



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

Preparando você para ter segurança em  
todos os momentos da sua vida!

# 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**. Pensando nisso, 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?**



# O que você vai ver aqui?



- 1 O que são golpes financeiros?
- 2 Dicas úteis para sua proteção pessoal
- 3 O que o banco BV não faz
- 4 Caí no golpe. E agora?
- 5 Tipos de golpes e fraudes
  - a) **Golpes para roubar suas informações**
    - E-mail e SMS falsos que possuem links para sites enganosos
    - Golpe da Mão Fantasma
    - Golpes no WhatsApp
    - Golpe da Falsa Central de Atendimento
  - b) **Golpes do cartão de crédito**
    - Golpe do falso motoboy
    - Golpe do falso delivery
    - Golpe do brinde/presente de aniversário.
  - c) **Golpes da conta**
    - Golpe do falso funcionário
    - Golpes do Pix
  - d) **Outros golpes comuns**
    - Empréstimo falso
    - Boleto falso
    - Golpe do FGTS
    - Golpe com anúncios falsos (sites/e-commerce)
    - Golpe do amor
    - Falso Investimento
- 6 Nossos canais oficiais
- 7 Dicas 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?

**Golpe financeiro ou ações de engenharia social são esquemas pensados para levar seu dinheiro e seus dados.**





Para isso, os golpistas sempre tentam conquistar seu interesse e confiança, normalmente, por meio de promessas e oportunidades que parecem imperdíveis, mas que são falsas.

Sabe aquele investimento que promete um mega retorno? Ou aquela promoção que parece boa demais para ser verdade?

**Cuidado! Realmente, pode ser tudo mentira.**





# Mas como um golpe chega até mim?

Existem muitas formas que fraudadores podem utilizar para enganar você, 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 acessar seus dados do banco.

### **Lembre-se!**

As mensagens falsas **podem se passar pelo banco BV trazendo situações comuns**, como atualização de senha, bloqueio do cartão de crédito e ofertas especiais.

# Você sabia?

Praticamente, **8** em cada **10** transações bancárias são digitais.

Por meio de mobile banking, internet banking ou WhatsApp.

Fonte: Febraban Tecnologia Bancária.

Empresas de segurança bloquearam quase

**3,4 milhões**  
de tentativas de golpes financeiros em 2021.



o equivalente a mais de

**22,5 mil** / **930**  
por dia por hora

Fonte: PSafe — aplicativo de segurança para aparelhos móveis.

Ao mesmo tempo:

**Aumentou quase 90%**  
a quantidade de contas abertas on-line durante a pandemia.

Fonte: Federação Brasileira de Bancos (Febraban).

Mesmo que as instituições financeiras adotem medidas de segurança, o número de golpes cresceu muito 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, SMS ou redes sociais, pois em caso de extravio do seu celular, um fraudador poderá se 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.**

**Atendimento 24 horas, todos os dias.**

- 3003 7728 (capitais e demais regiões metropolitanas) 0800 777 2828 (demais localidades)

**SAC - Serviço de Apoio ao Consumidor Para sugestões, cancelamentos, reclamações e informações gerais sobre produtos e serviços, 24 horas, 7 dias por semana.**

- 0800 772 8028 0800 771 0755 (para pessoas com deficiência auditiva e de fala)

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

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

- 4 **Evite abrir documentos recebidos de pessoas desconhecidas no WhatsApp.** Caso a mensagem seja de alguém conhecido que não costuma enviar arquivos, vale a pena fazer uma ligação para confirmar a intenção.
  
- 5 **Não responda mensagens de empresas desconhecidas** oferecendo benefícios que você não solicitou e que são fáceis demais.

#### **/ 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 cadastros e senhas ou desbloquear contas.
- 7 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 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 e verificar perfis e sites falsos do banco BV na internet.



## Realize 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.

Se seu celular foi roubado, apague remotamente dados que estão nele e avise sua operadora, pedindo para bloquear sua linha 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-mails e SMS falsos**

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

#### **Como acontece:**

- Fraudadores enviam mensagens por e-mail, WhatsApp 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, indicando, 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 via SMS com atenção e desconfie de pedidos estranhos, como produtos ou serviços milagrosos.
- 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 botão e confira se faz sentido com a suposta empresa.
- Desconfie de endereços de e-mails terminados em ".com" e sem ".br".
- Todos os aplicativos de e-mail possuem recursos para Relatar a Mensagem com 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 no WhatsApp

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 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, 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 (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 se realmente é a pessoa que está pedindo (por chamada de voz ou vídeo).



#### 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 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 escritórios e usam falas muito convincentes.

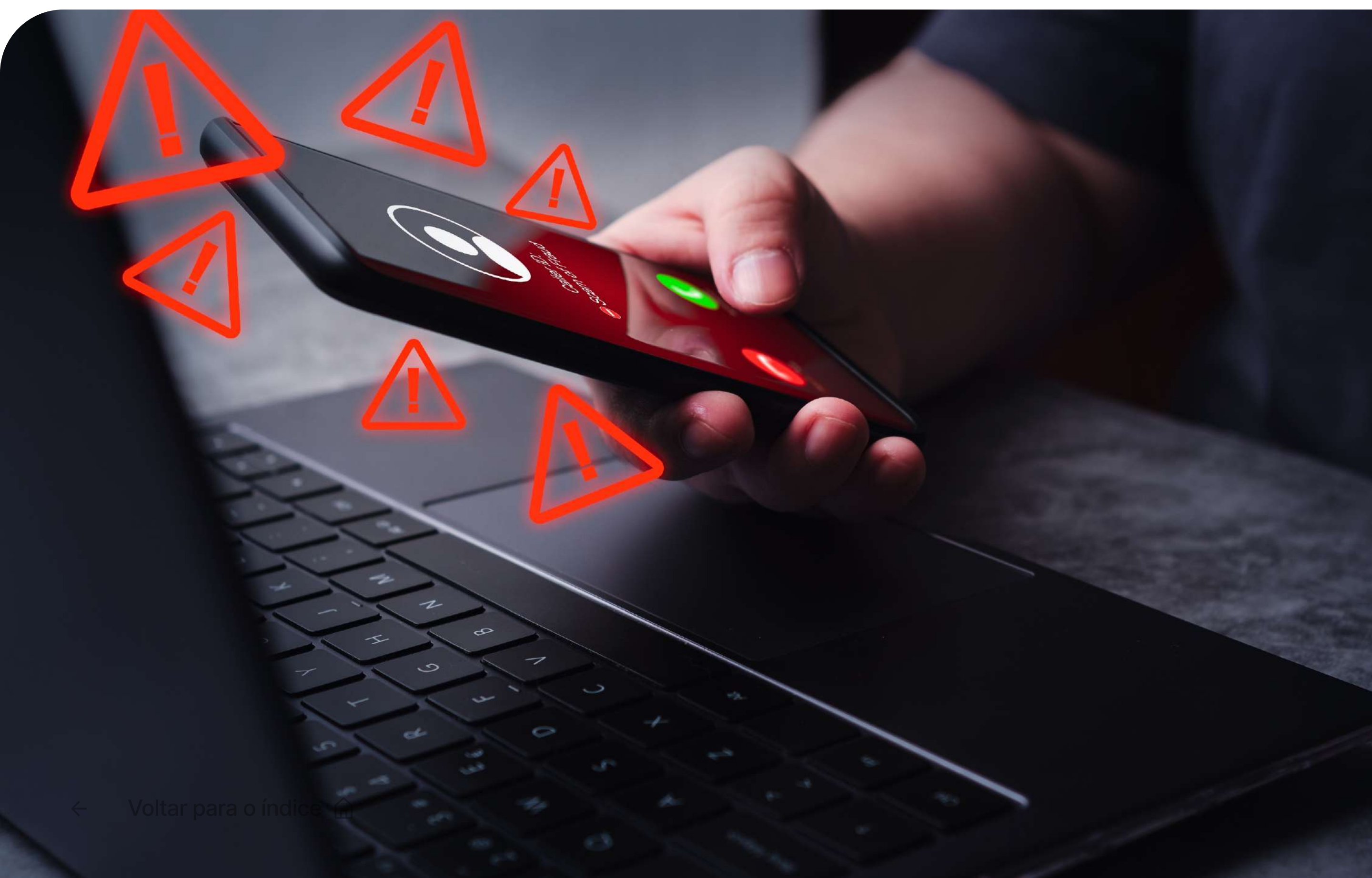
### **Como acontece:**

#### **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 informam que sua conta bancária ou 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 para enganar amigos e familiares.

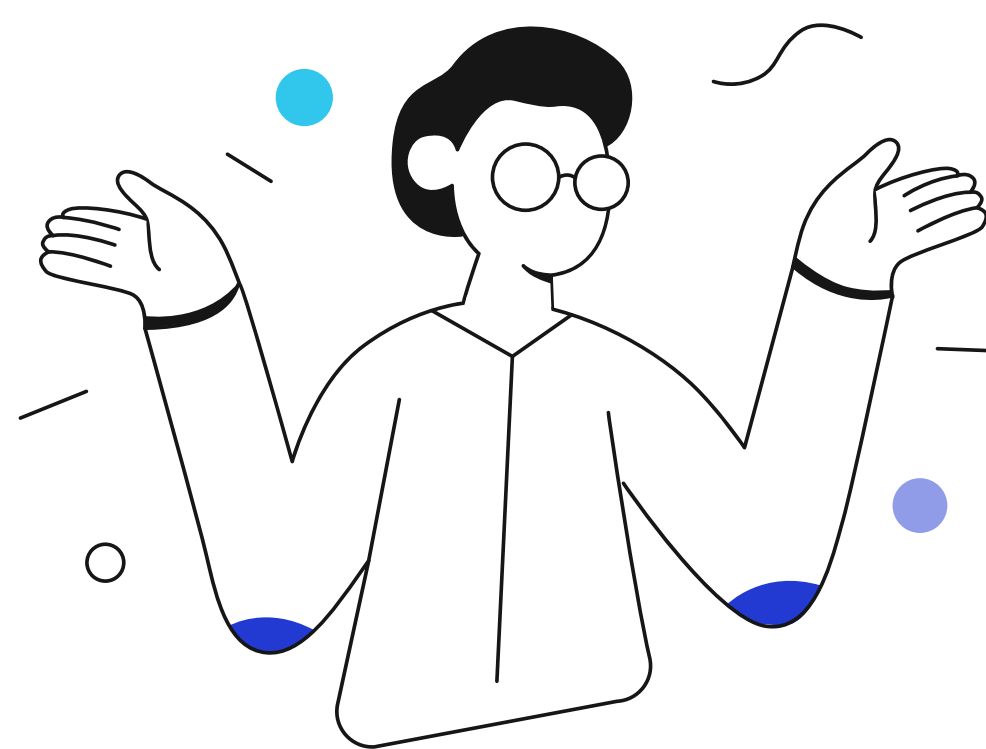
### **Como se proteger:**

- Nós **nunca pedimos senhas** por telefone, 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**.



## B Golpes do 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

#### Como acontece:

- O golpista entra em contato com você como se fosse um funcionário do banco, diz que houve uma compra duvidosa e pede para você ligar no número que fica no verso do cartão.
- 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 nos canais de atendimento. Assim, não tem o 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.
- 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 do aparelho estiver quebrada ou coberta de alguma forma.



## Golpe do brinde/presente de aniversário

Ganhou um presente ou brinde inesperado? Pode ser golpe.

### Como acontece:

#### a) Invasão da conta

- O golpista se apresenta como entregador e te aborda para deixar um brinde/presente.
- Para realizar a entrega, o golpista solicita dados pessoais e uma foto do seu rosto.
- Geralmente, eles fazem as entregas em datas especiais, como aniversários.
- Esse tipo de ação também pode acontecer no ambiente virtual, quando solicitam seus dados por aplicativos de mensagens ou redes sociais.

### Como se proteger:

- O banco BV não pede fotos do seu rosto, documentos ou o número do seu celular para fazer entregas.
- Contate o remetente e confirme se o estabelecimento te enviou algum brinde.
- Nunca informe seus dados bancários e informações pessoais.
- Não aceite que tirem fotos dos seus documentos ou do seu rosto com o aparelho do entregador.



## **Golpes na conta**

A conta corrente é uma das formas mais simples e práticas para você guardar e movimentar 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 padrões dos bancos. Veja como evitar esse tipo de golpe.

#### **Como acontece:**

- O golpista entra em contato com você, normalmente, por telefone ou WhatsApp, e diz que é um funcionário do banco.
- Durante a conversa, ele apresenta algum tipo de falsa solução por meio do envio de 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 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 do 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.
- 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 nova 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.
- 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 realizado.

### **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:**

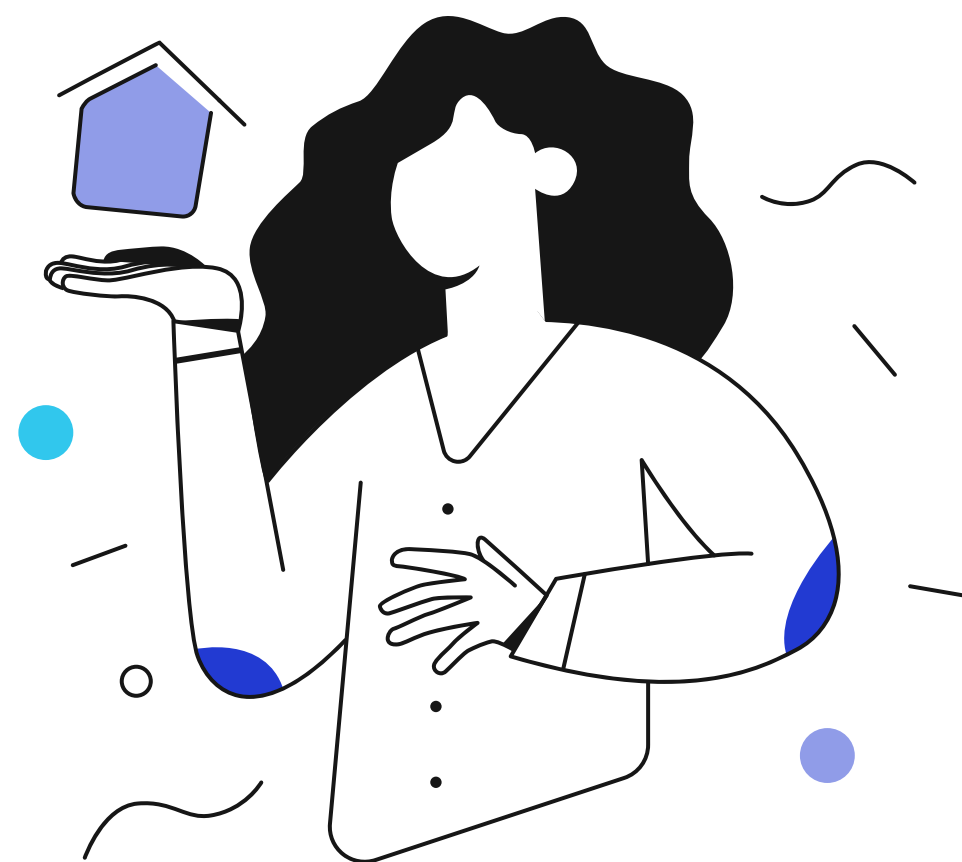
Funcionários e representantes do banco BV não ligam para os clientes para fazer cadastros e testes do Pix.

## D Outras 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 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. Veja como funciona.



#### Como acontece:

- O golpista oferece empréstimos com condições supervantajosas 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 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 pagamento de taxas.
- Pesquise se a empresa é parceira do banco BV. Verifique informações, como 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 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 é feito somente em aplicativos e sites oficiais.



#### Lembre-se:

criminosos dizem que o empréstimo foi aprovado e que é preciso pagar antecipadamente para concluir a negociação. Não acredite nisso.

## **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.
- É informado 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 do boleto. Os 3 primeiros dígitos devem ser iguais ao número do banco (o número do banco BV é 413 e 655), e os últimos, 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**

CNPJ 01.149.953/0001-89

**Banco Votorantim S.A.**

CNPJ 59.588.111/0001-03

**Banco BV S.A.**

CNPJ 01.858.774/0001-10

- Evite pagar boletos recebidos por correio. Se você é cliente de financiamento de veículos ou 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 Minha BV em [www.bv.com.br](http://www.bv.com.br).
- Utilize o DDA (Débito Direto Autorizado), que é 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.



**Lembre-se:**

O banco BV tem um validador de boletos, onde você pode verificar se eles são verdadeiros de um jeito simples. Acesse: [bv.com.br/boleto](http://bv.com.br/boleto).

## Golpe do FGTS

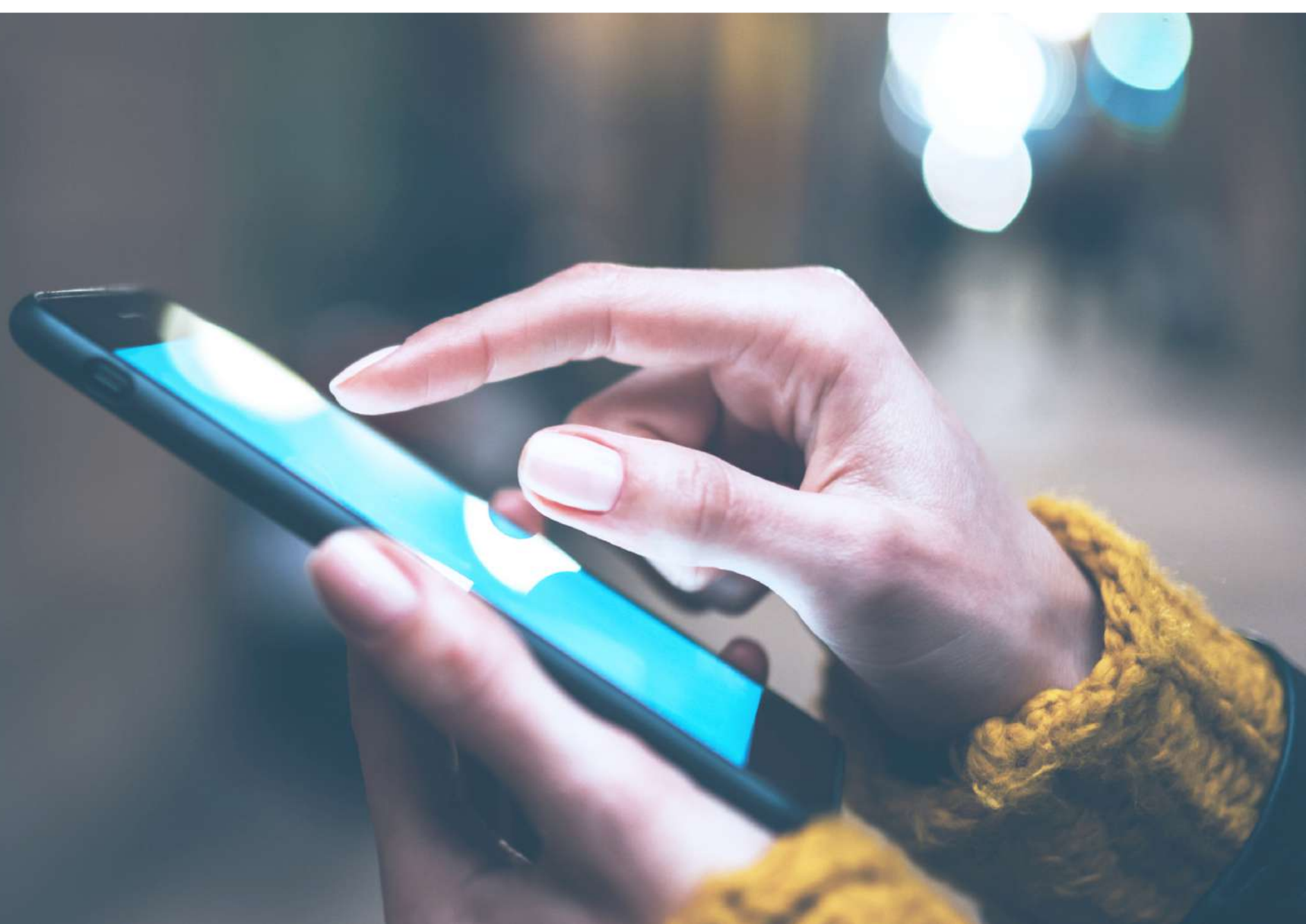
Nem seu FGTS fica livre dos olhos de golpistas. Confira como funciona e como proteger seu dinheiro.

### 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 pelos golpistas 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 com Anúncios Falsos (sites/e-commerce)**

Saiba se preparar quando for buscar descontos e promoções em compras on-line. É importante estar seguro e desconfiar de ofertas com valores fora da realidade. Veja as nossas dicas.

### **Como se proteger:**

- Acompanhe suas compras recentes e assim evite surpresas negativas;
- Busque utilizar seu cartão virtual para compras pela internet e, assim, tenha mais segurança e menos chances de fraudes.
- Consulte sempre sua fatura antes do fechamento e assim você consegue se programar e ter mais controle com suas finanças.

## **Golpe do Amor**

Aplicativos de relacionamento e golpes: saiba mais para se cair nessa abordagem.

### **Como se proteger:**

- Não compartilhe seus dados pessoais com pessoas desconhecidas, e atenção também com suas informações nos acessos aos Apps de relacionamento, golpistas do amor costumam usar dados de suas vítimas para diversos tipos de fraudes.
- Não é recomendado compartilhar detalhes e informações de sua rotina diária, fotos íntimas em aplicativos de namoro.
- Antes de iniciar uma conversa, busque verificar se o perfil é real. Fique atento às imagens e à escrita da conversa. Vale a pena realizar uma pesquisa de perfil em outras redes sociais.
- Evite responder perfis sem fotos.
- Outra dica é pesquisar a foto do perfil usando a busca reversa do Google – para encontrar imagens duplicadas.

## **Falso Investimento**

Saiba se prevenir também quando for buscar investir seus recursos: golpistas prometem rendimentos altos fora da realidade. Veja as nossas dicas.

### **Como se proteger:**

- Faça seus investimentos com o seu banco de confiança ou com empresas confiáveis com registro no banco central.
- Fique atento com falsos consultores com promessas de retorno muito acima das que são praticadas pelo mercado financeiro.
- Busque consultores certificados.
- Cuidado com as propagandas divulgadas em redes sociais, principalmente, atenção com pirâmides financeiras.



# 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 oficiais de atendimento:

## Site

Página oficial:  
[bv.com.br](http://bv.com.br)

Página de segurança:  
[bv.com.br/seguranca](http://bv.com.br/seguranca)

## Blog

Acesse mais informações no nosso blog **BV Inspira**:  
[bv.com.br/bv-inspira/seguranca](http://bv.com.br/bv-inspira/seguranca)

## Redes Sociais

Facebook:  
[facebook.com/bancobv](https://facebook.com/bancobv)

Instagram:  
[instagram.com/bancobv](https://instagram.com/bancobv)

Twitter:  
[twitter.com/bancobv](https://twitter.com/bancobv)

TikTok:  
[tiktok.com/@bancobv](https://tiktok.com/@bancobv)

LinkedIn:  
[linkedin.com/company/bancobv](https://linkedin.com/company/bancobv)

Spotify:  
[spotify.com/bancobv](https://spotify.com/bancobv)

## Telefones

Se você já é nosso cliente e quer solicitar um serviço ou obter informações sobre seu contrato, ligue, de 2ª a 6ª, das 7h às 22hs, para:

**3003 1616**

Capitais e demais regiões metropolitanas

**0800 701 8600**

Demais localidades

Para sugestões, cancelamentos, reclamações e informações gerais, ligue, 24 horas por dia, 7 dias por semana, para:

**0800 770 3335**

**0800 701 8661**

Atendimento especial para pessoas com deficiência auditiva e de fala.

Dicas bônus:

# 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 aceitar conexões com pessoas desconhecidas.
- 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 ela 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 ou até publicações suspeitas.
- Ative sua autenticação de dois fatores:
  - Acesse suas configurações
  - Vá na opção "Senha e segurança"
  - Entre na "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 ela 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 "Autenticação de dois fatores"
  - Escolha por onde quer receber seus códigos de segurança

## **Twitter**

- Escolha uma senha difícil, troque-a de tempos em tempos e não compartilhe ela com ninguém. É importante usar senhas diferentes para cada rede social.
  - Cadastre um e-mail e número de telefone de segurança.
  - Não acesse links desconhecidos ou suspeitos.
  - Use a autenticação em duas etapas:
    - Entre nas suas configurações e 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 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 regularmente.
- Cadastre uma senha PIN do 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, guarde ele de forma segura.
- Habilite o rastreamento do celular, caso necessite apagar os dados do aparelho e para localizá-lo remotamente.
- Evite salvar suas senhas de apps ou de bancos no celular e evite, também, salvar fotos de seus documentos.
- Procure aplicativos que gerem senhas para abrir cada aplicativo ou ative o Face ID em todos os possíveis.

---

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

- Faça o bloqueio do aparelho e o simcard (chip) junto a sua operadora de celular.
- Comunique seu banco sobre sua conta e peça o cancelamento de cartões.
- Avise amigos e parentes próximos sobre o furto e avise para não responderem a contatos ou mensagens suspeitas.
- Registre um boletim de ocorrência e informe os bancos e sua operadora.
- Modifique suas senhas de e-mails, redes sociais e apps.

