



Guia de segurança

A gente faz de tudo pra
te alertar e te proteger.





Aqui, você fica por dentro das nossas **soluções** para ter mais segurança, confere **dicas** importantes para o seu dia a dia e conhece os principais **golpes** financeiros do momento. Tudo para você se proteger e não se tornar uma vítima de fraudes.



A gente faz de tudo pra te alertar e te proteger.





Mandamentos da Segurança

1. Não compartilhe senhas com ninguém.
2. Escolha senhas difíceis de adivinhar.
3. Utilize sempre o domínio oficial do BB
www.bb.com.br
4. Desconfie de links recebidos por e-mail, SMS e redes sociais.
5. Evite usar redes wi-fi públicas ou serviços de VPN gratuitos.
6. Mantenha o antivírus instalado e atualizado.
7. Baixe aplicativos apenas de lojas oficiais.
8. Seu cartão não deve ser entregue a ninguém.
9. Antes de emprestar dinheiro solicitado por mensagem, ligue e confirme com quem pediu.
10. Confira sempre o destinatário antes de fazer uma transferência, Pix ou pagamento.



A gente faz de tudo pra te alertar e te proteger.





Soluções do Banco do Brasil

Conheça as nossas soluções para deixar os seus dados e o seu dinheiro sempre seguros.

Biometria

Um dos modos mais seguros de autenticação de transações financeiras, a biometria utiliza a impressão digital para validar a sua identidade.

BB Code

Agrega segurança ao utilizar a tecnologia QR Code para autorizar suas transações financeiras realizadas na Internet.

Cadastramento de dispositivos

Fornece maior comodidade para você movimentar a sua conta em computadores, tablets e smartphones.

Central de Senhas

Permite mais agilidade para você bloquear, desbloquear ou alterar as suas senhas pelo App BB.

Limites de Movimentação

Oferece a possibilidade de ajustar seus limites de acordo com cada canal (caixa eletrônico, celular ou computador, por exemplo) e conforme a sua necessidade.

BOT BB no WhatsApp

Basta digitar #segurança que o nosso assistente virtual iniciará uma conversa sobre o tema!

saiba mais



A gente faz de tudo pra te alertar e te proteger.





Conheça os principais golpes financeiros e saiba como se proteger.



Clique nos ícones para interagir

Phishing,
Smishing
e Vishing

Golpe da
falsa central de
atendimento

Golpes do
WhatsApp

Golpe do falso
motoboy

Golpe da
maquininha
quebrada

Golpe do
cadastramento
Pix

Golpe da
liberação de
dispositivos

Golpe
da troca
de cartões

Golpe do
falso boleto

Golpe
da mão
fantasma

Golpe
do bilhete
premiado

Golpe do
SMS com
pontos de
fidelidade



A gente faz de tudo pra
te alertar e te proteger.





Phishing, smishing, vishing



Como funciona:

Os golpistas, assim como na pesca, lançam uma isca, por e-mail, SMS, ligação telefônica, falso site ou falso pop-up inserido em sites desprotegidos. Utilizam-se de ofertas “imperdíveis” ou mensagens com senso de urgência e solicitam que você realize alguma ação, como abrir um link ou arquivo, fazer uma ligação ou instalar/atualizar um software específico.

O que fazer para não se tornar uma vítima:

Não clique em links ou em e-mails com ofertas muito lucrativas, em mensagens com senso de urgência e/ou com ameaças como "seu serviço será suspenso se..." ou "sua conta foi bloqueada...".

Não abra e-mails ou clique em anexos ou links enviados por desconhecidos.

Caso suspeite de um site ou mensagem em nome do BB, encaminhe as informações para abuse@bb.com.br.

Não repasse códigos de identificação enviados por SMS ou imagens do QR Code.

Na dúvida, fale com um dos nossos canais oficiais.



A gente faz de tudo pra te alertar e te proteger.





Golpe da falsa central de atendimento



Como funciona:

Golpistas fingem ser da nossa Central de Atendimento, simulam o número de telefone do Banco e usam recursos tecnológicos, como gravações e menus para aumentar a sua confiança, solicitam senhas, atualização de sistemas ou liberação de equipamentos.

Muitas vezes, durante o “atendimento”, são repassados endereços eletrônicos falsos, como “bbsuporte”, “bbrelacionamento” e “bbatendimento”, induzindo o cliente a digitar seus dados de segurança e acesso à conta.

O que fazer para não se tornar uma vítima:

O BB nunca solicita atualização e/ou cadastramento de módulo de segurança, computadores, celulares ou senhas e nem a instalação de softwares, aplicativos e componentes em navegadores via telefone.

Sempre acesse o BB pelo domínio (<https://bb.com.br>).

Lembre-se: o telefone 4004-0001 é um número para você ligar para nossa Central. O BB não realiza ligações a partir desse número.



A gente faz de tudo pra te alertar e te proteger.





Golpes do WhatsApp



Como funciona:

Existem dois tipos de golpes mais comuns:

1. Golpistas clonam o WhatsApp e se passam por conhecidos e familiares para pedir dinheiro emprestado.
2. Golpistas conseguem sua foto e um número de celular de algum contato, criam um perfil falso e mandam mensagem a esse conhecido comunicando a troca de número por algum problema. Depois, pedem dinheiro emprestado como se estivessem em alguma emergência.

O que fazer para não se tornar uma vítima:

Desconfie de contas com fotos de conhecidos, mas números diferentes.

Não faça transferências ou pagamentos por solicitação feita apenas por mensagens, sobretudo se o destinatário for uma terceira pessoa.

Ative no aplicativo de mensagens a opção de verificação em duas etapas e permissão para que apenas os seus contatos tenham acesso à sua foto de perfil.

(Configurações/Ajustes > Conta > Confirmação em duas etapas > Ativar)

(Configurações/Ajustes > Conta > Privacidade > Foto do perfil > Meus contatos.

Antes de transferir qualquer valor, ligue e confirme diretamente com o solicitante. Precaução antes de tudo.



A gente faz de tudo pra te alertar e te proteger.





Golpe do falso motoboy



Como funciona:

O golpista liga para seu telefone fixo se passando por funcionário do Banco, e faz você acreditar que seu cartão foi clonado. Em seguida, é solicitado que você ligue imediatamente no telefone disponível no verso do cartão.

A ligação supostamente é encerrada, porém, o golpista permanece na linha telefônica. Ao ligar para a Central de Atendimento, o golpista que permaneceu na linha simula o atendimento da Central de Atendimento. Solicita, então, dados, senha e orienta que o cartão seja cortado ao meio e entregue a um motoboy que irá até a residência.

O que fazer para não se tornar uma vítima:

Não entregue o seu cartão a ninguém, nem mesmo se estiver quebrado. O BB não envia motoboy para recolhimento de cartão. Caso desconfie da ligação, desligue o telefone e retorne para a Central de Atendimento BB por outro número de telefone.



A gente faz de tudo pra te alertar e te proteger.





Golpe da maquininha quebrada



Como funciona:

O golpe acontece principalmente em serviços de entrega de comida por delivery. O golpista cobra um valor maior do que seria o pagamento utilizando uma maquininha de cartão com o visor quebrado ou danificado.

O que fazer para não se tornar uma vítima:

Prefira pagar diretamente pelos aplicativos de entrega. Suspeite de cobranças adicionais no momento da entrega. Não aceite realizar pagamentos em maquininhas com visor quebrado ou danificado.

Ative o serviço de SMS para receber notificações de pagamentos.



A gente faz de tudo pra te alertar e te proteger.





Golpe do cadastro Pix



Como funciona:

Golpistas fingem ser de instituições financeiras para solicitar um suposto cadastro da chave Pix em sites falsos.

O que fazer para não se tornar uma vítima:

Desconfie de links recebidos por e-mail, SMS ou WhatsApp com convites para cadastramento de suas chaves Pix.

Cadastre suas chaves nos canais oficiais do Banco.

Não faça transações a pedido de terceiros para suposto teste de suas chaves.

Não compartilhe códigos de verificação recebidos por e-mail ou SMS no momento do cadastro das chaves Pix. Cadastre sua chave aleatória caso você não esteja seguro de fornecer seus dados de CPF, telefone ou e-mail ao receber um pagamento Pix.



A gente faz de tudo pra te alertar e te proteger.





Golpe da liberação de dispositivos



Como funciona:

O golpista finge ser funcionário do Banco, e por contato telefônico ou WhatsApp, cria um senso de urgência sob o argumento de fraude ou de restrições/bloqueios diversos e pede para que você compareça ao caixa eletrônico.

Ao chegar na agência, em frente ao terminal, o golpista diz para você tirar fotos ou filmar a tela do TAA, permitindo a visualização do QR CODE para autorização de celular ou computador, habilitação do BB CODE ou alteração de limites e senhas.

O que fazer para não se tornar uma vítima:

Desconfie! O BB não liga para pedir senhas, habilitação de BB Code e nem para liberar ou atualizar computadores e celulares.

Não tire foto e nem faça vídeo das telas do TAA.

O QR Code não deve ser compartilhado com ninguém.



A gente faz de tudo pra te alertar e te proteger.





Golpe da troca de cartões



Como funciona:

O golpista fica de olho na sua senha enquanto você usa a maquininha de pagamento. Depois da transação, devolvem a você um outro cartão parecido, mas que não é o seu.

Abordagens também podem ocorrer a pessoas com dificuldades nos caixas eletrônicos. O golpista, fingindo auxiliar na transação, realiza transações indevidas nas contas das vítimas, ou observa a digitação da sua senha e no final troca o seu cartão por outro.

O que fazer para não se tornar uma vítima:

Não entregue o cartão ao vendedor ao realizar um pagamento. Insira você o cartão na maquininha e o mantenha sempre sob supervisão. Caso isso não aconteça, verifique se o cartão devolvido é realmente o seu. Fique atento a olhares curiosos e verifique se está digitando a senha no campo correto.

Não aceite ajuda de estranhos nos caixas eletrônicos. Em caso de dificuldades, solicite ajuda de um funcionário do Banco devidamente identificado ou o auxílio de uma pessoa de confiança.



A gente faz de tudo pra te alertar e te proteger.





Golpe do falso boleto



Como funciona:

Golpistas falsificam cobranças em boleto para fazer com que o pagamento vá para outros beneficiários em vez de quitar sua despesa.

O que fazer para não se tornar uma vítima:

Cuidado com boletos enviados por e-mail, redes sociais ou SMS. Desconfie de boletos com erros ortográficos, manchas ou borrões na impressão.

Confira as informações que aparecem no boleto.

Verifique se os seus dados e os do recebedor estão corretos.

Confira o CPF ou o CNPJ do emissor, data de vencimento, o valor e se os três primeiros números do código de barras são do banco emissor. Um boleto do Banco do Brasil sempre começará com 001.



A gente faz de tudo pra te alertar e te proteger.





Golpe da mão fantasma



Como funciona:

O golpista entra em contato por telefone, se passando por uma falsa central do banco e induz a instalar um aplicativo, que sem que você perceba, possibilita a visualização e o controle do celular de forma remota.

Assim, o criminoso consegue acessar visualizar e operar o celular remotamente, tendo acesso a absolutamente tudo que existe nele, incluindo seus dados bancários.

O que fazer para não se tornar uma vítima:

O BB não liga solicitando a instalação de aplicativos. Não instale aplicativos desconhecidos em seu celular.

Caso receba uma ligação de suposto funcionário do BB com essa solicitação, desligue imediatamente e entre em contato por um dos nossos canais oficiais.



A gente faz de tudo pra te alertar e te proteger.





Golpe do bilhete premiado



Como funciona:

O golpe não utiliza nenhum tipo de tecnologia, apenas a engenharia social, na qual a vítima é ludibriada para que realize ações que contribuem para a efetivação do golpe. Os idosos são as principais vítimas.

O golpista apresenta um falso bilhete de loteria premiado e inicia uma dramatização dizendo que não pode ou que não consegue retirar o prêmio. Demonstrando uma necessidade urgente para resolver a situação, solicita ajuda para retirar o prêmio em troca de parte do valor ou oferece a venda do bilhete por um valor inferior ao do suposto prêmio.

Como garantia, em troca do bilhete, é solicitado da vítima, que entregue objetos que esteja portando, como colar, brincos ou relógio e/ou é solicitado a realização de transferências ou valores em espécie.

O que fazer para não se tornar uma vítima:

Desconfie de promessas de dinheiro fácil e rápido. Evite dar abertura para conversa a estranhos na rua, principalmente em relação a questões que envolvam dinheiro. Não saque e nem transfira valores para desconhecidos.



A gente faz de tudo pra te alertar e te proteger.





Golpe do SMS com pontos de fidelidade



Como funciona:

Golpistas vêm se passando por instituições financeiras, enviando SMS com supostos pontos de fidelidade expirando ou que a pessoa ganhou sem saber. Junto ao conteúdo falso, enviam links suspeitos para clientes, que são direcionados a uma página fake.

A partir daí, as vítimas são induzidas a preencher dados, como CPF, número da agência bancária e até a senha do cartão ou do aplicativo do Banco.

O que fazer para não se tornar uma vítima:

Fique de olho: o BB não encaminha esse tipo de SMS, e programas de fidelidade não enviam SMS pedindo informações bancárias. Caso você receba alguma mensagem suspeita, encaminhe gratuitamente via celular para o número 7726 ou para o e-mail abuse@bb.com.br.



A gente faz de tudo pra te alertar e te proteger.





Falar sobre segurança nunca é demais, por isso, a gente tem uma última dica: compartilhe este Guia com todo mundo.

Essas informações podem ajudar na prevenção de golpes, na proteção de informações pessoais e na segurança das suas transações.

Contamos com a sua ajuda.



A gente faz de tudo pra te alertar e te proteger.





Pra tudo
que você
imaginar

Siga a gente nas Redes Sociais

