# Saiba **como se proteger** quando o assunto é **dinheiro.**

Preparando você para ter segurança
em todas as suas versões

banco

# Olá!

Você sabe o que nos move aqui, no banco BV? As suas conquistas! Por isso, nós oferecemos diferentes soluções que te ajudam a alcançar cada uma delas com mais facilidade.

Nosso propósito é tornar sua vida financeira mais tranquila. E, para isso, tem uma coisa que não pode faltar: **segurança**. Preparamos este material exclusivo, com dicas, cuidados e muita informação para te ajudar na proteção contra golpes e fraudes. Tudo de um jeito simples, dinâmico e leve!

**Vamos começar?**

banco

# O que você vai encontrar aqui:

1. O que são golpes financeiros?
2. Dicas úteis para sua proteção pessoal e a proteção de seus dados.
3. O que o banco BV não faz.
4. Caí no golpe. E agora?
5. Os golpes mais comuns no mercado.

**a) Golpes para roubar suas informações**

- E-mail, SMS falsos que possuem links para sites e páginas falsas (*Phishing/Vishing/Smishing*);
- Golpe da Vídeo Chamada (ou Golpe da Mão Fantasma);
- Golpes via WhatsApp/Telegram;
- Golpe da falsa Central de Atendimento;
- Falsa restituição de IR (Imposto de Renda);
- Falsa encomenda retida nos Correios;
- Falsa oferta de emprego.

**b) Golpes relacionados a cartão de crédito**

- Golpe do falso motoboy (casos de entrega/retirada de cartões);
- Golpe do falso delivery;
- Golpe do brinde/presente de aniversário;
- Golpe da maquininha;
- Golpe da troca de cartão;
- Uso de dados do cartão na internet;
- Falsa expiração de pontos do cartão.

**c) Golpes na conta**

- Golpe do falso funcionário;
- Golpes envolvendo Pix;
- Falso investimento (pirâmides financeiras);
- Falsa investigação do gerente de conta ou do banco;
- Boleto falso.

# O que você vai encontrar aqui:

**d) Outros golpes comuns**

- Empréstimo falso;
- Golpe do FGTS;
- Golpe do Amor/Aplicativos de namoro;
- Falsa ajuda humanitária;
- Falso advogado;
- Falso leilão;
- Jogos de azar (bilhete de loteria premiado);
- Golpe da tarefa (renda extra);
- Golpes envolvendo Inteligência Artificial (*Deep Fake*/Criptomoedas/simuladores de voz).

6 Nossos canais oficiais e canais de denúncias de fraudes/golpes.

7 Dica bônus: Sua segurança é da nossa conta!

- Segurança nas redes sociais;
- Roubo de celular – como agir para se proteger

# 1 O que são golpes financeiros?

Golpes financeiros são práticas fraudulentas e enganosas, que visam roubar dinheiro, dados e informações pessoais de forma ilícita.

Os golpistas costumam usar estratégias para conquistar sua atenção e confiança, geralmente com promessas tentadoras e oportunidades que aparentam ser incríveis, mas que, na realidade, são enganosas.

Por exemplo: aquele investimento com retorno espetacular ou aquela promoção irresistível que parece um sonho? **É preciso ter cuidado, porque pode ser golpe.**

# Mas como um golpe chega até mim?

Existem muitas formas que fraudadores podem utilizar para enganar você, tais como:

- Oferta de vendas
- Proposta de emprego
- Contratação de serviços
- Boletos e contas falsas

**E por onde isso pode ser recebido?**
Os meios pelos quais as fraudes são enviadas também variam:

- E-mail
- Redes Sociais
- SMS
- Telefone/celular

Em geral, o primeiro passo dos golpistas é conseguir suas informações pessoais para tentar acessar seus dados do banco.

**Lembre-se!**

Cuidado com mensagens falsas **que se passam pelo banco BV**. Essas mensagens podem falar sobre atualização de senha, bloqueio de cartão de crédito ou ofertas especiais. Sempre verifique se a comunicação é verdadeira!

# Você sabia?

As transações bancárias aumentaram significativamente em 2024, atingindo **R$ 186 bilhões**, com destaque para o mobile banking, que **cresceu 22%**.

Praticamente, **7** em cada **10** transações bancárias são realizadas pelo celular.

Fonte: Pesquisa Febraban de Tecnologia Bancária| Volume 2 | 2024

Ao mesmo tempo:

**O prejuízo com golpes financeiros supera os**

**R$ 10 bilhões**

**em 2024, afirma a Febraban.**

**A cada 16 segundos**

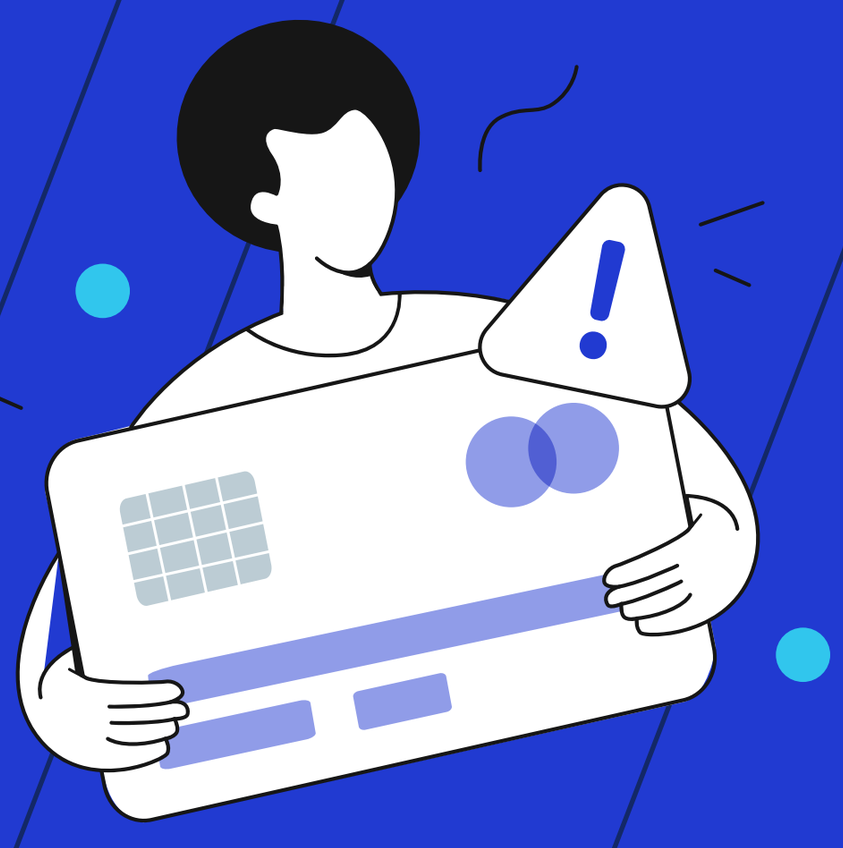
**acontece uma fraude bancária, um crime no sistema financeiro eletrônico no Brasil.**

Fonte: Folha de São Paulo, 12/3/25 | Dados do 2º Congresso de Prevenção e Repressão a Fraudes, Segurança Cibernética e Bancária.

E segundo a pesquisa Febraban de Tecnologia Bancária de 2024, os bancos estimaram um investimento de **R$ 47,4 bilhões em tecnologia.**

As instituições financeiras seguem implantando diversas medidas de segurança, porém, os números de golpes ainda apresentam um aumento significativo no mundo digital. E o nosso cuidado tem que aumentar também!

# 2 Como posso me proteger?



## Confira algumas dicas importantes:

1. Evite compartilhar dados pessoais e senhas nas conversas por WhatsApp/Telegram, SMS ou redes sociais, pois em caso de extravio do seu celular, um fraudador poderá utilizar dessas informações para se passar por você e acessar outros dados.

2. **Fique de olho na fatura do seu cartão e no seu extrato.** Se desconfiar de algo, entre em contato pelos nossos Canais de Atendimento. Estamos sempre aqui para ajudar!

3. **Ao receber uma ligação suspeita, desligue, espere 5 minutos e entre em contato com nossos Canais de Atendimento oficiais.**

   **Atenção:** é importante esperar esses minutos para não ter o risco da sua ligação ser interceptada pelos golpistas, combinado?

   **Lembre-se:** o banco BV não pede dados importantes por telefone.

4. **Evite abrir documentos recebidos de pessoas desconhecidas no WhatsApp/Telegram.** Caso a mensagem seja de alguém conhecido, mas que não costuma enviar arquivos, vale a pena fazer uma ligação para a pessoa e confirmar a veracidade do documento.

5. **Evite responder mensagens de empresas desconhecidas**, que oferecem benefícios não solicitados que pareçam extremamente vantajosos. Pense bem antes de trocar seus dados por descontos, produtos ou serviços.

   **Lembre-se:** você pode encontrar os canais oficiais das empresas em seus sites. Verifique se o número de telefone, endereço de e-mail ou perfil na rede social são verdadeiros.

# 3 O que o banco BV não faz.

1. Não pedimos suas informações bancárias e senhas.
2. Não mandamos funcionários para sua residência.
3. Não recolhemos cartões, mesmo aqueles que você não utiliza mais.
4. Não solicitamos nenhum tipo de depósito ou transferência em contas bancárias.
5. Não pedimos que você acesse links de redes sociais, e-mail, SMS ou WhatsApp.
6. Não enviamos links para você atualizar cadastro, senha, baixar softwares de segurança ou desbloquear contas.
7. Não enviamos boletos de quitação com descontos exorbitantes.
8. Não solicitamos acesso aos seus aplicativos do banco ou a qualquer outro sistema.

# 4 Caí num golpe. E agora?

Nós entendemos que qualquer pessoa pode estar sujeita a enfrentar um golpe financeiro. E o jeito mais seguro de lidar com essa situação é aprender a diminuir os danos causados por ela.

Por isso, **conheça as principais medidas a serem tomadas caso você seja vítima de uma fraude:**

### Informe o banco BV

Ao perceber a tentativa de golpe e fraude financeira, acione o banco BV imediatamente por meio de nossos canais de comunicação oficiais, como redes sociais (Facebook, Instagram, Twitter e LinkedIn), site, app, Centrais de Atendimento e Ouvidoria.

Solicite nosso auxílio para cancelar cartões, verificar perfis e sites falsos do banco BV na internet.

### Faça um boletim de ocorrência

Em caso de golpes e fraudes, o banco BV recomenda sempre registrar formalmente uma denúncia e evitar que novas cobranças sejam feitas em seu nome.

Em posse de todas as informações sobre o evento ocorrido, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico pelo site da Polícia Civil do seu estado.

Caso seu celular seja roubado, apague remotamente dados que estão nele e avise sua operadora para bloquear sua linha telefônica e o IMEI do aparelho.

# 5 Quais são os tipos de golpe que existem?

Conheça alguns dos principais.

# A Golpes para roubar suas informações

Já ouviu falar que, hoje em dia, informação vale ouro? Pois é. Muitos golpes começam com "simples" dados pessoais e podem acabar trazendo um prejuízo enorme. Por isso, é muito importante sempre cuidar bem das suas informações.

## E-mail, SMS falsos que possuem links para sites e páginas falsas *(Phishing/Vishing/Smishing)*

*Phishing* vem do inglês "*fishing*", que significa pescaria. Esse tipo de fraude rouba seus dados e senhas por meio de mensagens e sites falsos.

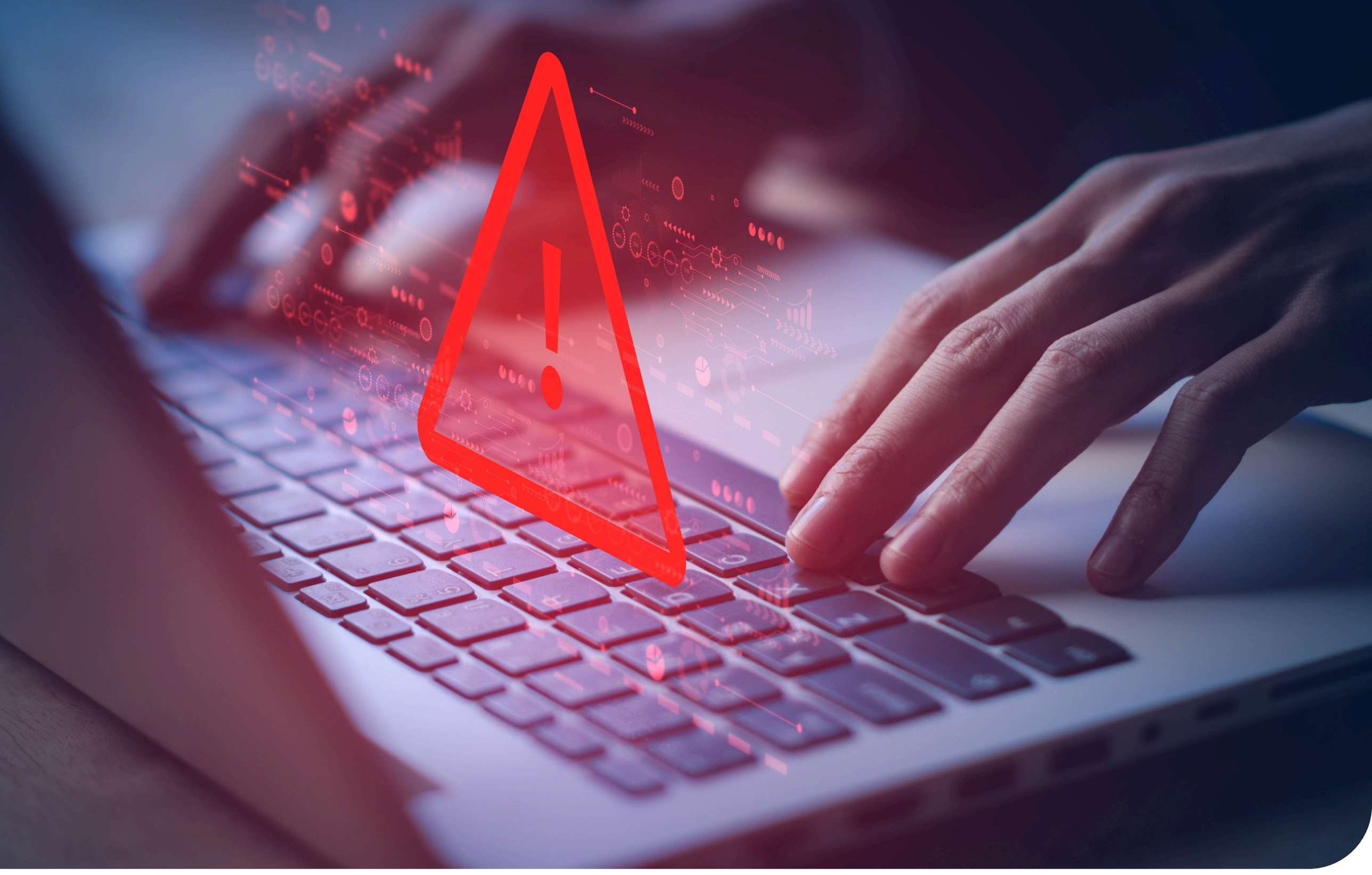
Saiba mais sobre esse tipo de golpe e veja como não morder essa isca.

### Como acontece:

- Fraudadores enviam mensagens por e-mail, WhatsApp/Telegram ou SMS com promoções incríveis ou assuntos alarmantes, com a intenção de que você clique em um link ou abra um anexo;
- É comum que essas mensagens possuam ameaças para te pressionar. Elas podem indicar, por exemplo, que caso você não preencha determinadas informações, sua conta será bloqueada por irregularidade no cadastro ou falta de atualização;
- Quando você envia os dados, o golpista utiliza as informações passadas para acessar sua conta bancária ou fazer compras indevidas na internet.

### Como se proteger:

- Leia e-mails e mensagens SMS com atenção, e desconfie de pedidos estranhos.
- Não informe dados pessoais e importantes por telefone, e-mail ou SMS.
- Cuidado com mensagens com erros de português e que passam um tom de urgência, exigindo respostas rápidas.
- Não abra anexos de desconhecidos e bloqueie números suspeitos.
- Passe o mouse sobre o endereço do link ou o botão e confira se faz sentido com a suposta empresa.
- Desconfie de endereços de e-mail terminados em ".com" e sem ".br".
- Todos os aplicativos de e-mail possuem recursos para Relatar a Mensagem como "Spam" ou "Phishing". Utilize esses recursos sempre que possível.
- Em caso de dúvidas, entre em contato com nossos Canais de Atendimento oficiais para confirmar a mensagem recebida.



## **Golpe da Vídeo Chamada** (ou Golpe da Mão Fantasma)

Esse tipo de golpe ocorre no ambiente virtual, quando os criminosos enviam links por meio de aplicativos de mensagens ou redes sociais. Uma vez que o golpista tem controle remoto sobre o seu dispositivo, ele pode realizar diversas atividades maliciosas.

### Como acontece:

- Ao clicar no link enviado pelos golpistas, eles conseguem instalar malware nos dispositivos, facilitando o acesso e o roubo de informações pessoais, como senhas e dados bancários.

### Como se proteger:

- Para evitar cair nesse golpe, é fundamental ter cautela ao abrir links, especialmente se vierem de fontes desconhecidas.
- Mantenha seus dispositivos sempre atualizados e, se possível, providencie um antivírus para eles.
- Evite utilizar redes abertas de Wi-Fi quando for consultar suas transações financeiras.

## Golpe via WhatsApp/Telegram

Tomar cuidado com seu "zap" também é muito importante para não cair em fraudes. Veja os dois principais golpes no aplicativo de mensagens mais utilizado pelos brasileiros.

### Como acontece:

**a) Invasão da conta**

- O golpista entra em contato como se fosse um funcionário do banco e te convence a informar o código de segurança, normalmente enviado por SMS;
- Com o código em mãos, o golpista consegue acessar seu WhatsApp/Telegram no aparelho dele;
- Ao entrar na sua conta, ele finge ser você e pede dinheiro emprestado para seus contatos.

**b) Criação de conta falsa**

- O golpista cria uma nova conta de WhatsApp/Telegram utilizando seu nome e sua foto de perfil (retirada das redes sociais, por exemplo);
- Com a conta falsa, ele diz aos seus contatos que aquele é seu novo número;
- Conversa vai, conversa vem, o golpista, se passando por você, pede dinheiro emprestado.

### Como se proteger:

- Nunca passe os códigos de confirmação do WhatsApp/Telegram (normalmente recebidos por SMS).
- Não compartilhe seu número em redes sociais. Lembre-se de que qualquer pessoa pode ter acesso a informações que são postadas.
- Se um amigo ou familiar pedir dinheiro emprestado, sempre confirme por chamada de voz ou vídeo se realmente é a pessoa que está pedindo.

**Dica:**
O WhatsApp também oferece ferramentas dentro do aplicativo para a sua segurança:

**Confirmação em duas etapas:** abra as Configurações, clique em “Contas” e depois, em “Confirmação em duas etapas”. Crie uma senha e coloque seu e-mail. De tempos em tempos, o aplicativo pedirá para você digitar sua senha e deixará sua conta mais segura.

**Acesso à foto de perfil:** configure o acesso à sua foto de perfil apenas para aos seus contatos. Abra as Configurações, clique em "Conta", selecione "Privacidade" e depois, "Foto de Perfil".

Além disso, instale somente aplicativos oficiais no seu aparelho. Faça também uma varredura em seus apps, desinstalando aqueles que você não conhece ou não utiliza há muito tempo.

## Golpe da falsa central de atendimento

Sabe qual é uma das principais estratégias dos golpistas para conquistar a sua confiança? **Ligar fingindo ser um funcionário do banco**. Alguns até chegam a simular barulhos de escritório e usam falas muito convincentes.

### Como acontece:

**a) Invasão da conta**

- A abordagem pode acontecer por telefone ou WhatsApp e, durante a conversa, o golpista finge trabalhar no banco e propõe algum tipo de solução especial, ou informa que sua conta bancária ou seu cartão estão com algum problema. Porém, há sempre uma condição: o envio de dados, como senhas, cartões e códigos de segurança do celular. Com isso, eles podem fazer transferências, compras ou invadir seu perfil do WhatsApp/Telegram para enganar amigos e familiares.

### Como se proteger:

- Nós **nunca pedimos senhas** por telefone, e-mail, redes sociais ou SMS.
- Não passe seus dados pessoais e informações importantes por telefone.
- **Ao receber uma ligação suspeita**, espere 5 minutos e **ligue para o banco BV pelos canais oficiais**.

## Falsa restituição de IR (Imposto de Renda)

Golpes envolvendo falsa restituição do Imposto de Renda (IR) são uma prática comum de criminosos, especialmente durante o período de declaração. Aqui estão algumas características e dicas para se proteger:

### Como acontece:

- Os golpistas enviam mensagens falsas por e-mail, SMS ou redes sociais, alegando que há pendências no CPF ou que a restituição está disponível, mas precisa ser "liberada";
- Essas mensagens geralmente contêm links para sites fraudulentos que imitam o portal da Receita Federal. Ao acessar, a vítima é induzida a fornecer dados pessoais e bancários;
- Outra tática é o envio de correspondências físicas com intimações falsas, pedindo regularização de dados cadastrais.

### Como se proteger:

- Desconfie de mensagens que pedem ações urgentes ou oferecem vantagens incomuns.
- Sempre acesse o site oficial da Receita Federal (gov.br) para verificar informações.
- Não clique em links suspeitos ou forneça dados pessoais sem confirmar a autenticidade da solicitação.
- Utilize o aplicativo oficial "Meu Imposto de Renda" ou o e-CAC para realizar consultas e declarações.

## Falsa encomenda retida nos Correios

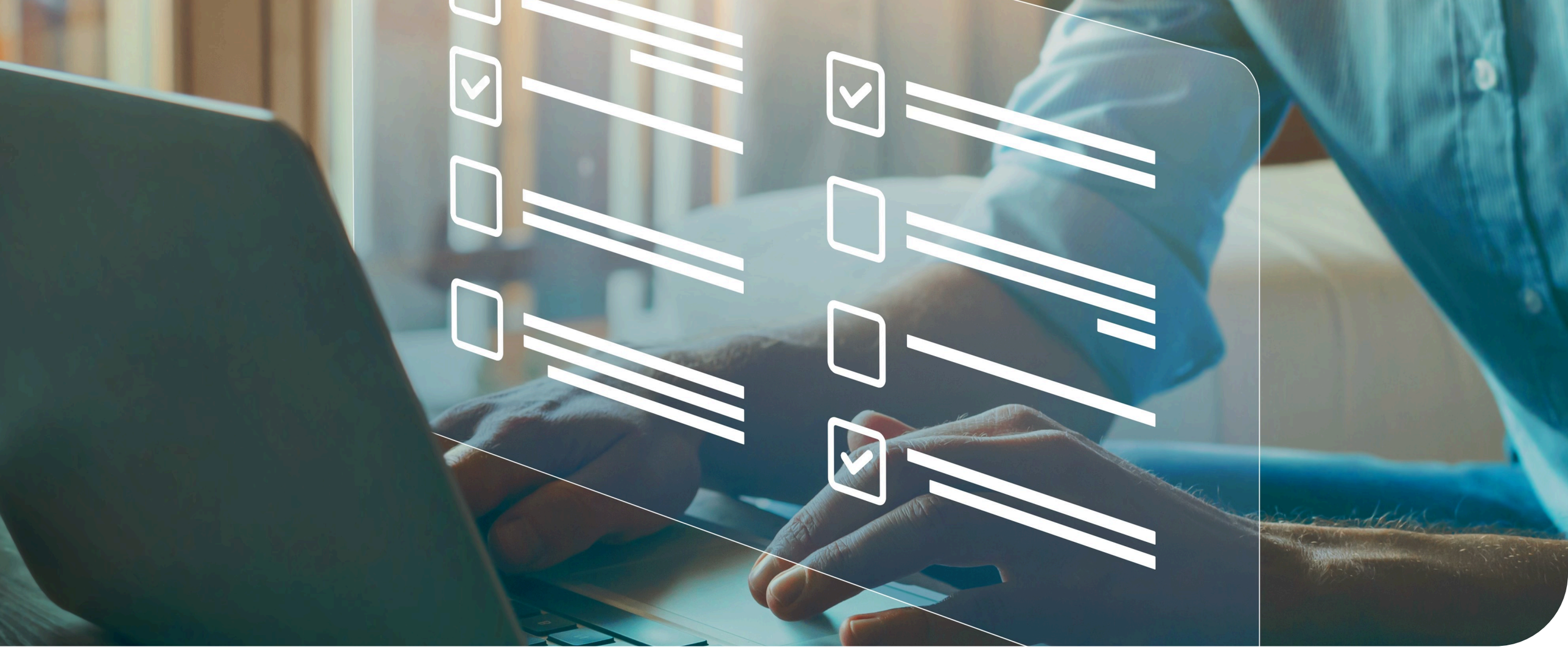
Golpes envolvendo falsas encomendas retidas nos Correios são uma prática comum de criminosos, especialmente com o aumento das compras online. Aqui está um resumo de como esse golpe funciona:

### Como acontece:

- Os golpistas enviam mensagens falsas por e-mail, SMS ou redes sociais, alegando que uma encomenda está retida na alfândega ou nos Correios;
- Essas mensagens geralmente contêm links para sites fraudulentos que imitam o site oficial dos Correios, solicitando dados pessoais, como CPF e informações bancárias, ou o pagamento de uma suposta taxa de liberação;
- Em alguns casos, os golpistas enviam boletos falsos ou pedem transferências via Pix.

### Como se proteger:

- Verifique sempre o endereço do site (URL).
  O site oficial dos Correios é **correios.com.br**.
- Desconfie de mensagens que criam um senso de urgência ou pedem pagamentos imediatos.
- Nunca clique em links suspeitos. Acesse diretamente o site oficial dos Correios para rastrear encomendas.
- Utilize o aplicativo oficial dos Correios para verificar o status de suas encomendas.



## Falsa oferta de emprego

Se você está nessa fase de procurar emprego, confira a seguir como identificar se a vaga é verdadeira ou se é um golpe do falso emprego:

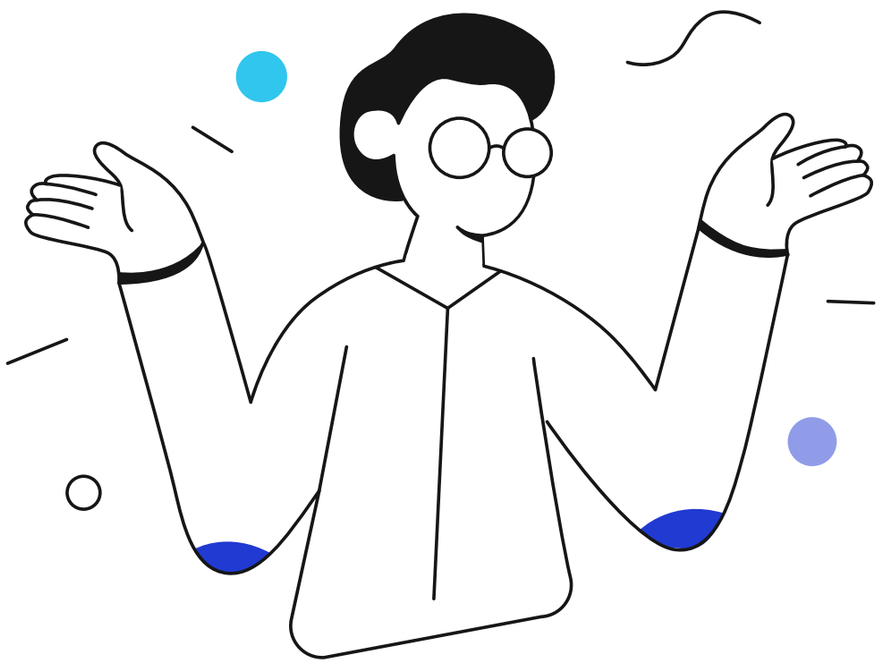
### Como acontece:

- O **golpe do falso emprego** começa com uma oferta de trabalho vantajosa que chama a atenção até de quem já tem uma boa ocupação. Os pontos mais atrativos são o **salário acima da média do mercado, pouca exigência de tempo e conhecimento**;
- Os golpistas podem enviar links de formulários **para a vítima preencher com informações sensíveis ao se candidatar**. Eles usam esses dados para fazer empréstimos usando o nome da pessoa;
- O ponto em comum entre as abordagens dos criminosos é que, assim que você paga o valor que eles pedem ou passa suas informações, **a suposta empresa desaparece**, os contatos são bloqueados e você não recebe retorno deles.

### Como se proteger:

- Se a vaga pede pouca experiência, poucas horas de trabalho e paga um salário muito alto, isto é um sinal de fraude. Desconfie quando a companhia abre mão de algo que o mercado costuma pedir, como tempo de experiência e alguma formação na área.
- Infelizmente, existem diversos perfis de recrutadores e agências de emprego que postam falsas vagas como se fossem de grandes empresas;
- Verifique a reputação da agência e da empresa em sites como o Reclame Aqui;
- Tome cuidado com contatos que pedem urgência para se candidatar e enviar documentos para a seleção. Normalmente, esse tipo de golpe vai pedir para você pagar pelo exame, fazer um curso ou vai alegar outro motivo.

# B Golpes relacionados a cartão de crédito



O cartão de crédito é uma das formas de pagamento mais utilizadas e um dos meios mais visados para a aplicação de golpes. Por isso, é importante conhecer as principais abordagens para se prevenir contra elas.

## **Golpe do falso motoboy** (casos de entrega/retirada de cartões)

### Como acontece:

- O golpista entra em contato com você como se fosse um funcionário do banco, diz que houve uma compra duvidosa ou que seu cartão foi bloqueado, e pede para você ligar no número que fica no verso do cartão. Ele pode interceptar uma ligação;
- Ainda na linha, o golpista coloca uma música de espera, igual à utilizada pelo banco;
- Depois são solicitadas informações importantes, como dados pessoais e senhas;
- Em seguida, é informado que um funcionário visitará sua residência para trocar seu cartão. Com os dados e o cartão em mãos, o golpista pode fazer diversos saques, compras e transações.

### Como se proteger:

- Não passe seus dados pessoais e informações importantes por telefone.
- Não entregue nenhum cartão, mesmo que a pessoa fale que é funcionária do banco.
- Corte o chip de cartões cancelados, danificados ou que você não vai mais utilizar.
- Confirme se as ligações que você recebe são verdadeiras. Você sempre pode pedir ajuda em nossos Canais de Atendimento oficiais.

**Lembre-se:**
Após receber uma ligação suspeita, espere alguns minutos antes de ligar para os Canais de Atendimento. Assim, não tem risco de os golpistas interceptarem a ligação.

## Golpe do falso delivery

### Como acontece:

Com a participação de entregadores de aplicativo e serviços de delivery, o golpe acontece por meio da adulteração da máquina de cartões. Existem 3 estratégias principais:

- O entregador diz que o visor da maquininha está quebrado e, assim, cobra um valor maior sem você perceber;
- – Diz que o estabelecimento cobrou o valor errado no pedido, exigindo um pagamento extra no momento da entrega;
- – Fala que houve problemas com o pagamento e que ele não foi creditado, pedindo para você pagar novamente.

### Como se proteger:

- Sempre que possível, escolha o pagamento direto pelo aplicativo.
- Caso precise pagar na entrega, utilize dinheiro sempre que conseguir.
- Confirme o valor digitado na maquininha de cartões. Se possível, solicite o comprovante impresso.
- Não entregue seu cartão para outras pessoas.
- Prefira pagar no crédito e cubra as informações do cartão, como número e CVV (código de segurança do cartão).
- Desconfie se a tela da maquininha de cartão estiver quebrada ou coberta de alguma forma.

## Golpe do brinde/presente de aniversário

O golpista se apresenta como entregador e te aborda para deixar um brinde ou presente. Na maioria das vezes, eles aparecem em datas comemorativas, como aniversários:

### Como acontece:

- Para realizar a entrega, o golpista pode solicitar dados pessoais e uma foto do seu rosto (selfie). Com seus dados e foto, eles podem abrir contas em seu nome ou pegar empréstimos, por exemplo;
- Ele pode cobrar uma taxa de entrega com valor baixo, para não levantar suspeitas, mas quando você consulta sua conta posteriormente, verifica que o valor cobrado foi muito maior.

### Como se proteger:

- Nunca forneça seus dados bancários ou suas informações pessoais.
- Não aceite que tirem fotos dos seus documentos ou do seu rosto com o aparelho do entregador.
- Contate o remetente e confirme se o estabelecimento te enviou algum brinde/presente.
- Não faça pagamentos de taxas, principalmente se o visor da maquininha estiver danificado.

## Golpe da maquininha

Em momentos de distração, é comum não verificarmos os valores na maquininha quando vamos fazer algum pagamento, o que pode levar a cobranças indevidas.

### Como acontece:

- Para realizar um pagamento, a maquininha de cartão pode estar danificada ou adulterada, dificultando a visualização do valor digitado;
- Os criminosos podem usar maquininhas falsas, que imitam as originais, para clonar dados e cartões.
- Em alguns casos, os golpistas manipulam o software da maquininha para capturar informações sensíveis ou realizar cobranças indevidas.

### Como se proteger:

- Verifique sempre o visor da maquininha antes de inserir o cartão. Se possível, solicite o comprovante impresso.
- Monitore regularmente o extrato do cartão para identificar transações não autorizadas.
- Configure, no app do seu banco, a confirmação de compras via mensagem SMS ou push.

## Golpe da troca de cartão

É um golpe comum em que golpistas podem aproveitar de um momento de distração e realizar a troca do seu cartão por um cartão semelhante.

### Como acontece:

- Os golpistas podem distrair suas vítimas com conversas ou situações inesperadas enquanto observam a senha sendo digitada;
- Isso pode acontecer em caixas eletrônicos, estabelecimentos comerciais ou até mesmo com vendedores ambulantes;
- Com o cartão e a senha em mãos, eles realizam transações fraudulentas rapidamente, causando grandes prejuízos financeiros.

### Como se proteger:

- Para evitar esse golpe, é importante estar atento ao manuseio do cartão e nunca compartilhar sua senha.
- Cole adesivos em seu cartão para facilitar a identificação.
- Não aceite ajuda de estranhos. Desconfie de pessoas que se oferecem para ajudar, especialmente em locais com grande concentração de pessoas ou em caixas eletrônicos.

## Uso de dados do cartão na internet

O roubo de dados de cartão de crédito é um golpe sofisticado e perigoso. Ele ocorre quando criminosos obtêm informações sensíveis, como número do cartão, nome do titular, data de validade e código de segurança (CVV), geralmente por meio de técnicas como clonagem, *phishing*, engenharia social ou quando cadastramos dados do cartão e salvamos ele para utilizar em sites/páginas de *e-commerces*.

**Como se proteger:**

- Para evitar esse golpe, você pode utilizar o seu cartão virtual temporário ou para pagamentos recorrentes.
- Evite compartilhar informações do cartão em sites não confiáveis.
- Use a autenticação em duas etapas e monitore suas transações regularmente.

## Falsa expiração de pontos do cartão

O golpe da falsa expiração de pontos do cartão é uma fraude que utiliza programas de recompensas de cartões de crédito como isca.

### Como acontece:

- Os criminosos enviam mensagens fraudulentas por e-mail, SMS ou WhatsApp/Telegram, afirmando que os pontos acumulados estão prestes a expirar;
- Essas mensagens contêm links que levam a páginas falsas, feitas para imitar sites oficiais de bancos ou operadoras de cartões.

### Como se proteger:

- Golpistas frequentemente usam o senso de urgência para enganar as vítimas. Se receber mensagens sobre expiração de pontos, evite agir impulsivamente.
- Nunca clique diretamente em links enviados por e-mail, SMS ou WhatsApp/Telegram.
- Sempre acesse o site oficial do seu banco ou contate a operadora do cartão para confirmar a informação.

# Golpes na conta

A conta corrente é uma das formas mais simples e práticas para você guardar e movimentar o seu dinheiro. Por isso, ela é um grande alvo de golpistas. Saiba como se proteger!

## Golpe do falso funcionário

Fingir ser funcionário do banco é uma forma muito utilizada pelos golpistas para conquistar a confiança das vítimas. Alguns deles até simulam barulhos de escritório e usam falas padrão dos bancos. Veja como evitar esse tipo de golpe.

### Como acontece:

- O golpista entra em contato com você, normalmente por telefone ou WhatsApp/Telegram, e diz que é um funcionário do banco;
- Durante a conversa, sempre com um tom alarmista, ele te convence a passar seus dados, como senhas de aplicativos, cartões e códigos de segurança do celular;
- Ao conseguir essas informações, faz transferências e compras, ou invade seu perfil do WhatsApp/Telegram para extorquir familiares e amigos.

### Como se proteger:

- Nunca informe sua senha para outras pessoas.
- Explique e alerte sobre o golpe do funcionário falso para as pessoas que moram com você.
- Ative a verificação em duas etapas para aplicativos de mensagens e do banco.
- Desconfie de qualquer contato surpresa que envolva empresas conhecidas ou desconhecidas.

## Golpes envolvendo Pix

O "faz um Pix" virou uma frase comum em nossas vidas, não é? Mas precisamos tomar muito cuidado com os golpes que vieram junto com essa nova forma de pagamento. Conheça os dois principais.

### Como acontece:

**- Capturador de tela**

- Os golpistas encaminham um e-mail com link ou PDF com um arquivo malicioso;
- Se aberto, o arquivo infecta seu celular ou computador com um vírus que alerta os golpistas quando um aplicativo ou site de banco é acessado;
- Feito isso, eles conseguem capturar seus dados e acessos do banco.

**- Falso funcionário**

- Os golpistas fingem que são funcionários do banco e entram em contato com você;
- Eles pedem dados pessoais e financeiros, dizendo que é para regularizar seu cadastro do Pix ou criar uma chave Pix;
- Por fim, dizem que é preciso fazer testes para ver se tudo está funcionando. Dessa forma, os golpistas fazem com que você realize transferências, sem perceber que caiu em um golpe.

**- Pix errado**

- Os golpistas mandam uma mensagem dizendo que enviaram um Pix errado para você e solicitam a devolução do dinheiro via MED (Mecanismo Especial de Devolução);
- Para comprovar a transação, eles enviam um comprovante do Pix. Porém, pode ser um comprovante falso ou, até mesmo, um Pix agendado que ainda não foi efetuado.

### Como se proteger:

- Entre em contato com nossos Canais de Atendimento oficiais para tirar dúvidas e verificar se a mensagem é verdadeira.
- Não abra links de mensagens que oferecem benefícios, brindes, cupons, prêmios ou atualização de dados por meio da chave Pix.
- Ao receber um pagamento pelo Pix, confirme se o valor realmente caiu na sua conta ou espere a liberação do Pix.

**Lembre-se:**
Funcionários e representantes do banco BV não ligam para os clientes para fazer cadastros e testes do Pix.

## **Falso investimento** (pirâmides financeiras)

### O que é pirâmide financeira?

- Uma pirâmide financeira é um esquema baseado no recrutamento de participantes, com a promessa de retornos elevados e relativamente fáceis. Para que esses rendimentos sejam pagos, as pessoas que ingressam dependem da entrada de novos membros, que vão aportando dinheiro e chamando novos integrantes para o grupo.

- Conforme a base aumenta, os mais antigos no grupo recebem recursos dos que entraram mais recentemente, e isso dá a falsa ilusão de que o sistema é lucrativo. Porém, em uma pirâmide financeira, o dinheiro simplesmente passa de um nível para o outro, pois não existe nenhum produto ou serviço em contraprestação. A sustentação da pirâmide é temporária, portanto, tende sempre a ruir.

### Como se proteger:

- Entre em contato com nossos Canais de Atendimento oficiais para tirar dúvidas e verificar se o produto para investimento é real.

## Falsa investigação do gerente de conta ou do banco

Criminosos ligam para clientes de bancos e alegam que sua agência bancária ou gerente está sob investigação.

### Como acontece:

- Com a justificativa de proteger a conta bancária, os criminosos orientam a vítima a transferir os recursos da conta para favorecidos indicados por eles, durante o andamento da suposta investigação criminal. "E chegam até a mandar um boletim de ocorrência falso para dar credibilidade ao golpe", conforme afirma a Febraban em nota.

### Como se proteger:

- Os bancos, entidades ou autoridades policiais nunca pedem que clientes façam transações bancárias.
- Se receber este tipo de contato, encerre-o na hora.
- E se tiver dúvidas, esclareça diretamente através dos canais oficiais do seu banco.

## Boleto falso

Imagina pagar seu boleto e descobrir que ele era falso. Ninguém merece, né? Saiba como funciona e como identificar esse tipo de golpe.

### Como acontece:

- O golpista envia boletos falsos e personalizados por e-mail, SMS ou até pelo correio;
- Ele informa que, se o boleto não for pago, algum serviço será cancelado, como financiamento, cartão de crédito ou empréstimo;
- Em alguns casos, é criado até um site falso onde a vítima gera esse tipo de boleto;
- Não conseguir fazer a leitura do código de barras pode ser um sinal de boleto falso. Normalmente, esses boletos não conseguem ser lidos por caixas eletrônicos ou câmeras de celulares, fazendo você digitar o número manualmente;
- Ao fazer o pagamento, o valor é repassado para a conta do golpista.

### Como se proteger:

- Confira sempre o código de barras e os últimos números do boleto, que correspondem ao valor a ser pago.
- Verifique se o beneficiário final está correto. Ele sempre deve ser um dos beneficiários abaixo:

| BV Financeira S.A. CFI | Banco Votorantim S.A. | Banco BV S.A. |
|---|---|---|
| CNPJ 01.149.953/0001-89 | CNPJ 59.588.111/0001-03 | CNPJ 01.858.774/0001-10 |

- Evite pagar boletos recebidos por correio. Se você é cliente do Financiamento de Veículos BV ou do Cartão BV, a forma mais segura de acessar seus boletos é pelo nosso app. Para todos os clientes, temos também a opção de acessar os boletos pela “Minha BV”.
- Baixe o nosso app na loja de aplicativos do seu celular ou acesse a “Minha BV” em www.bv.com.br.
- Utilize o DDA (Débito Direto Autorizado), um tipo de serviço em que o boleto é enviado diretamente para a sua conta. Ele é mais prático e seguro, já que, dessa forma, o boleto é acessado somente por você por meio eletrônico.

# D Outros golpes comuns

Contratação de empréstimos, pagamento de boletos ou saque do FGTS: existem golpes até para as atividades financeiras mais comuns do nosso cotidiano. Saiba como eles acontecem!

## Empréstimo falso

Imagina só: você está precisando de dinheiro, encontra uma oportunidade imperdível de empréstimo e, no fim, acaba de mãos vazias. Isso acontece com muitas pessoas nesse tipo de golpe.

### Como acontece:

- O golpista oferece empréstimos com condições super vantajosas em nome do banco;
- Ao te convencer a fechar um acordo, ele cobra valores como adiantamento, além de pedir vários dados pessoais;
- Depois o golpista desaparece, levando todo o dinheiro e as informações coletadas, que podem ser usadas para realizar outros golpes.

### Como se proteger:

- Desconfie de ofertas muito atrativas de empréstimo, sem consulta de crédito, por exemplo.
- Nunca deposite valores adiantados, nem para o pagamento de taxas.
- Pesquise se a empresa é parceira do banco BV. Verifique informações como o contato oficial (e-mail e telefone), endereço, imagens e comentários de clientes. Acessar as redes sociais também é importante para ter certeza de que a instituição existe e é confiável.
- Escolha sites de confiança para fazer simulações. Na dúvida, procure nossos Canais Oficiais para saber se eles são parceiros do banco BV.
- Não forneça dados pessoais por meio das redes sociais. Nada de informar documentos, endereço, telefone e e-mail. O envio desses dados deve ser feito somente em aplicativos e sites oficiais, combinado?!

**Lembre-se:**
Criminosos dizem que o empréstimo foi aprovado e que só é preciso enviar os documentos para concluir a negociação. Não acredite nisso.

## Golpe do FGTS

Nem seu FGTS fica livre dos olhos de golpistas. Confira como funciona e como proteger seu dinheiro.

### Como acontece:

- Os golpistas dizem que você tem dinheiro do FGTS disponível para saque;
- Junto com a mensagem, enviam um link para sites falsos, onde você precisa responder uma pesquisa sobre seus últimos saques e se tem interesse em receber algum valor;
- Em seguida, solicitam dados pessoais que são utilizados para fazer saques do FGTS, contratar empréstimos ou abrir contas em bancos.

### Como se proteger:

- Entre em contato com o FGTS pelos canais de atendimento oficiais para verificar se realmente existem valores disponíveis e se a mensagem recebida é verdadeira.
- A imprensa normalmente informa quando saques do FGTS são liberados. Verificar se existem notícias sobre o assunto é uma boa forma de se proteger.
- Desconfie e não clique em links de mensagens enviadas por canais não-oficiais.
- Verifique se o site que pede suas informações é oficial e confiável. Na dúvida, não passe seus dados.
- Utilize senhas difíceis, troque-as de tempos em tempos e não passe elas para ninguém.
- Baixe o aplicativo do FGTS. Com ele, você consegue acompanhar o seu saldo mensal.
- Verifique o seu CPF em sites especializados como o Serasa, para garantir que não estão usando seus dados indevidamente.

## Golpe do amor/Aplicativos de namoro

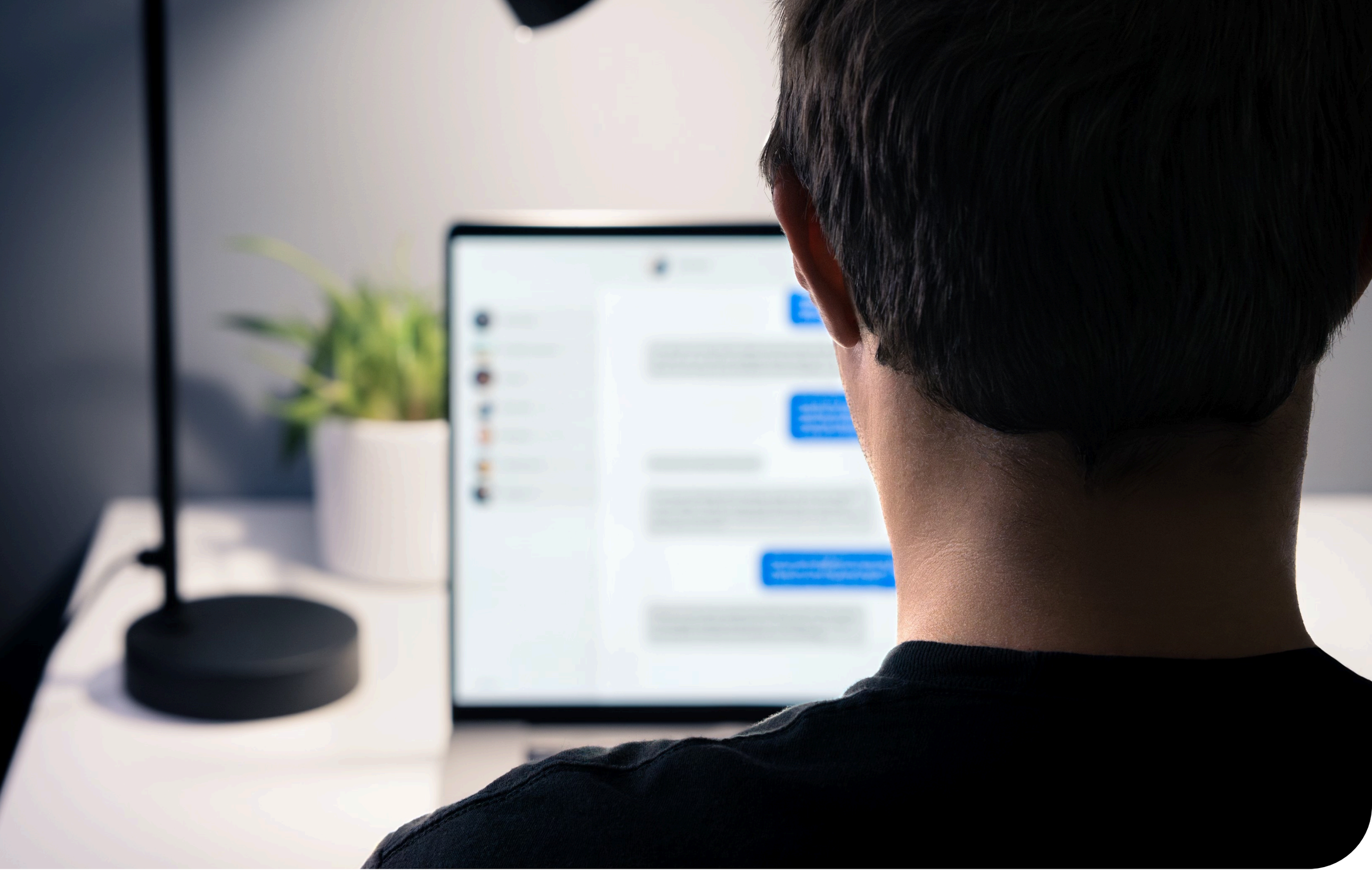
Com certeza você já ouviu falar sobre pessoas que caíram (ou quase) em golpes dentro de sites de relacionamento. Nesse tipo de golpe, criminosos exploram plataformas de namoro para enganar pessoas em busca de relacionamentos genuínos.

Eles utilizam histórias cativantes e envolventes para estabelecer uma conexão emocional. Com isso, há uma variação enorme **do golpe de relacionamentos on-line, veja algumas abordagens:**

- Atenção aos APPs de namoro: golpistas encorajam você a clicar em um link de terceiros para verificar sua conta. Após clicar, serão solicitados seus dados pessoais como nome, endereço, número de telefone, e-mail, CPF, data de nascimento e até informações bancárias ou de cartão de crédito.
- Pode acontecer, também, a instalação de um malware que captura suas informações.
- Os golpistas criam perfis falsos em redes sociais ou sites de relacionamento, apresentando-se como pretendentes amorosos.
- Posteriormente, solicitam favores financeiros, alegando emergências e explorando a vulnerabilidade emocional da vítima.
- Pedem seus dados em troca de fotos íntimas.
- Podem ter abordagem através de uma suposta herança. O golpista finge precisar se casar para herdá-la e, após construir um relacionamento com a vítima, pede dinheiro para trazer essa herança ao país da vítima, mas nunca aparece.
- Embora algumas dessas histórias possam ser improváveis, é importante lembrar que as vítimas estão sozinhas ou vulneráveis. O golpista pede dinheiro para pagar voos (ou às vezes um passaporte) para visitar o país da vítima.

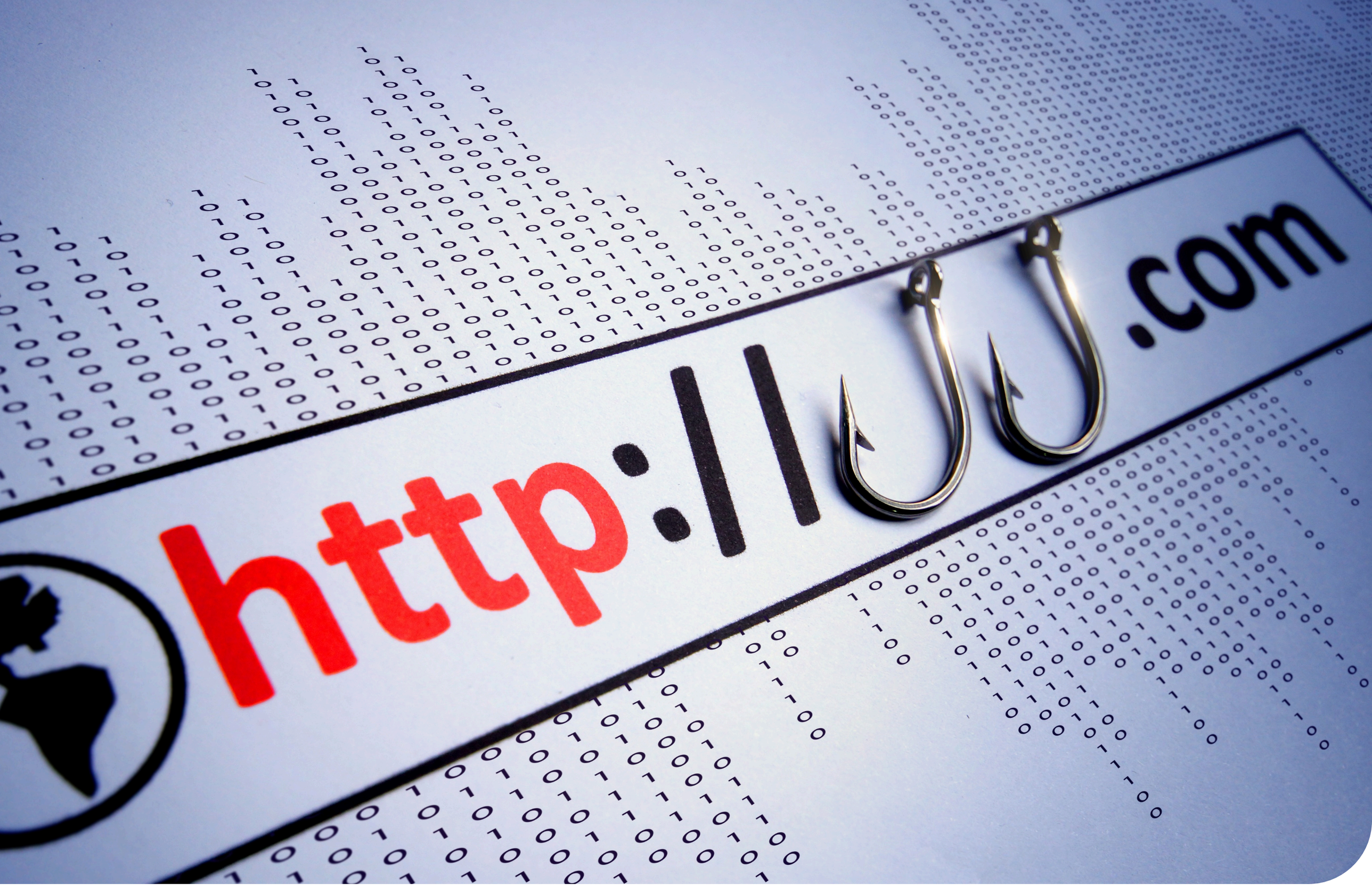
**O golpista pode solicitar também que:**

- A vítima pague sua conta de telefone ou compre um novo notebook, para que possa se comunicar com a vítima;
- Recurso financeiro para pagar um tratamento médico, seja para si mesmo ou para um familiar próximo;
- Pagar o imposto de supostos itens valiosos presos na alfândega;
- Dinheiro para concluir sua formação educacional antes de visitar a vítima.



## Como se proteger:

- Desconfie de abordagens amorosas repentinas, especialmente se envolverem solicitações de dinheiro ou informações pessoais.
- Mantenha um nível saudável de ceticismo ao interagir online com pessoas desconhecidas.
- Evite compartilhar detalhes financeiros com pessoas que você conheceu recentemente online.
- Use sites de relacionamento de boa reputação e comunique-se sempre por meio do serviço de mensagens deles. Os fraudadores querem que você mude rapidamente para SMS, redes sociais ou telefone, para que não haja evidências no site de relacionamento de que pediram dinheiro a você.
- Cuidado com mensagens exageradamente elogiosas e se você concordar em encontrar pessoalmente um pretendente, avise à familiares e aos amigos próximos.
- Cole o texto em um mecanismo de busca ou de Inteligência Artificial e veja se as mesmas palavras aparecem em sites dedicados a expor golpes de romance.




## Falsa ajuda humanitária

Os golpistas se aproveitam de crises humanitárias para aplicar golpes. Eles criam vaquinhas e chaves Pix com nomes similares aos dos verdadeiros donos para aparentar veracidade. Por exemplo: o esquema "Ajuda Humanitária aos Palestinos" infecta computadores por meio de e-mails de *phishing* ou sites maliciosos, que se disfarçam como canais legítimos de doação para causas humanitárias.

### Como acontece:

- Os golpistas se aproveitam de crises humanitárias para aplicar golpes. Eles criam vaquinhas e chaves Pix com nomes similares aos dos verdadeiros donos para aparentar veracidade. Por exemplo: o esquema "Ajuda Humanitária aos Palestinos" infecta computadores por meio de e-mails de *phishing* ou sites maliciosos, que se disfarçam como canais legítimos de doação para causas humanitárias.

### Como se proteger:

- Se receber essas mensagens, não as responda, não envie dinheiro em nenhuma moeda, nem forneça dados pessoais. Além disso, é recomendável classificar a tentativa de contato como "spam" se for feita via e-mail, ou denunciar e bloquear o usuário se a mensagem for enviada por redes sociais.

## Falso advogado

### Como acontece:

- O golpista entra em contato com as vítimas alegando que um processo está em fase final, que a advogada está no tribunal e que o cálculo do processo está pronto.
- Os criminosos **acessam o processo da pessoa na Justiça e coletam os dados**. Depois, criam uma conta em um aplicativo de conversa com a foto e o nome do advogado da vítima. Eles se passam pelo advogado, entram em contato por mensagem e **afirmam que a pessoa ganhou uma ação judicial**.
- Para convencer os clientes, os golpistas ainda **falsificam documentos**, usando até o logotipo da justiça.
- A vítima confirma essas informações por acreditar que realmente está falando com seu advogado ou com o escritório e, por vezes, deposita esses valores para ter o montante da indenização depositado em sua conta.
- Assim que conseguem a transferência, os bandidos apagam as mensagens e bloqueiam o contato da vítima.

### Como se proteger:

- Para evitar prejuízos, é importante desconfiar de solicitações de pagamento e verificar a identidade do advogado antes de qualquer transação.

## Falso leilão

O golpe do falso leilão é uma fraude online em que criminosos criam sites falsos de leilões. As vítimas são levadas a acreditar que estão comprando um bem por um preço baixo, mas acabam pagando por algo que não recebem.

### Como acontece:

- Criminosos criam sites falsos com nomes semelhantes aos de sites de leilões;
- As vítimas acessam o site falso acreditando que é o site oficial, para arrematar um suposto veículo;
- Os criminosos solicitam transferências via Pix para contas de terceiros.

### Como se proteger:

- Peça os dados do anunciante.
- Confira nome e CNPJ na internet.
- Não acredite em valores muito abaixo dos praticados pelo mercado.
- Verifique os documentos que o site de leilões envia sobre o bem.
- Verifique se existem erros de ortografia nas páginas.
- Verifique se o Pix não está sendo realizado em contas particulares.

## **Jogos de azar** (bilhete de loteria premiado)

O golpe do bilhete premiado é um crime em que o golpista apresenta um bilhete premiado na loteria. O criminoso inventa diferentes desculpas para justificar o golpe, como não saber ler ou estar sem documentos para retirar o prêmio. Outros golpistas simulam uma ligação para o gerente de um banco, que confirma o bilhete como sendo verdadeiro. É importante estar ciente desse golpe e tomar medidas para se proteger.

## **Golpe da tarefa** (renda extra)

Através de uma oferta de trabalho vantajosa, que chama a atenção pelo valor do salário e a baixa exigência de tempo e conhecimento, essa tática atrai quem quer fazer uma renda extra.

### Como acontece:

- Os criminosos divulgam a oferta em mensagens de WhatsApp, SMS, e-mails, redes sociais, anúncios na internet e alegam ser representantes de uma empresa conhecida;
- Eles sabem que a vítima tem pressa e está disposta ao que for possível para conseguir trabalho;
- Chegam a oferecer um trabalho de meio período e um alto ganho diário. Algumas propostas oferecem de R$ 300 a R$ 5.000 por dia;
- No início, a vítima recebe o pagamento das tarefas para acreditar que é um serviço confiável. Pouco tempo depois, a empresa exige o pagamento de um valor como parte da atividade e avisa que irá retornar uma quantia maior na sequência.

### Como se proteger:

- Se a vaga pede pouca experiência, poucas horas de trabalho e paga um salário muito alto, isto é um sinal de fraude.
- Desconfie de empresas que pedem para você pagar pelo exame, pagar para fazer um curso, pelo uniforme ou alegam outro motivo. Há grandes chances de ser golpe.
- Evite se cadastrar em plataformas que não conhece e desconfie de contato de grandes companhias por canais informais, como WhatsApp e redes sociais;

## Golpes envolvendo Inteligência Artificial
*(Deepfake/Criptomoedas/simuladores de voz)*

A inteligência artificial é uma **tecnologia capaz de simular o raciocínio humano e atividades realizadas por nós**, como aprendizado, tomada de decisões, compreensão da linguagem natural, reconhecimento de padrões, entre outras. Mesmo sendo desenvolvida para facilitar várias tarefas, algumas pessoas aproveitam dessa tecnologia para **aplicar golpes**.

Atualmente, é possível produzir textos, imagens, áudios e, até mesmo, videoclipes com a IA. Por conta dessas diversas possibilidades, também existem **variados tipos de golpes com Inteligência Artificial**.

Separamos a seguir as principais modalidades que você deve conhecer e ficar atento:

### *Deepfake*

- **É uma técnica que utiliza recursos de Inteligência Artificial para substituir rostos em vídeos e imagens, com o propósito de chegar o mais próximo possível da realidade**. O termo é uma mistura das expressões "*deep learning*" e "*fake*", e significa o emprego da IA para criar uma situação falsa.

- Lembra do caso do influenciador que teve sua voz recriada? Ainda que essa fraude possa ser classificada como Golpe do Pix, os criminosos usaram essa técnica para recriar a voz dele e aplicar golpes em seus familiares.

- É muito comum os golpistas também usarem imagens de pessoas influentes de um nicho para **aumentar o nível de convencimento** das informações criadas e, assim, conseguirem enganar mais vítimas. Por exemplo: usando a **imagem de um médico** para a propaganda de um remédio.

### *Vishing*

- É uma das modalidades de golpe com Inteligência Artificial. No *Vishing*, **os criminosos simulam um atendimento de serviços de telefonia ou de internet para extrair dados pessoais** como CPF, número do cartão de crédito e, até mesmo, senhas. Tudo com o objetivo de obter, de forma fraudulenta, empréstimos bancários ou cartão de crédito em seu nome.
- Para ter sucesso nessas fraudes, os golpistas usam os recursos de voz da IA para se passarem por autoridades, servidores de órgãos governamentais ou especialistas.
- Além disso, eles **criam um senso de urgência** durante essa ligação, para a vítima ficar tão receosa que nem ao menos suspeite que está sendo enganada — como o aviso de que seus dados foram vazados e você corre risco, por exemplo.

## Simuladores de Voz

- Uma das modalidades de golpe favorita dos criminosos é a que **envolve o Pix**, pois a transferência é instantânea e **mais difícil de ser recuperada pelas vítimas**.
- Essas fraudes podem acontecer de diferentes formas, mas a IA vem sendo usada para simular a voz de pessoas conhecidas, convencendo seus amigos ou familiares a realizarem transferências para a conta informada — como aconteceu com o pai de um influenciador, por exemplo.
- Isso também pode acontecer com pessoas influentes. Os criminosos usam a Inteligência Artificial para criar vídeos dessas personalidades divulgando, por exemplo, **investimentos com alta rentabilidade em Criptomoedas**.
- **Uma dica:** para evitar esse tipo de fraude, combine com seus amigos e familiares palavras de segurança caso alguém tente se passar por uma pessoa que você conhece. Assim, será possível identificar a veracidade de uma ligação ou mensagem de áudio.

## Como se proteger:

### 1. Desconfie e fique atento aos detalhes

- Ao receber uma ligação solicitando dinheiro ou suas informações pessoais, sempre desconfie. O melhor a fazer é encerrar a ligação e confirmar a veracidade de outra forma. Caso consiga pessoalmente, é a melhor opção. Afinal, no mundo real esse tipo de golpe com Inteligência Artificial não funciona!

- Além disso, fique atento aos detalhes, como um número desconhecido ou, até mesmo, a ligação de um banco em que você não possui conta.

### 2. Pense antes de tomar uma decisão

- Os golpistas usam de artimanhas para criar um senso de urgência em seus pedidos e, em muitas vezes, conseguem convencer as vítimas a abandonarem o bom senso e tomarem decisões impensadas.

- Portanto, por mais difícil que seja, **você deve respirar fundo e pensar antes de agir.**

- Faça como dissemos antes e tente confirmar aquelas informações pessoalmente antes de fazer qualquer transferência bancária ou compartilhar dados pessoais.

### 3. Conheça os golpes com Inteligência Artificial

- A melhor forma de **evitar cair em um golpe** de IA é conhecer as fraudes e entender como esses golpistas atuam.

- Então, sempre que encontrar notícias e conteúdos como esses, **separe alguns minutos para ler com atenção essas informações e aumentar seus conhecimentos sobre o assunto**.

- Com essa bagagem, será mais fácil identificar essas ações criminosas para proteger seus dados pessoais e o seu dinheiro.

## 4. Questione-se e analise contextualmente

Além de prestar atenção nos detalhes acima, ao assistir um conteúdo suspeito, questione-se:

- A situação parece exagerada ou até absurda?
- A veracidade do conteúdo foi confirmada por alguma agência de checagem de fatos ou por um veículo de comunicação confiável?
- Se o conteúdo estiver usando a imagem de uma personalidade famosa ou de uma autoridade, procure na internet outros canais que estejam comentando sobre o assunto. Com uma simples busca no Google você consegue encontrar uma notícia informando se aquele vídeo, áudio ou imagem se trata de "*deepfake*".

Outra dica importante para evitar **fraudes financeiras** entre sua família é: crie um código de segurança entre vocês. Ou seja, antes de fazer o Pix para sua filha que está desesperada precisando do dinheiro, pergunte qual o código de segurança.

# 6 Na dúvida, é só chamar!

Sempre que tiver dúvidas ou desconfiar de algo, seja por e-mail, site, SMS, telefone ou WhatsApp, entre em contato pelos nossos Canais de Atendimento oficiais:

## Site

Página oficial:
bv.com.br

Página de segurança:
bv.com.br/seguranca

Canal de Denúncias:
ri.bv.com.br/canal-de-denuncia

Portal de Transparência - LGPD:
bv.com.br/portaldetransparencia/home

## Blog

Acesse mais informações no nosso blog **BV Inspira**:
bv.com.br/bv-inspira/seguranca

## Telefones

### Clientes

Fale com um especialista pelo chat no app ou pelos números abaixo:

Atendimento 24h, todos os dias.

**3003 1616**

Capitais e demais regiões metropolitanas

**0800 701 8600**

Demais localidades

### Não clientes

Entre em contato pelo nosso SAC:

Atendimento 24h, todos os dias.

**0800 772 8028**

Conta Digital e Cartões

**0800 770 3335**

Empréstimos e Financiamentos

Lembre-se: o banco BV não pede dados importantes por telefone.

## Redes Sociais

Facebook:
facebook.com/bancobv

Instagram:
instagram.com/bancobv

X (antigo Twitter):
x.com/bancobv

TikTok:
tiktok.com/@bancobv

LinkedIn:
linkedin.com/company/bancobv

Spotify:
spotify.com/bancobv

Dica bônus:

# 7 Sua Segurança é da nossa conta

Conhecer bem as redes sociais e suas ferramentas pode te ajudar na identificação de possíveis ataques e na proteção dos seus dados. Por isso, separamos algumas dicas que podem melhorar a segurança das suas informações e acessos, além de reduzir a criação de perfis falsos.

## Facebook

• Evite divulgar quem são os membros da sua família (mãe, pai, filhos e irmãos).

• Escolha uma senha difícil, troque-a de tempos em tempos e não compartilhe com ninguém.

• Deixe suas postagens, fotos e perfil privados apenas para seus amigos.

• Não faça publicações com informações importantes ou sensíveis. Se for realmente necessário, publique no modo privado.

• Não aceite solicitações de amizade ou mensagens de pessoas que você não conhece. Verifique se o perfil de seus conhecidos é realmente o verdadeiro.

• Você sempre tem a opção de denunciar perfis e publicações suspeitas.

• Ative sua autenticação de dois fatores:

- Acesse suas configurações
- Vá na opção "Senha e segurança"
- Entre na opção "Autenticação de dois fatores"
- Escolha o melhor método de segurança para você

## Instagram

• Deixe sua conta privada.

• Escolha uma senha difícil, troque-a de tempos em tempos e não compartilhe com ninguém.

• Bloqueie contas suspeitas.

• Verifique a atividade de login, que mostra onde, quando e em quais dispositivos sua conta foi acessada.

• Ative sua autenticação de dois fatores:

- Entre nas suas configurações
- Selecione a opção "Segurança"
- Entre na opção “Autenticação de dois fatores”
- Escolha por onde quer receber seus códigos de segurança

### X (antigo Twitter)

• Escolha uma senha difícil, troque-a de tempos em tempos e não compartilhe com ninguém. É importante usar senhas diferentes para cada rede social.

• Cadastre um e-mail e um número de telefone de segurança.

• Não acesse links desconhecidos ou suspeitos.

• Use a autenticação em duas etapas:

- Entre nas suas configurações de privacidade
- Selecione "Segurança e acesso à conta"
- Clique em "Autenticação em duas etapas"
- Escolha o método de segurança que preferir

---

### LinkedIn

• Confira suas sessões ativas, com local e dispositivo que teve acesso à sua conta.

• Gerencie seus dados e atividades dentro do aplicativo na opção "Privacidade dos Dados".

• Configure quem pode ver seus dados, como e-mail e sobrenome. Além disso, há uma opção para limitar a visibilidade do seu perfil fora do LinkedIn.

• Bloqueie pessoas e perfis suspeitos.

• Ative sua verificação em duas etapas:

- Entre nas Configurações
- Selecione "Acesso e segurança"
- Acesse a opção "Verificação em duas etapas"
- Escolha a forma de verificação que preferir

---

### WhatsApp

• Configure a foto de perfil apenas para seus contatos.

• Não envie o código de confirmação do seu acesso para ninguém (normalmente enviado por SMS).

• Bloqueie números suspeitos.

• Não baixe fotos, áudios ou arquivos enviados por desconhecidos.

• Ative a confirmação em duas etapas:

- Entre nas Configurações
- Escolha a opção "Conta"
- Clique em "Confirmação em duas etapas"
- Coloque seu e-mail e crie uma senha PIN

---

### Telegram

• Gerencie suas sessões em todos os dispositivos.

• Escolha quem pode te adicionar em grupos e canais.

• Escolha quem pode ver suas informações, como foto de perfil e número.

• Crie uma senha de bloqueio, para bloquear e desbloquear o app quando quiser.

• Ative a verificação em duas etapas:

- Entre nas Configurações
- Escolha a opção "Privacidade e Segurança"
- Crie sua senha adicional

## Roubo de celular – como agir e se proteger

Outra dica importante é como configurar seu aparelho para que ele fique mais seguro:

• Ative o bloqueio temporário do seu aparelho celular, estipule um tempo curto para o bloqueio de tela.

• Altere suas senhas regulamente.

• Cadastre uma senha PIN no chip do seu celular.

• Busque desativar a função “Preencher senha” e sempre verifique o status das “Recomendações de segurança” do aparelho.

• Tenha com você o código IMEI do celular e guarde ele de forma segura.

• Habilite o rastreio do celular, caso necessite apagar os dados do aparelho ou localizá-lo remotamente.

• Evite salvar suas senhas de apps ou de bancos no celular e evite, também, salvar fotos de seus documentos.

• Procure por aplicativos que gerem senhas para abrir cada app ou ative o reconhecimento facial e biométrico sempre que possível.

---

**Agora, se seu celular foi roubado/furtado, siga esses passos:**

• Faça o bloqueio do aparelho e do chip junto à sua operadora de celular.

• Na sua loja de aplicativos, baixe o app Celular Seguro, aplicativo do Governo junto com o Ministério da Justiça, faça o login com a sua conta gov.br e cadastre os dados do seu aparelho. Em caso de perda, furto ou roubo, registre uma ocorrência no site ou app do Celular Seguro.

• Comunique seu banco sobre sua conta e peça o cancelamento de cartões.

• Se não puder usar o app, acesse os sites dos aplicativos pelo computador e altere as senhas de e-mails, redes sociais e demais aplicativos.

• Avise amigos e parentes próximos sobre o roubo/furto e peça para que não respondam
a contatos ou mensagens suspeitas.

• Registre um boletim de ocorrência e compartilhe com os bancos e a sua operadora telefônica.

banco