês, ou até a sobrevivência do negócio.

### A história da Padaria Bom Dia

*Caso ilustrativo.* A Padaria Bom Dia compra farinha do mesmo fornecedor há oito anos. Um dia, a dona, Cláudia, recebeu um e-mail do fornecedor informando que a empresa havia mudado de banco e enviando um boleto com os novos dados. O e-mail tinha a logomarca, a assinatura e o tom de sempre.

Cláudia pagou R\$ 12.400. Semanas depois, o fornecedor cobrou a fatura em atraso. O e-mail tinha vindo de um endereço quase igual ao verdadeiro, com uma letra diferente. O boleto direcionava o dinheiro para a conta de um golpista.

Esse é o golpe da **troca de dados bancários do fornecedor**, um dos mais comuns contra empresas de todos os tamanhos.

### Os golpes mais comuns contra pequenos negócios

| Golpe                        | Como funciona                                                  | Quem costuma ser alvo              |
|------------------------------|----------------------------------------------------------------|------------------------------------|
| Troca de dados do fornecedor | E-mail ou mensagem informa nova conta bancária para pagamentos | Quem faz pagamentos a fornecedores |

| Golpe                           | Como funciona                                               | Quem costuma ser alvo                    |
|---------------------------------|-------------------------------------------------------------|------------------------------------------|
| Falso dono ou diretor           | Mensagem do "chefe" pede pagamento urgente e confidencial   | Funcionários do financeiro               |
| Boleto adulterado               | Boleto verdadeiro alterado para cair na conta do golpista   | Contas a pagar                           |
| Falso cliente                   | Compra com comprovante falso ou cartão clonado              | Lojas, especialmente online e delivery   |
| Ransomware                      | Programa malicioso que bloqueia computadores e pede resgate | Empresas com computadores desatualizados |
| Falsa cobrança de órgão público | Cobrança de taxas, multas ou registros que não existem      | Empresas recém-abertas e MEIs            |
| Falso suporte técnico           | Ligação oferecendo ajuda com sistema ou maquininha          | Lojas com maquininha de cartão           |
| Invasão de redes sociais        | Golpista assume o perfil da loja e engana clientes          | Negócios que vendem pelo Instagram       |

## O golpe contra empresas recém-abertas

Quem abre um CNPJ ou MEI costuma receber, nas semanas seguintes, uma enxurrada de boletos e cartas com aparência oficial: "taxa de registro", "cadastro nacional de empresas", "anuidade obrigatória". Muitos desses documentos são enviados por empresas privadas que se aproveitam da confusão, ou por golpistas.

Antes de pagar qualquer cobrança desse tipo, confirme no portal oficial do governo ou com o seu contador se ela realmente existe.

## Regras de ouro para pagamentos

A maior parte dos prejuízos em pequenos negócios acontece na hora de pagar. Algumas regras simples resolvem muito:

1. **Nunca altere dados bancários de fornecedor só por e-mail ou mensagem.** Confirme por telefone, usando um número que você já tinha.
2. **Desconfie de pedidos urgentes e confidenciais,** mesmo que pareçam vir do dono.
3. **Confira o nome do beneficiário** no boleto e na tela do Pix antes de pagar.
4. **Separe funções:** quem cadastra o pagamento não deve ser a mesma pessoa que aprova.
5. **Defina limites:** pagamentos acima de um valor exigem a aprovação de duas pessoas.

## 6. Mantenha uma lista oficial de fornecedores com seus dados bancários confirmados.

### Protegendo os computadores e sistemas

O ransomware, aquele programa que sequestra os arquivos e pede resgate, também atinge pequenos negócios. Muitos não têm cópia de segurança dos dados e ficam sem saída.

| Medida                              | Por que é importante                             |
|-------------------------------------|--------------------------------------------------|
| Backup regular                      | Permite recuperar dados sem pagar resgate        |
| Backup fora do computador principal | Impede que o ataque destrua também a cópia       |
| Sistemas e antivírus atualizados    | Fecham falhas exploradas por ataques             |
| Senhas fortes e diferentes          | Evitam invasão de contas da empresa              |
| Verificação em duas etapas          | Protege e-mail, banco e redes sociais da empresa |
| Contas separadas por funcionário    | Permitem controlar e retirar acessos             |

Uma regra prática para backups é a **3-2-1**: ter três cópias dos dados importantes, em dois tipos de armazenamento diferentes, com uma delas fora da empresa ou na nuvem. Teste a restauração de vez em quando para ter certeza de que funciona.

### Treinando a equipe

Funcionários são a primeira linha de defesa. Não é preciso um treinamento caro. Bastam conversas curtas e frequentes:

- Mostre exemplos de golpes reais recebidos pela empresa.
- Crie uma regra clara: na dúvida, ninguém paga, ninguém clica, ninguém informa dados.
- Deixe claro que questionar um pedido do chefe nunca será motivo de bronca.
- Reconheça quem identificar e reportar uma tentativa de golpe.

### Protegendo a reputação do negócio

Golpistas também usam o nome de negócios honestos para enganar clientes. Criam perfis falsos da loja ou invadem o perfil verdadeiro. Para se proteger:

- Ative a verificação em duas etapas nas redes sociais da empresa.
- Informe aos clientes quais são os canais oficiais de venda e pagamento.
- Avise publicamente quando identificar perfis falsos.
- Prefira formas de pagamento rastreáveis e em nome da empresa.

## LGPD também vale para você

Se o seu negócio guarda dados de clientes, como nome, telefone, endereço ou CPF, ele também precisa cumprir a LGPD. Isso significa coletar apenas o necessário, proteger essas informações e não compartilhá-las sem motivo. Além de evitar problemas legais, isso aumenta a confiança dos clientes.

### Na prática

- ☐ Confirme por telefone qualquer mudança de dados bancários de fornecedores.
- ☐ Exija aprovação de duas pessoas para pagamentos acima de um valor definido.
- ☐ Faça backup dos dados importantes, com uma cópia fora do computador principal.
- ☐ Ative a verificação em duas etapas no e-mail, banco e redes sociais da empresa.
- ☐ Combine com a equipe: na dúvida, ninguém paga e ninguém clica.
- ☐ Confirme com o contador antes de pagar cobranças de registros e taxas desconhecidas.
- ☐ Divulgue aos clientes seus canais oficiais de venda e pagamento.

## Capítulo 13: Caí no golpe, e agora?

Se você chegou a este capítulo porque acabou de cair em um golpe, respire. Você não está sozinho, e há coisas importantes que podem ser feitas agora. Quanto mais rápido você agir, maiores as chances de reduzir o prejuízo.

E lembre do que dissemos no início do livro: cair em um golpe não é sinal de burrice. Você foi vítima de criminosos profissionais.

### A história de Eduardo

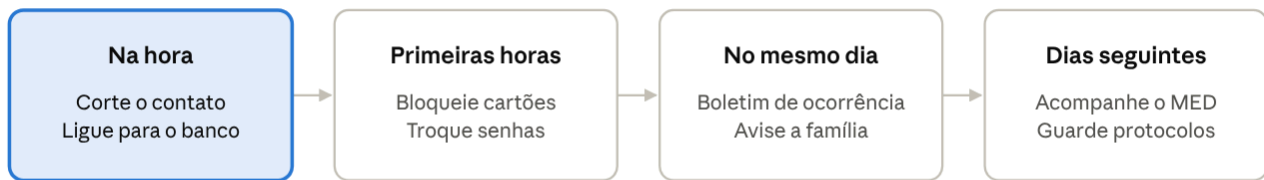
*Caso ilustrativo.* Eduardo, 36 anos, fez um Pix de R\$ 2.700 para uma loja falsa às 14h. Às 14h40, desconfiado porque o site havia saído do ar, ligou para o banco pelo número oficial e informou a fraude. O banco registrou o pedido de devolução e bloqueou a parte do dinheiro que ainda estava na conta de destino.

Ele também registrou um boletim de ocorrência pela internet no mesmo dia. Dias depois, recebeu de volta parte do valor. Não recuperou tudo, mas recuperou muito mais do que se tivesse esperado.

**A lição: a velocidade da reação faz diferença.**

## As primeiras horas: o que fazer, em ordem

Quanto antes você reage, maior a chance de recuperar o dinheiro



Reação ao golpe · 4 momentos

A tabela abaixo detalha cada passo e explica por que ele importa.

| Quando              | O que fazer                                                   | Por quê                                                                 |
|---------------------|---------------------------------------------------------------|-------------------------------------------------------------------------|
| Imediatamente       | Pare de falar com o golpista e não faça novas transferências  | Golpistas costumam voltar com novas cobranças, como "taxa de devolução" |
| Imediatamente       | Ligue para o seu banco pelo número oficial e informe a fraude | O banco pode bloquear valores e iniciar a devolução                     |
| Nas primeiras horas | Bloqueie cartões e troque senhas comprometidas                | Impede novos prejuízos                                                  |
| No mesmo dia        | Registre um boletim de ocorrência                             | É exigido em muitos processos e ajuda as investigações                  |
| No mesmo dia        | Avise familiares e contatos                                   | O golpista pode tentar enganar outras pessoas usando seu nome           |
| Nos dias seguintes  | Acompanhe o pedido no banco e guarde todos os protocolos      | Ajuda a cobrar uma resposta e a recorrer, se necessário                 |

## O MED: o mecanismo de devolução do Pix

O Banco Central criou o **Mecanismo Especial de Devolução**, conhecido como **MED**, para casos de golpe e fraude com Pix.

Funciona assim:

1. Você informa ao seu banco que fez um Pix por causa de um golpe.
2. Seu banco comunica o banco que recebeu o dinheiro.
3. O banco recebedor pode bloquear o valor que ainda estiver na conta do golpista.

4. Os dois bancos analisam o caso.

5. Se a fraude for confirmada, o dinheiro disponível é devolvido para você.

Alguns pontos importantes:

- O pedido deve ser feito **o mais rápido possível**. O prazo máximo é de 80 dias após o Pix, mas quanto antes, maior a chance de o dinheiro ainda estar na conta.
- O MED só devolve o que ainda estiver na conta do golpista. Se o dinheiro já foi transferido para outras contas, a devolução pode ser parcial ou não acontecer.
- O Banco Central vem aprimorando o mecanismo, inclusive com a possibilidade de contestar pelo próprio aplicativo do banco. Consulte as opções disponíveis no seu banco.
- O MED é para golpes e fraudes. Ele não serve para desacordos comerciais comuns, como um produto que chegou diferente do anunciado por uma loja real.

## Golpes com cartão

Se o golpe envolveu cartão de crédito ou débito:

- Bloqueie o cartão imediatamente pelo aplicativo ou pela central oficial.
- Conte as compras que você não reconhece.
- Peça um novo cartão.
- Verifique se há outras compras ou parcelamentos que você não fez.

Em compras com cartão de crédito, o processo de contestação costuma ser mais simples e as chances de recuperar o valor tendem a ser maiores do que no Pix.

## Golpes com boleto

Se você pagou um boleto falso:

- Avise imediatamente o seu banco e o banco emissor do boleto, que aparece no início do código de barras.
- Guarde o boleto, o comprovante de pagamento e as mensagens recebidas.
- Registre o boletim de ocorrência.
- Se o boleto foi enviado por uma empresa que teve o sistema invadido, informe a empresa. Ela pode ter responsabilidade.

## Contas invadidas

Se o golpista invadiu seu WhatsApp, e-mail ou redes sociais:

1. Tente recuperar a conta pelos canais oficiais do serviço.
2. Troque a senha e ative a verificação em duas etapas.

3. Avise seus contatos por outros meios que sua conta foi invadida.
4. Verifique se outras contas usam a mesma senha e troque todas.
5. Revise os dispositivos conectados à conta e desconecte os que não reconhecer.

## Como registrar o boletim de ocorrência

Na maioria dos estados, é possível registrar o boletim de ocorrência pela internet, na delegacia virtual da Polícia Civil. Reúna antes:

| Informação         | Exemplos                                                   |
|--------------------|------------------------------------------------------------|
| Dados da transação | Data, hora, valor, chave Pix, nome e banco do destinatário |
| Comprovantes       | Prints do comprovante de pagamento                         |
| Conversas          | Prints das mensagens, e-mails, perfis e números usados     |
| Sites e links      | Endereço do site falso, anúncio ou perfil                  |
| Descrição          | Um relato simples, em ordem, do que aconteceu              |

O boletim é importante para pedidos ao banco, contestações, ações judiciais e para que a polícia identifique padrões e quadrilhas.

## Se o banco não resolver

Se o banco negar o pedido ou não responder, você pode:

1. Registrar reclamação na **ouvidoria** do banco.
2. Registrar reclamação no **Banco Central**, pelo canal oficial de reclamações.
3. Registrar reclamação no **Procon** ou na plataforma **consumidor.gov.br**.
4. Buscar orientação jurídica. Em alguns casos, especialmente quando houve falha de segurança do banco, a Justiça tem reconhecido o direito à indenização.

## Cuidado com o golpe da recuperação

Depois de um golpe, muitas vítimas recebem contatos de pessoas que prometem recuperar o dinheiro: falsos advogados, falsos policiais, falsos funcionários do banco ou "especialistas em rastreamento". Eles cobram uma taxa antecipada e desaparecem.

Ninguém sério cobra antecipadamente para "rastrear" ou "recuperar" dinheiro de golpe por mensagem. Trate esse contato como um novo golpe.

## Cuide também de você

Cair em um golpe mexe com a autoestima, a confiança e o sono. Muitas pessoas sentem vergonha e se isolam. Conversar com a família, com amigos ou com um profissional ajuda a atravessar esse momento.

Compartilhar o que aconteceu também protege outras pessoas. Cada história contada é um golpe a menos no futuro.

## Na prática: guarde este roteiro

- ☐ Pare de falar com o golpista e não faça novas transferências.
- ☐ Ligue imediatamente para o banco pelo número oficial e peça o MED.
- ☐ Bloqueie cartões e troque senhas.
- ☐ Registre o boletim de ocorrência no mesmo dia.
- ☐ Avise familiares e contatos.
- ☐ Guarde todos os comprovantes, prints e protocolos.
- ☐ Se o banco não resolver, recorra à ouvidoria, ao Banco Central e ao Procon.
- ☐ Desconfie de qualquer pessoa que prometa recuperar o dinheiro mediante pagamento.

## Conclusão: os 10 mandamentos antigolpe

Chegamos ao fim deste guia. Você agora conhece como os golpistas pensam, como se organizam, quais truques usam e, principalmente, como se proteger.

Os golpes vão continuar mudando. Amanhã surgirá uma nova história, um novo aplicativo, uma nova tecnologia. Mas os princípios que você aprendeu continuam valendo, porque os golpistas sempre vão precisar das mesmas coisas: **pressa, emoção e isolamento**.

Para facilitar, reunimos tudo em dez mandamentos. Imprima, cole na geladeira, compartilhe com a família.

## Os 10 mandamentos antigolpe

1. **Pressa e segredo são sinais de golpe.** Sempre que alguém pedir urgência e sigilo envolvendo dinheiro, pare.
2. **Confirme sempre por outro canal.** Desligue e ligue você mesmo para o número que já conhece.
3. **Banco não pede senha, código, transferência nem cartão.** Nunca, em nenhuma situação.
4. **Códigos recebidos no celular são só seus.** Não informe para ninguém, por nenhum motivo.

5. **Confira o nome antes de confirmar o Pix.** Se o nome não bate, cancele.
6. **Desconfie do que é bom demais.** Preço muito baixo, ganho muito alto e amor muito rápido merecem desconfiança.
7. **Ver e ouvir não é mais prova.** Voz e vídeo podem ser falsos. Use a palavra-código da família.
8. **Nunca pague para trabalhar ou para receber um prêmio.** Quem paga é quem contrata ou quem premia.
9. **Ative a verificação em duas etapas.** No e-mail, no WhatsApp e nas contas importantes.
10. **Caiu? Aja rápido e sem vergonha.** Ligue para o banco, registre o boletim e avise a família.

## Checklist geral de proteção

Use esta lista para conferir se você já colocou em prática o que aprendeu:

### Celular e contas

- ☐ Bloqueio de tela com senha forte ou biometria.
- ☐ Sistema e aplicativos atualizados.
- ☐ PIN no chip do celular.
- ☐ Verificação em duas etapas no e-mail e no WhatsApp.
- ☐ Senhas diferentes para os serviços importantes.

### Banco e pagamentos

- ☐ Número oficial do banco salvo na agenda.
- ☐ Limites de Pix ajustados para o seu uso real.
- ☐ Notificações de transações ativadas.
- ☐ Cartão virtual para compras online.

### Família

- ☐ Palavra-código combinada pessoalmente.
- ☐ Regra da ligação antes de transferências fora do comum.
- ☐ Cartão de bolso para os idosos.
- ☐ Controle parental nos aparelhos das crianças.

### Dados pessoais

- ☐ Registrato consultado nos últimos seis meses.
- ☐ Nenhuma foto de documento ou selfie enviada a desconhecidos.
- ☐ Perfis de redes sociais com privacidade revisada.

## Negócio (se tiver)

- ☐ Confirmação por telefone para mudança de dados de fornecedores.
- ☐ Aprovação dupla para pagamentos altos.
- ☐ Backup atualizado e testado.

## Contatos e canais úteis

| Canal                                            | Para que serve                                          |
|--------------------------------------------------|---------------------------------------------------------|
| Central oficial do seu banco                     | Informar fraudes, bloquear cartões e pedir o MED do Pix |
| Registrato, do Banco Central                     | Consultar contas, chaves Pix e empréstimos em seu nome  |
| Canal de reclamações do Banco Central            | Reclamar de bancos que não resolveram seu problema      |
| Delegacia virtual da Polícia Civil do seu estado | Registrar boletim de ocorrência pela internet           |
| Polícia Militar: 190                             | Emergências, como ameaças ou extorsão em andamento      |
| Meu INSS (aplicativo e site) e telefone 135      | Serviços e informações oficiais do INSS                 |
| Procon do seu estado e consumidor.gov.br         | Reclamações contra empresas                             |
| CVM                                              | Verificar se empresas podem oferecer investimentos      |
| Birôs de crédito, como Serasa, SPC e Boa Vista   | Consultar dívidas e uso do seu CPF                      |

Anote aqui os seus contatos importantes:

| Contato                         | Telefone |
|---------------------------------|----------|
| Central do meu banco            |          |
| Pessoa de referência da família |          |
| Outro contato de confiança      |          |

## Uma palavra final

Golpistas contam com o silêncio. Contam com a vergonha de quem caiu, com a pressa de quem está ocupado e com a solidão de quem não tem com quem conversar.

A melhor resposta é o contrário disso: conversar, compartilhar, perguntar e ajudar. Cada pessoa que aprende a reconhecer um golpe protege não só a si mesma, mas também a família, os amigos e a comunidade.

Agora que você chegou até aqui, passe adiante. Converse com seus pais, seus filhos, seus colegas de trabalho. Conte o que aprendeu.

**Não caia nessa. E não deixe ninguém que você ama cair também.**

# PRESSA E SEGREDO SÃO AS DUAS MARCAS DO GOLPE.

Uma mensagem do seu filho pedindo um Pix. Uma ligação do banco avisando de uma compra suspeita. Um vídeo de um famoso indicando um investimento imperdível. Tudo parece real. E é exatamente assim que os golpes digitais funcionam hoje.

Com linguagem simples e exemplos do dia a dia, este livro mostra como os golpistas pensam, quais truques usam e o que fazer para proteger você, sua família e seu negócio.

## NESTE LIVRO, VOCÊ VAI APRENDER A

- Reconhecer os golpes mais comuns de WhatsApp, Pix e compras online
- Identificar vozes e vídeos falsos criados com inteligência artificial
- Criar uma palavra-código para proteger a família
- Agir rápido nas primeiras horas depois de um golpe

**FELIPE PINTO GOMES**

[Mini biografia do autor: experiência em segurança digital e gestão de riscos de TI.]

Área reservada para o código de barras