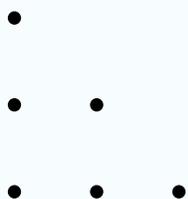


# Fique atento e proteja-se dos golpes financeiros



• • • • • • • •  
• • • • • • • •

**Entre janeiro e setembro de 2024, mais de 70 mil casos de violação patrimonial mediante golpes digitais e presenciais foram denunciados por meio do Disque 100 – metade destes, contra pessoas idosas.**

**De acordo com informações da Federação Brasileira dos Bancos (Febraban), os golpes mais comuns contra idosos costumam usar a engenharia social: uma tática para conquistar a confiança da pessoa e ter acesso a informações privadas. Também é comum que golpes via internet e até presenciais se aproveitem da falta de familiaridade com a tecnologia.**

**Conheça alguns dos golpes mais frequentes e veja dicas de como manter-se em segurança.**



# 1. Ajuda no caixa eletrônico



## Como funciona:

Neste caso, o golpista se aproxima para oferecer ajuda na utilização do caixa eletrônico e copia ou altera a senha bancária da vítima, para ter acesso ao recurso futuramente.

## Como evitar:

Ao utilizar máquinas de caixa eletrônico, não aceite ajuda de pessoas estranhas. Confirme, com calma, se a pessoa é funcionária do banco, principalmente verificando se está usando um crachá. Se desconfiar de alguma coisa, interrompa a transação imediatamente, utilizando a tecla “anula” do caixa. Lembre-se também de retirar seu cartão da máquina.

Se for utilizar caixas eletrônicos localizados em agências bancárias, dê preferência ao horário de expediente bancário. A maior parte dos golpes presenciais acontece em horários logo no início da manhã ou à noite, quando os funcionários da agência não estão presentes.

## 2. Golpe do pix errado



### Como funciona:

O golpista envia um Pix para a conta da vítima. Em seguida, manda uma mensagem ou liga dizendo que o Pix foi enviado por engano e pede para que a pessoa devolva o dinheiro. Só que, ao invés de dar a chave Pix da transferência original, o golpista fornece uma chave de uma terceira conta. Quando a vítima devolve o dinheiro para essa terceira conta, o bandido aciona o MED (Mecanismo Especial de Devolução) para tentar obter de volta o Pix originalmente enviado à vítima. Se tiver êxito, além de receber o dinheiro enviado pela vítima, o bandido recebe também o valor pelo MED e a vítima fica no prejuízo.

### Como evitar:

Este tipo de golpe é especialmente complexo, porque apela para a boa-fé da vítima, que se sensibiliza para efetuar a devolução do dinheiro de um Pix feito para o destinatário errado, algo que realmente pode acontecer.

Portanto, redobre a atenção: caso precise fazer uma devolução de dinheiro via Pix, sempre efetue a transação para a conta original que o Pix foi feito. Para isso a pessoa deve entrar em seu aplicativo bancário e, dentro das funcionalidades do Pix, utilizar a opção de devolução da transação recebida, que automaticamente envia o valor para a conta de origem.

### 3. Golpe do falso empréstimo consignado

#### Como funciona:

O fraudador oferece por telefone um empréstimo consignado em boas condições, passando-se por um funcionário de instituição financeira. Para fechar a falsa proposta, solicita dados pessoais e pede um depósito bancário para cobrir as taxas de cadastro ou como adiantamento de parcela.

#### Como evitar:

Empréstimos em condições regulares não exigem, sob nenhuma hipótese, pagamento antecipado, seja de taxas ou de parcela.

Vale ressaltar: nunca deposite dinheiro para alguém com a finalidade de garantir um negócio ou de resgatar um prêmio que parece vantajoso.

Outro alerta importante neste caso: transações financeiras via ligação telefônica oferecem pouca segurança contra fraudes, visto que é relativamente fácil passar-se por outra pessoa. Portanto, apesar de parecer algo burocrático, é fundamental que esse tipo de operação seja feito via acesso pessoal, com identificação e senha, para a sua segurança!



## 4. Golpe da maquininha quebrada



### Como funciona:

Este tipo de golpe ocorre principalmente em pedidos via delivery (entrega em domicílio) em que o golpista se passa por entregador. Na hora de efetuar o pagamento com cartão, é apresentada uma maquininha com o visor danificado ou o golpista se posiciona de uma forma que a vítima não veja o preço cobrado na tela. O valor inserido é bem superior ao pedido e a vítima só percebe que fez um pagamento maior depois de um tempo.

### Como evitar:

Não passe seu cartão em telas com defeito, que impeçam que você confira o valor da cobrança.

Outro ponto importante: antes de efetuar o pagamento no ato da entrega, lembre-se se você realmente não pagou pelo produto no momento do pedido, via site ou aplicativo. Em caso positivo, não efetue nenhum pagamento extra na hora da entrega.

## 5. Golpe do link falso

### Como funciona:

Normalmente ocorre pelo envio de mensagens e e-mails com um link que pode parecer legítimo. No entanto, esse endereço virtual pode solicitar o compartilhamento de dados ou simplesmente instalar um vírus capaz de roubar informações do seu computador ou celular.

### Como evitar:

Antes de clicar em um link, verifique se você conhece quem enviou aquela mensagem. Caso a mensagem afirme ser de um banco ou instituição financeira, não clique no link e faça contato por meio de um dos canais oficiais dessa instituição.



## 6. Golpe do falso motoboy



### Como funciona:

O golpe começa quando o cliente recebe uma ligação do golpista que se passa por funcionário do banco, dizendo que o cartão foi fraudado. O falso funcionário solicita a senha e pede que o cartão seja cortado, mas que o chip não seja danificado. Em seguida, diz que o cartão será retirado na casa do cliente. O outro golpista aparece onde a vítima está e retira o cartão. Mesmo com o cartão cortado, o chip está intacto e os fraudadores podem utilizá-lo para fazer transações e roubar o dinheiro da vítima.

### Como evitar:

Os bancos nunca solicitam que o cliente devolva um cartão, muito menos com retirada em domicílio. Caso receba algum contato nesse sentido, interrompa a conversa imediatamente e não atenda nenhuma das solicitações.

## 7. Golpe do falso funcionário

### Como funciona:

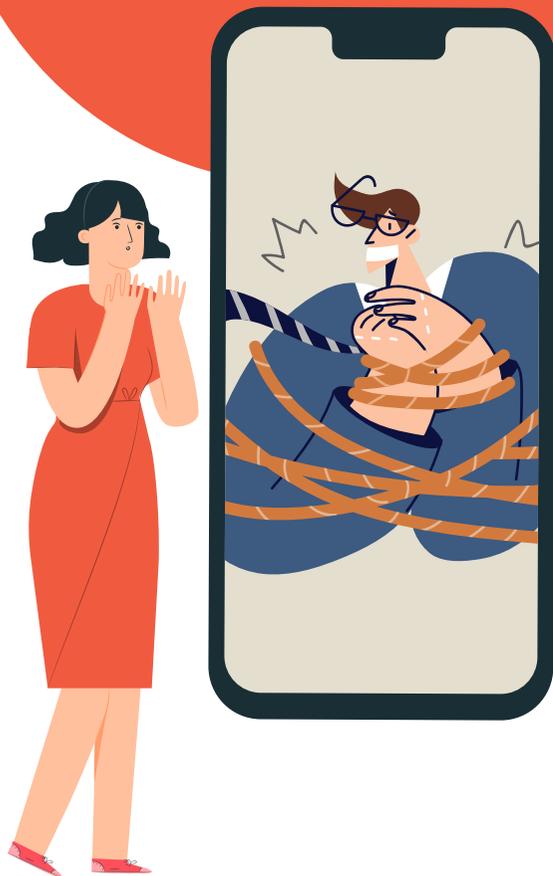
O fraudador entra em contato com a vítima se passando por funcionário de banco com a qual ela tem um relacionamento ativo. Informa que sua conta foi invadida, clonada ou outro problema e, a partir daí, solicita os dados pessoais e financeiros da vítima. Muitas vezes, pede para que a vítima ligue para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

### Como evitar:

Os bancos nunca solicitam por telefone dados pessoais, senhas ou chaves de segurança, nem pedem transferências ou pagamentos. Ao receber uma ligação suspeita, a orientação é desligar e entrar em contato com o banco pelos canais oficiais, de preferência utilizando outro telefone, para garantir que os golpistas não permaneceram na linha.



## 8. Golpe do falso sequestro



### Como funciona:

Apesar de conhecido há anos, este golpe ainda faz muitas vítimas, porque utiliza a engenharia social para envolver a pessoa em uma situação de desespero, o que facilita a tomada de decisões impensadas. Geralmente é aplicado via ligação telefônica: uma pessoa simula uma voz de choro, chamando pela mãe ou pelo pai, dizendo que foi sequestrada. Outro criminoso entra na linha e exige um dinheiro para o resgate do falso sequestro.

### Como evitar:

Sempre desconfie desse tipo de ligação e nunca fale o nome de uma pessoa que poderia ter sido sequestrada. O recomendado é desligar o telefone o quanto antes porque ao manter-se na ligação, a vítima pode acabar revelando informações pessoais que dão aspecto mais realista ao golpe. Se for possível, ligue imediatamente para este familiar, preferencialmente de outro telefone.

**Informação de qualidade também é prevenção:** a Febraban mantém uma página exclusiva e atualizada sobre os golpes financeiros mais comuns em todo o Brasil. Clique aqui para conhecer e compartilhe com seus familiares e amigos: <https://portal.febraban.org.br/AntiFraude/#1>





[www.funsest.com.br](http://www.funsest.com.br)

