Guia de Segurança:

Entenda como se proteger dos principais tipos de golpes do mercado bancário.

Safra

Sumário

No Safra, a segurança é um valor inegociável no relacionamento com o cliente. Para isso, compartilhar informações e conscientizar o próximo é fundamental.

Aqui estão algumas dicas de segurança para que você possa identificar as principais modalidades de golpes ativas no sistema bancário:

Golpe da Falsa Central

Ao telefone, o criminoso diz ser um funcionário do banco no qual a vítima possui conta. Ele oferece ajuda para o cadastro da chave Pix ou orienta um teste para regularizar o cadastro já existente, induzindo a vítima a fazer a transferência para o criminoso.

Em outra modalidade, o criminoso diz que a conta está com problemas e que será necessário confirmar dados bancários como agência, conta, senhas e tokens.

Como evitar?

Lembre-se que funcionários de bancos não ligam para os clientes para solicitar alteração de dados (incluindo endereço) para fazer testes ou solicitar dados como senhas e tokens para cancelar operações.

No caso de qualquer suspeita, desligue, procure outra linha telefônica e entre em contato com a Central de Atendimento.

Golpe do Motoboy

Ao telefone, o golpista diz que o cartão da vítima foi clonado ou que está realizando a confirmação de uma compra suspeita. Para isso, precisará de dados pessoais.

Ele recomenda que o cartão seja cortado ao meio e afirma que enviará alguém para recolhê-lo no endereço.

Como evitar?

Consulte imediatamente seu gerente sobre alguma irregularidade. Quando precisar destruir seu cartão, corte em várias partes e não deixe o chip inteiro.

Golpe do boleto falso

O criminoso descobre informações sobre você na internet, como débitos em aberto. Dessa forma, ele oferta a quitação do débito com um valor abaixo da dívida e envia o boleto falso por e-mail ou redes sociais.

Você acredita que está pagando um boleto verdadeiro, mas o valor é direcionado para a conta do golpista.

Como evitar?

Ao pagar um boleto, confira os dados do beneficiário, como CNPJ, banco, valor, titular da conta, vencimento e demais dados estão corretos. **Clique aqui** para assistir o vídeo e saber mais.

Golpe do e-commerce falso

Atuam durante o ano todo, mas de forma mais intensa durante datas comemorativas, como o Dia das Mães, Black Friday e Natal.

Como evitar?

Confira o endereço eletrônico do site, pesquise a reputação da empresa e desconfie de preços muito abaixo do mercado.

Na dúvida, acesse os canais oficiais da empresa para confirmar a veracidade da promoção ou entre em contato com o Atendimento ao Cliente.

Golpe do site de leilões falso

Ao participar do leilão em um dos sites falsos, você recebe os dados para depósito em nome de pessoas físicas. Após fazer o pagamento, os golpistas bloqueiam as redes sociais e param de atender ligações.

Como evitar?

Não envie informações pessoais por meio de canais não oficiais e desconfie de preços muito abaixo do mercado.

Golpe do WhatsApp clonado

Por telefone, o golpista oferece um voucher ou promoção e, para validar a participação, é necessário informar um código enviado por SMS (o código de verificação do WhatsApp)

Ao receber o código, a sua conta do WhatsApp é ativada em outro celular e o golpista pede dinheiro emprestado a amigos e parentes em seu nome.

Como evitar?

Habilite a “confirmação em duas etapas” do WhatsApp e jamais envie, para qualquer pessoa, o código de 6 números.

Android: Toque no ícone de três pontos > Configurações > Conta > Verificação em duas etapas e siga os passos da tela.

iOS: Toque em Ajustes > Conta > Verificação em duas etapas > Ativar e siga os passos da tela.

Lembre-se: Nunca compartilhe códigos, senhas ou tokens. Esses dados são pessoais e ninguém além de você deve ter acesso.

Golpe de Phishing

Em português, “phishing” significa “pescaria”, exatamente a tática usada pelos golpistas para conseguir dados como senhas, CPF, RG e outros.

Em e-mails com links falsos, SMS ou sites com ofertas tentadoras, os golpistas usam assuntos do momento para induzir a vítima a clicar.

Como evitar?

Desconfie de mensagens por e-mail, SMS, WhatsApp e Telegram que solicitam dados pessoais, com download de extensões, URL incomuns, erros gramaticais, etc.

Golpe da Maquininha

Ao pedir comida via App, os golpistas relatam que houve um problema no pagamento do pedido. Então, o entregador digita nas máquinas de cartão valores bem superiores ao real.

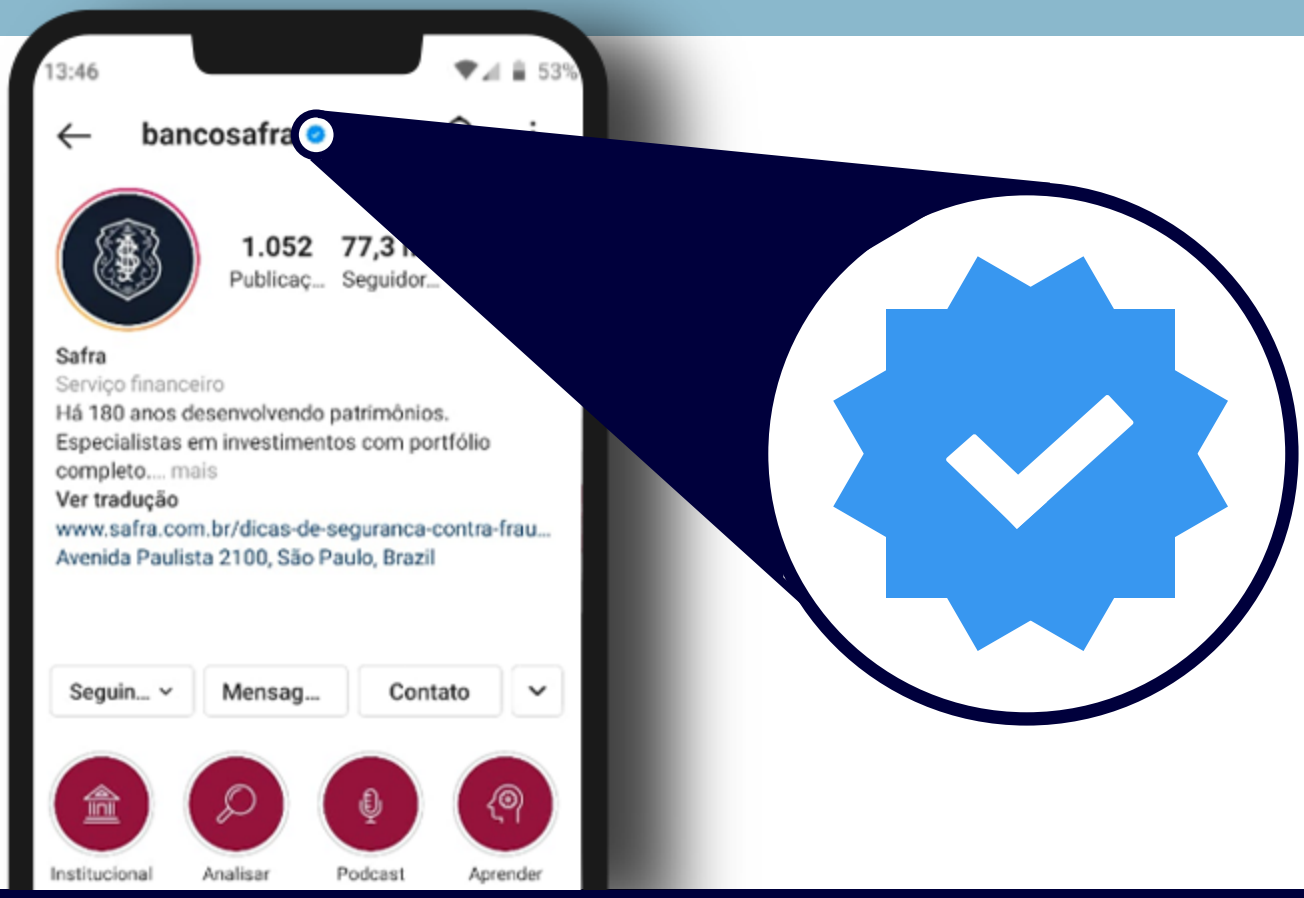
Em ambientes de pouca luz como a portaria de prédios, o interior de um táxi ou deixando o visor da maquininha quebrado, a vítima, em geral, não percebe a fraude e digita a senha.

Como evitar?

Sempre confira o valor cobrado, certifique-se que a tela de digitação da maquininha está no campo senha e, de preferência, faça pagamentos remotos por meio dos apps. Recuse qualquer pedido de pagamento suspeito e não siga com a compra.

Como saber se estou falando com um canal oficial do Safra?

A comunicação do Safra é sempre realizada por e-mail ou em postagens nas redes sociais oficiais. Busque sempre os selos de verificação para confirmar que as contas são legítimas.



Clique aqui para assistir o vídeo e saber mais.

Lembre-se: nem o Safra, nem seus funcionários enviam mensagens privadas em redes sociais para oferecer produtos ou empréstimos.

Meu celular foi roubado! O que fazer?

É muito importante que você lembre de realizar todos os procedimentos que podem evitar fraudes, como:

- Notificar imediatamente o Safra para o bloqueio dos acessos à sua conta por meio da Central de Atendimento. O canal está disponível 24h por dia.
- Entrar em contato com sua operadora para solicitar o bloqueio da linha e IMEI.
- Caso seja possível, apagar as informações do seu celular de forma remota.
- Trocar suas senhas de redes sociais e de e-mails associados ao seu celular, incluindo a senha de acesso a sua loja de aplicativos.
- Verifique se há algum dispositivo desconhecido conectado ao seu aparelho:

No Android:

1. Acesse sua Conta do Google.
2. No painel de navegação à esquerda, selecione Segurança.
3. No painel Seus dispositivos, selecione Gerenciar dispositivos.
4. Selecione um dispositivo conectado à sua Conta do Google para ver mais detalhes.

No iOS:

1. Inicie sua sessão na página da conta do ID Apple e role até Dispositivos.
2. Se os dispositivos não forem exibidos imediatamente, clique em “Ver detalhes” e responda às perguntas de segurança.
3. Clique em um dispositivo para ver as informações dele, como modelo, número de série e versão do sistema operacional.

Desconfio que fui vítima de um golpe. O que fazer?

Neste caso, entre em contato com o Safra imediatamente por meio do SAC (Serviço de Atendimento ao Consumidor) no número 0800 772 5755. O atendimento está disponível 24 horas por dia.

Aproveite as dicas deste guia para se proteger de fraudes bancárias e, caso precise de mais informações, acesse: https://www.safra.com.br/dicas-de-seguranca-contra-fraudes.htm.