Cartilha de **Segurança Digital**

Prevenção contra golpes e fraudes.

Juntos pela sua proteção no ambiente digital.

Sicredi

A proteção dos seus dados bancários e pessoais, assim como dos nossos associados, é fundamental. E, para garantir o cuidado que essas informações merecem, essa cartilha traz dicas para evitar fraudes e golpes em ambientes digitais, aumentando a sua segurança e a dos nossos associados em suas transações.

Boa leitura!

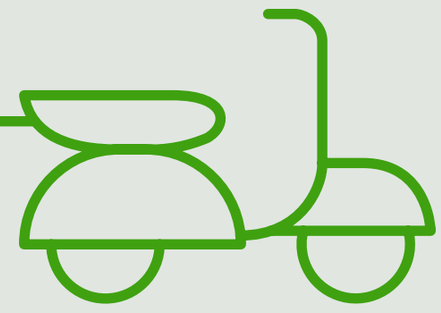
1.

Golpes com cartões

Como acontecem

Esses golpes também podem ser aplicados por vendedores ambulantes e até por taxistas mal-intencionados. Nem sempre o golpista parece suspeito! Existem várias fraudes e recomendamos que nossos colaboradores e associados fiquem atentos a todas elas:

Falso motoboy



Se receber uma ligação dizendo que há transações suspeitas em seu cartão e que será enviado um motoboy para coletá-lo, não passe informações (especialmente sua senha) e desligue na hora. Lembre-se de que nenhuma instituição financeira tem essa prática.

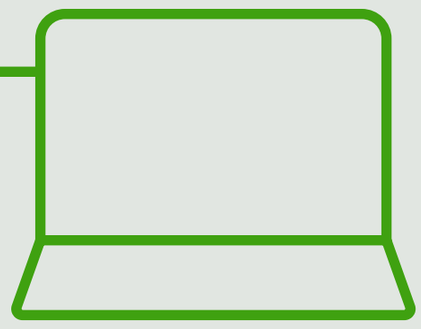
No comércio

O golpista fica de olho na senha digitada pela pessoa e, após a vítima usar a maquininha, devolve um cartão parecido de outra pessoa. Eles também usam de alguma distração para pedir que a pessoa digite a senha no campo de valor.

No caixa eletrônico

O golpista oferece ajuda para usar o terminal de atendimento, guardando a senha e trocando o cartão da vítima por outro muito parecido.

No comércio eletrônico



Atenção com essa modalidade: quando o golpista tem acesso a dados como nome, número do cartão, data de validade e código de segurança, está apto a fazer compras on-line.

Voltar ao menu

Na entrega do cartão

No processo de entrega, o cartão é interceptado por golpistas que buscam os dados da vítima na internet. Em seguida, o golpista contata a vítima se passando pela instituição financeira e solicita o desbloqueio do cartão para que possa corrigir o “extravio”. A partir deste momento, o golpista pode usar o cartão da vítima para compras.

Como evitar

- **Cuidado com o golpe do motoboy.** Nós não realizamos a retirada do seu cartão; ao inutilizá-lo, certifique-se de cortar o chip.

- **Preste muita atenção** na hora de fazer qualquer compra, seja ela física ou on-line.

- **Verifique se está digitando a senha no campo correto** e confira o seu cartão na devolução.

- **Jamais desbloqueie um cartão** que não esteja em suas mãos.

- **Nos terminais de atendimento, não aceite a ajuda de estranhos.** Se precisar de auxílio, sempre recorra a um funcionário identificado.

- **Nunca divulgue os dados do seu cartão** para outras pessoas ou em redes sociais.

- **Utilize um cartão virtual para suas compras on-line.** Com ele, você tem mais praticidade e maior segurança, e suas compras com cartão virtual vêm na mesma fatura do seu cartão físico.

Voltar ao menu

2.

Golpe com falsos funcionários

Como acontece

Golpistas entram em contato, se passando por funcionários da instituição financeira para obter informações confidenciais. Embora o repertório de contato tenha inúmeras variações, por vezes mencionam inclusive que trabalham na área de segurança e que precisam confirmar supostas transações realizadas. A intenção dos golpistas é coletar informações pessoais e dados bancários para utilização indevida.

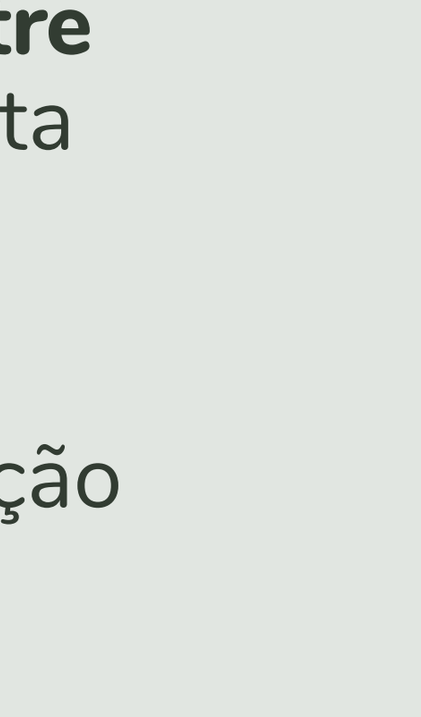
Como evitar

- Independente do motivo da abordagem, a dica nesse caso é **ficar atento a qualquer solicitação de dados** pessoais e pedidos de senhas ou códigos token.

- **Nunca forneça essas informações por telefone, ou através de links recebidos por SMS, WhatsApp, e-mails, redes sociais, entre outros.** Não digite seus dados em uma suposta central de atendimento.

- Nesse tipo de golpe, **os golpistas podem até simular o número de telefone** da instituição financeira e usar recursos tecnológicos, como gravações e menus para aumentar a sua confiança.

Voltar ao menu



Falsos funcionários

Lembre-se

Nós entramos em contato com você,
mas nunca para realizar:

- **Atualização do módulo de segurança;**
- **Atualização cadastral;**
- **Atualização para cadastramento**

e ativação do Pix.

E, independente do motivo do contato,
nunca pediremos:

- **Suas senhas;**
- **Código token;**
- **Códigos recebidos por SMS.**

Também não pediremos que digite esses dados em sites ou iremos transferir você para digitar esses dados em algum atendimento eletrônico. Se receber esse tipo de contato, não forneça nenhuma informação, desligue imediatamente e contate sua cooperativa.

Essas informações são confidenciais e devem ser utilizadas apenas para realizar suas operações financeiras nos canais oficiais do Sicredi.

Voltar ao menu

Falsos funcionários

3.

Golpe por WhatsApp

Como acontece

Nesse golpe, o WhatsApp da vítima é clonado por golpistas que fingem ser do serviço de atendimento de sites de compra para roubar a conta no aplicativo. Com a conta disponível, os golpistas enviam mensagens pelo aplicativo se fazendo passar pela pessoa e solicitam dinheiro emprestado aos seus contatos mais conhecidos.

Como evitar

- A medida mais simples e eficaz para evitar que o WhatsApp seja clonado **é habilitar a opção "Verificação em duas etapas" (Configurações/Ajustes > Conta > Verificação em duas etapas).** Dessa forma, é possível cadastrar uma senha que será solicitada periodicamente pelo aplicativo.

- Se alguém pedir dinheiro emprestado, **é importante ligar para confirmar se é realmente essa pessoa,** mesmo que a foto do contato seja de quem você conhece.

- E, para evitar que sua foto seja utilizada indevidamente, você pode exibi-la apenas para seus contatos de confiança. Esse cuidado vai evitar que golpistas usem a sua imagem e se passem por você para enganar seus conhecidos. **É simples ativar essa opção:**

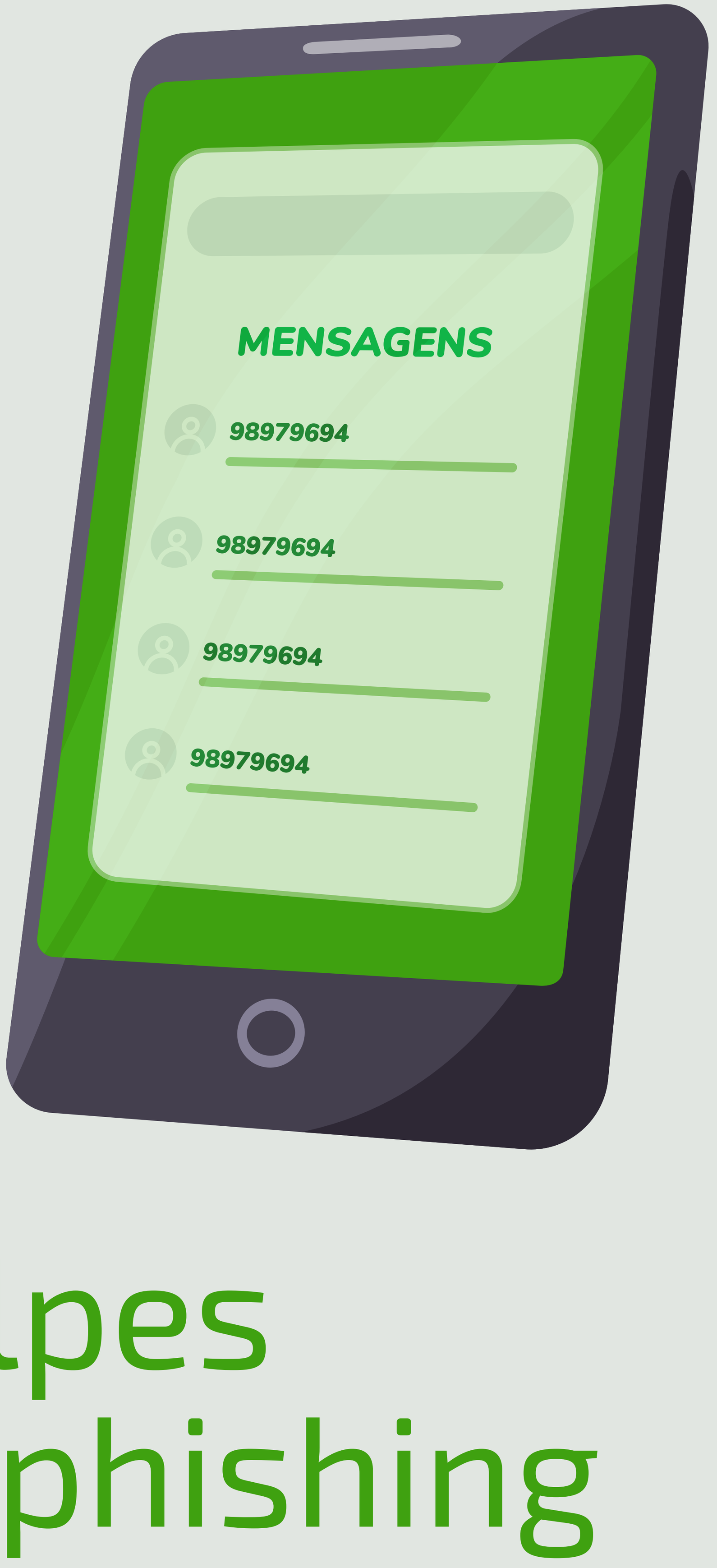
iOS: no WhatsApp, acesse Ajustes > Conta > Privacidade > Foto de perfil > Meus contatos

Android: no WhatsApp, acesse Menu > Configurações > Conta > Privacidade > Foto de perfil > Meus contatos

- Além disso, em hipótese alguma forneça o código de confirmação recebido por SMS para outras pessoas. Nem no WhatsApp, nem em nenhum outro aplicativo. Essa é uma dica que vale para todos os ambientes digitais.

Voltar ao menu

4.



Golpes de phishing

Como acontecem

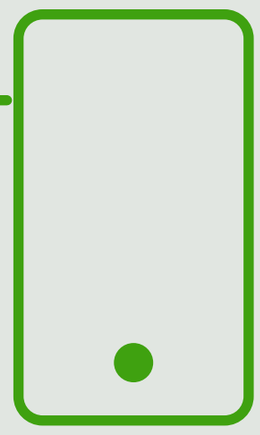
Esses golpes visam roubar senhas ou dados pessoais e bancários, como códigos, números de cartões e suas validades e códigos de segurança. Muitas vezes eles podem provocar a instalação de softwares maliciosos e trazer muitos problemas ao colaborador e ao associado.

Golpe do bloqueio de conta

O golpista envia um falso e-mail ou SMS sobre bloqueio de conta em nome da instituição financeira informando possíveis irregularidades em seu cadastro, ou pedindo uma atualização dele, que pode levar a conta ao bloqueio total.

Golpe da atualização cadastral ou atualização de segurança

O golpista envia um e-mail ou SMS com link, em nome da instituição financeira, informando a falta de atualização ou sincronização do código pedindo senhas e informações pessoais. A vítima é direcionada para um formulário ou página falsa que captura os dados da vítima para o golpista usar posteriormente.



Golpe do SMS com link

Esse golpe é praticado com o envio de um link malicioso por SMS, direcionando a vítima para um formulário ou página que pedirá dados pessoais e bancários, como: senhas, códigos de segurança, números de cartões, entre outros. Por isso, é preciso ter atenção redobrada com esse tipo de mensagem.

Voltar ao menu

Como evitar

- **Desconfie de promoções imperdíveis.**
Ao receber anexos por e-mail ou mensagem por WhatsApp, mesmo que o remetente seja conhecido, é importante verificar se existe aviso sobre extensões que precisam ser ativadas. Cuidado redobrado em páginas desconhecidas ou suspeitas (observar sempre a URL).

- **Cuidado com os SMS.**
Não clique em links com promoções suspeitas e não forneça dados pessoais ou senhas.

- **Cuidado com mensagens recebidas via WhatsApp ou Telegram.**
Elas também podem ser maliciosas e trazer conteúdos semelhantes aos enviados por e-mail ou SMS.

- **Não clique em links desconhecidos.**
Em tempos de pandemia, é preciso cuidado ao participar de ações solidárias transmitidas nas redes, mesmo que recebidas de pessoas conhecidas. O conteúdo e os formulários onde você deixa seus dados podem ser maliciosos.

Lembre-se sempre

de que a forma ideal para acessar um site é digitando o endereço (URL) diretamente no navegador.

Voltar ao menu

Como identificar um e-mail suspeito:

- **O nome no endereço “De:” corresponde ao endereço de e-mail?**
- **O texto está bem escrito ou contém erros ortográficos e gramaticais?**
- **O logotipo está desfocado ou deformado?**
- **Está solicitando informações pessoais ou confidenciais?**
- **Há um senso de urgência na mensagem?**
- **A URL do site é incomum? Tem anexo? Se o tipo de arquivo parecer estranho, não abra.**

Voltar ao menu

5.

Golpes em sites falsos

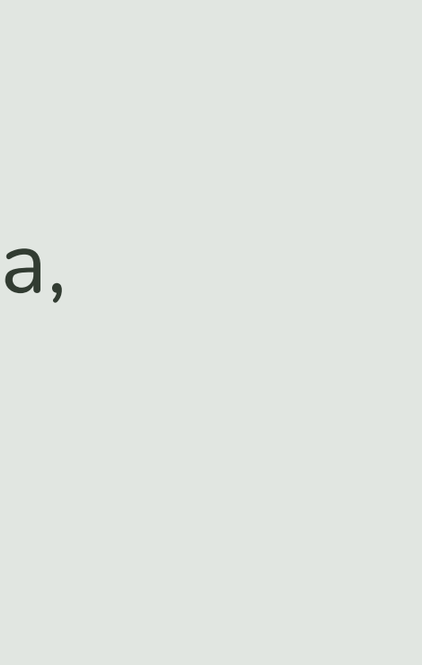
Como acontecem

Com a internet, muitos comportamentos mudaram. Hoje realizamos muitas de nossas compras on-line, mas ainda não nos acostumamos a conferir a veracidade desses sites e os requisitos básicos de segurança para garantir que estamos em um ambiente seguro. Assim, golpes envolvendo sites falsos são bastante recorrentes e costumam iniciar pelo envio de links por SMS e e-mail.

Com frequência, o objetivo é atingir clientes de sites de comércio eletrônico através de um site quase idêntico ao verdadeiro. As vítimas não percebem a fraude, escolhem os produtos desejados e realizam o pagamento sem saber que nunca vão receber a mercadoria.

Para chamar atenção, os golpistas normalmente fazem promoções tentadoras, trazendo produtos com descontos fora do comum. Pensando em dar credibilidade à farsa, se valem de marcas conhecidas e sérias.

Voltar ao menu



Como evitar

- **Dando preferência para conexões seguras.** Evite se conectar por redes Wi-Fi públicas.

- **Fazendo uma pesquisa de mercado comparando preços.** Desconfie se o valor for muito baixo.

- **Checando de forma minuciosa** o endereço (URL) do site em que está comprando. Sites falsos possuem domínios bastante similares aos verdadeiros. Dê preferência a sites cujos domínios terminam em **.com.br**. Sites que possuem domínios **.com** indicam que estão hospedados em servidores situados fora do Brasil.

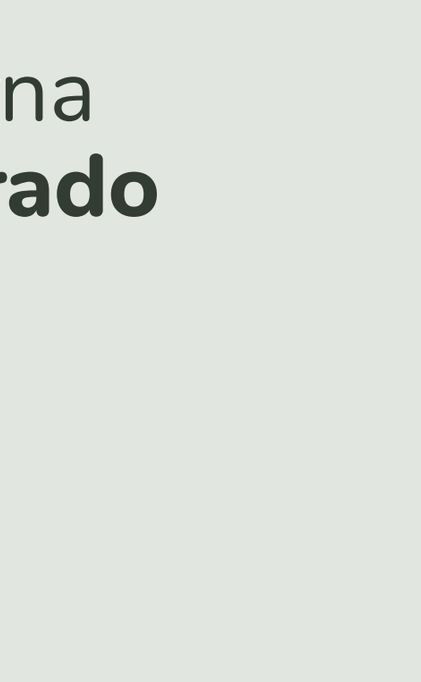
- **Não clicando em links** que direcionem direto aos sites de compras. Esses sites podem ser falsos e conter malware (vírus) capaz de copiar dados sigilosos.

- **Fazendo um teste.** Digitar o endereço da loja oficial direto no navegador.

- Sites .com.br permitem uma pesquisa sobre o seu titular em www.registro.br, assim se torna possível **avaliar se de fato o site está registrado** em nome da empresa correspondente.

- **Localizando o cadeado do navegador:** um site seguro apresenta o desenho de um cadeado ao lado da URL (endereço do site). Ao clicar nele, será exibido o certificado de segurança.

Voltar ao menu



6.

Golpe
do anúncio
duplicado

Como acontece

Golpistas se aproveitam de anúncios legítimos de compra e venda de produtos e serviços (normalmente carros e motos), e enganam vendedor e comprador ao mesmo tempo.

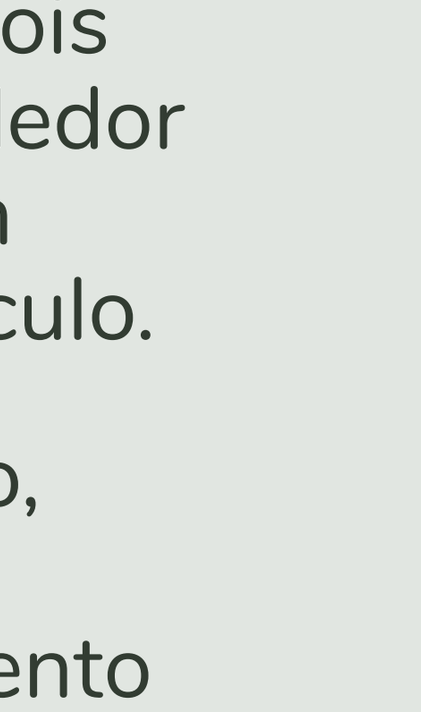
Exemplo:

O estelionatário contata o vendedor através do anúncio e demonstra interesse em adquirir o produto anunciado em um site como a OLX. Ao dar início à negociação, pede que o vendedor (primeira vítima) retire o anúncio do site, pois está fechando negócio. Depois usa todas as informações do veículo anunciado e faz um novo anúncio com valores menores para atrair compradores mais facilmente (segunda vítima).

O golpista arma um encontro entre as duas vítimas (vendedor e comprador) pedindo que não falem em valores, identificando-os como um terceiro que vai fechar o negócio. Se as vítimas não perceberem nada de errado até esse momento, elas chegam à fase de pagamento do produto. Para dar veracidade à negociação fraudulenta, depois de feita a transferência, as duas vítimas (vendedor e comprador) são orientadas a comparecerem a um cartório e realizar a transferência do veículo.

Por último, no momento da entrega do veículo, as vítimas se dão conta de que caíram em um golpe, pois o vendedor não recebeu o pagamento e o comprador repassou seu dinheiro para o golpista, que fez o papel de intermediário da negociação.

Voltar ao menu



Anúncio duplicado

Como evitar

- **Mantenha um diálogo aberto** entre o vendedor e o comprador, encontrem-se pessoalmente, analisem o veículo e falem sobre a situação dele (valores, pendências, etc).

- Se você é o comprador, **identifique a pessoa titular da conta** bancária em que o pagamento será realizado.

- Na condição de vendedor, é essencial que a entrega do carro (ou moto) e o preenchimento do recibo somente sejam **efetivados após a confirmação do recebimento** do valor na sua conta bancária.

Voltar ao menu

Anúncio duplicado

7.

Golpe do boleto falso

Como acontece

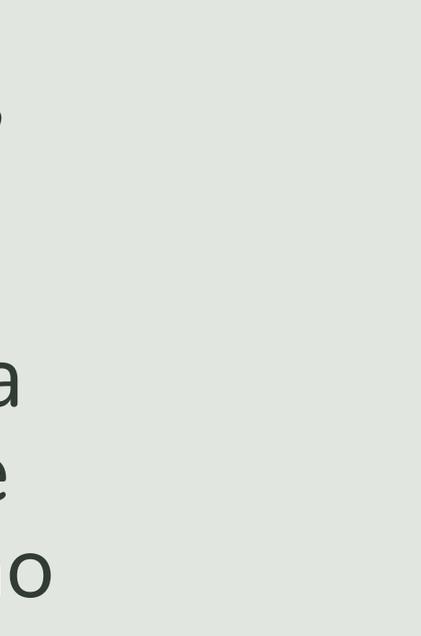
Essa é outra situação bastante comum, que normalmente ocorre através do envio por e-mail, mas também pode ocorrer por redes sociais, WhatsApp, sites falsos e outros canais.

A vítima recebe em seu e-mail um boleto verdadeiro de determinada compra feita ou serviço contratado. Antes de efetuar o pagamento, chega um novo e-mail contendo outro boleto, agora com valor inferior. No texto do e-mail normalmente é informado que houve um erro no cálculo de algum imposto ou que o cliente ganhou um desconto.

O cliente acreditando ter realmente recebido o boleto da empresa responsável pelo produto ou serviço, acaba realizando o pagamento. Algum tempo depois começa a receber cobranças das empresas, sinalizando que o boleto não foi quitado. Sem entender o que está acontecendo, a vítima apresenta os comprovantes de pagamento, momento em que é constatado a fraude no boleto.

Esses boletos falsos possuem um formato bastante semelhante ao dos boletos originais, mas apresentam algumas diferenças que apontam terem sido os dados manipulados, principalmente em relação à linha digitável, na qual constam os dados da conta bancária que receberá o valor a ser pago. Com a adulteração da linha digitável, os golpistas conseguem fazer com que o dinheiro da vítima vá para contas bancárias dos próprios golpistas ou de “laranjas”.

Voltar ao menu



Como evitar

- **Observe se os seus dados** (nome, CPF, endereço) que constam no boleto estão corretos e se há algum erro de português ou de formatação.

- **Confira se os 3 primeiros números do código de barras** correspondem à instituição financeira cuja logomarca aparece no boleto.

- **Verifique se os últimos números do código de barras** correspondem ao valor do documento.

- **Fique atento a descontos e promoções inesperadas.** Na dúvida, ligue para a empresa e confirme o valor e demais dados do documento.

- **Faça uma consulta ao CNPJ** da empresa credora do boleto no site da Receita Federal e certifique-se de que realmente é a empresa contratada.

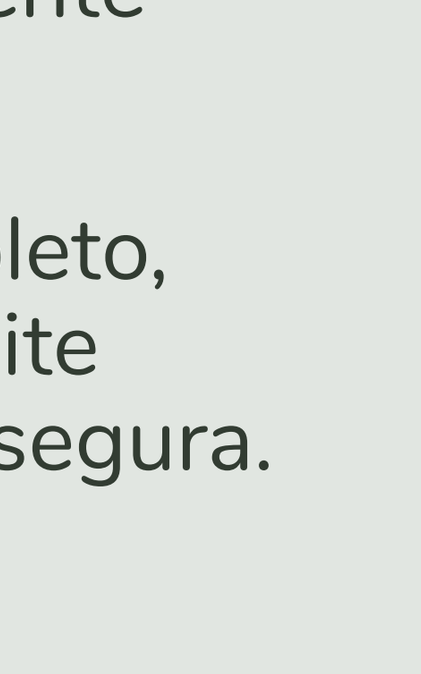
- Opte por pagar o boleto **utilizando o leitor do código de barras** disponível no aplicativo.

- Ao fazer a leitura do código de barras **verifique se o nome do beneficiário** é realmente da empresa/pessoa contratada.

- Ao necessitar emitir uma segunda via de boleto, **faça o download do boleto** diretamente no site da empresa credora, utilizando uma conexão segura. Evite utilizar Wi-Fi público.

- **Em caso de suspeita,** sempre entre em contato com a empresa para confirmar a legitimidade do boleto.

Voltar ao menu



8.

Cuidados com o Pix

Os cuidados que você, colaborador, e os nossos associados deverão adotar na hora de realizar uma transação através do Pix deverão ser os mesmos adotados ao fazer qualquer transação financeira. Portanto, sempre confira os dados do "recebedor" da transação Pix (pagamento ou transferência), seja para uma pessoa ou um estabelecimento.

Voltar ao menu

Confira algumas dicas de boas práticas para aproveitar os benefícios do Pix de forma mais segura:

- **Não acesse links** encaminhados por e-mail, postagens em mídias sociais ou SMS provenientes de pessoas e órgãos duvidosos. Sempre desconfie dos links que você recebe.

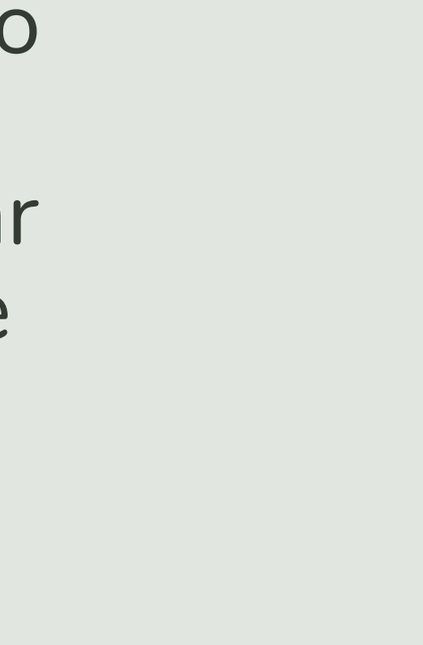
- **O cadastro da sua chave Pix deve ser realizado somente no ambiente seguro** da sua instituição financeira, através do Internet Banking ou Mobile Banking. Os aplicativos móveis devem ser instalados a partir das lojas oficiais da Apple (Apple Store) e do Google (Play Store).

- **Cuidado com os e-mails** ou mensagens de WhatsApp sobre convites de pré-cadastro ou cadastro do Pix. Na dúvida, não passe nenhuma informação.

- **Cuidado com ligações** de “supostos funcionários” da sua instituição financeira oferecendo o cadastramento do Pix ou mesmo oferecendo um serviço de atualização via conexão remota com o argumento de atualizar ou fazer um teste. Na dúvida, desligue e entre em contato com seu Gerente.

- **Não faça transferências** ou realize transações para supostamente fazer um teste na sua chave Pix – isso não existe!

Voltar ao menu



9.

Redes sociais e privacidade

As redes sociais são ferramentas de comunicação, informação e entretenimento. Mas como quase todo ambiente digital, elas demandam cuidados com a segurança e privacidade de dados e informações, tanto pessoais quanto bancárias.

Confira algumas dicas básicas para uso das redes sociais de forma segura:

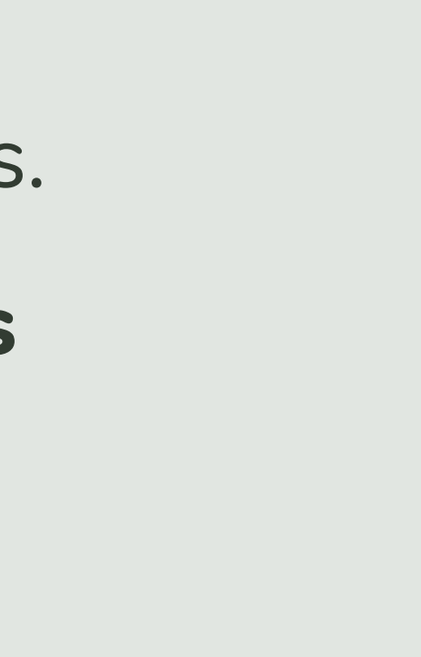
- **Evite expor** exageradamente informações pessoais, financeiras e corporativas nas redes sociais, ou que possam passar a impressão de ostentação.

- **Configure a privacidade** de suas postagens.

- **Nunca coloque suas informações pessoais em formulários** de promoções sem verificar no site oficial da empresa a legitimidade.

- **Dissemine esses cuidados** para seus amigos e familiares.

Voltar ao menu



10.

Senha e autenticação

Alguns cuidados básicos que podem aumentar a segurança das senhas:

- **Trocar senhas periodicamente** (a cada 2 meses, ou sempre que houver suspeita de que sua senha foi comprometida).

- **Não compartilhe senhas** e nem utilize a mesma senha para vários serviços.

- **Não salve senhas** em cadernos, arquivos, no celular ou navegador.

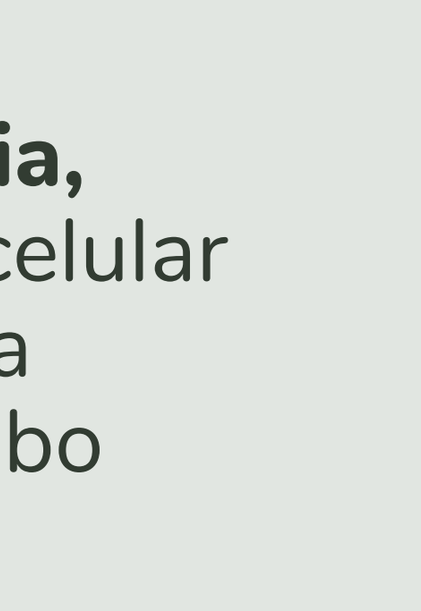
- **Crie senhas difíceis** de serem descobertas. Utilize letras (maiúsculas e/ou minúsculas), números e caracteres especiais quando for permitido.

- **Utilize Gerenciadores de senhas,** pois eles criptografam credenciais e geram senhas complexas e aleatórias.

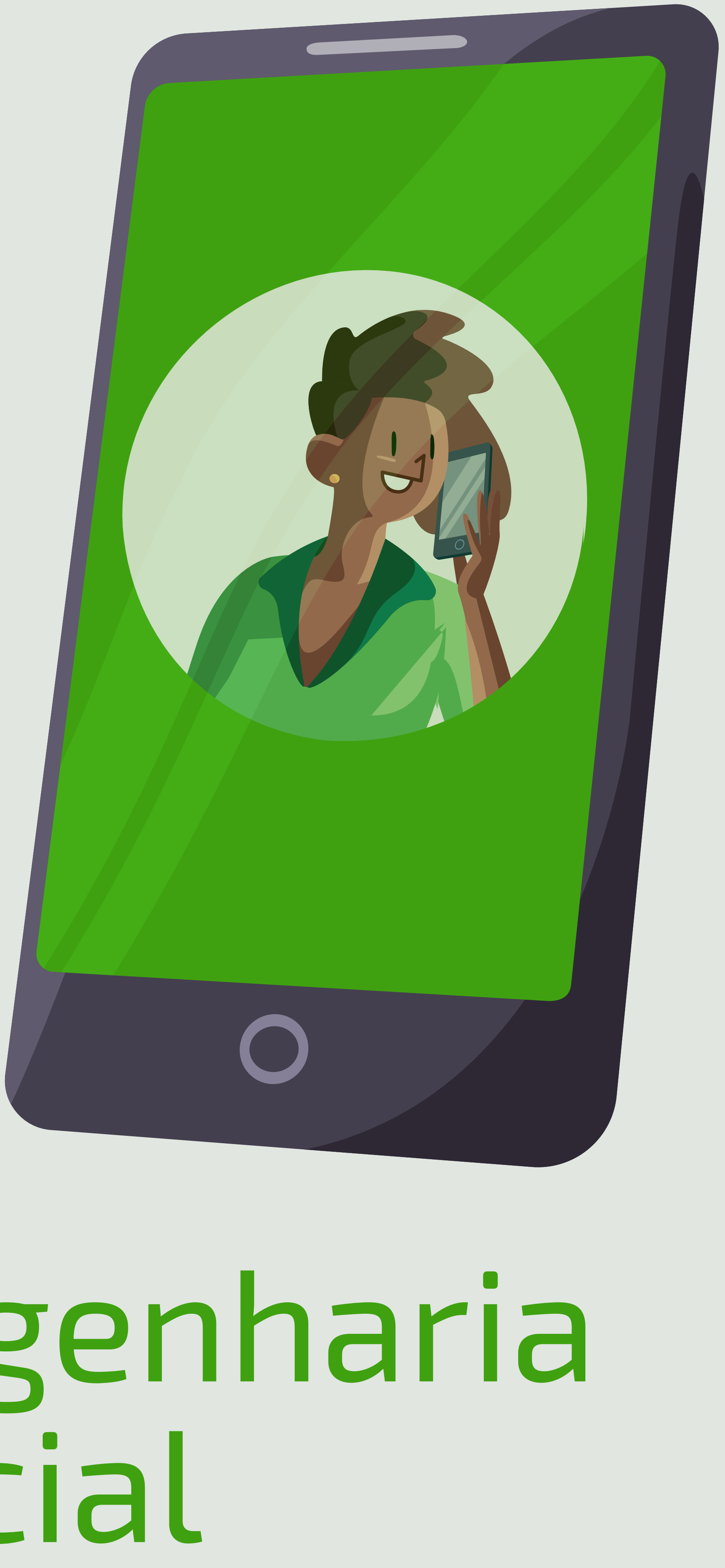
- **Use sempre a autenticação** de dois fatores. Exemplo: ao transacionar via Internet Banking, utilize o dispositivo QR Code, que possui uma segunda camada de autenticação.

- **Ao utilizar o recurso de login por biometria,** saiba que toda biometria cadastrada em seu celular terá acesso aos aplicativos em que você utiliza essa funcionalidade. Em caso de perda ou roubo do celular, comunique imediatamente sua instituição financeira para solicitar o bloqueio da conta e acesso ao aplicativo, evitando assim a utilização indevida por terceiros.

Voltar ao menu



11.



Engenharia social

O que é engenharia social?

É uma técnica empregada por golpistas para induzir usuários desavisados a repassarem dados confidenciais (ex: senhas e dados de cartões de crédito), infectar seus terminais com malwares (vírus) ou abrir links para sites infectados.

Ao contrário do que muitos pensam, não é necessário qualquer equipamento de tecnologia avançada para realizar essa atividade. Na verdade, a engenharia social é simplesmente uma manipulação psicológica do usuário, de modo a convencê-lo a fazer o que o criminoso quer, burlando procedimentos básicos de segurança.

Um exemplo clássico de ataque de engenharia social ocorre quando golpistas se passam por funcionários de uma instituição financeira e ligam para informar que o sistema está sendo atualizado. Assim, argumentam que é preciso realizar um procedimento para permanecer com acesso à conta e informam a necessidade de acessar determinado link, aproveitando para solicitar informações pessoais como dados da conta e senhas.

Atenção!

Nenhuma instituição financeira realiza esse procedimento.

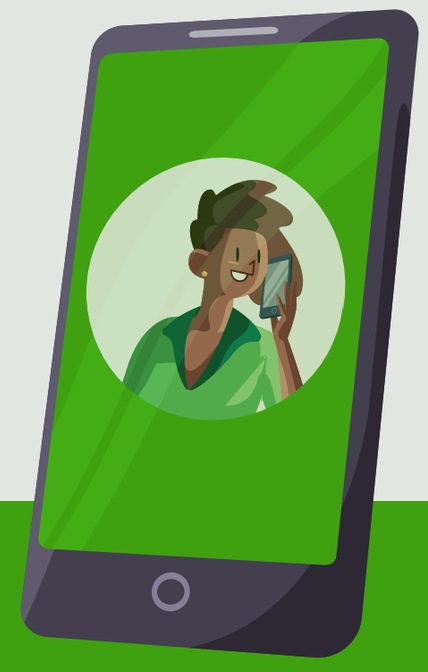
Voltar ao menu

O Sicredi entra em contato com seus associados, **PORÉM** não solicita:

- **Acesso a senhas, códigos bancários e dados pessoais.**
- **Acesso ao App com dados pessoais.**
- **Atualização de dispositivos.**

Em caso de qualquer abordagem semelhante, você deve procurar a sua cooperativa!

Voltar ao menu



12.

Dicas rápidas

Para facilitar sua consulta, reunimos as principais dicas dessa cartilha:

- **Ative a chave Pix** somente nos nossos canais oficiais e não realize nenhuma transação de teste.

- **Habilite a verificação em duas etapas no WhatsApp.**

iOS: no WhatsApp, acesse Ajustes > Conta > Confirmação em duas etapas > Ativar.

Android: no WhatsApp, acesse Menu > Configurações > Conta > Confirmação em duas etapas > Ativar.

- **E, para evitar que sua foto no WhatsApp seja utilizada indevidamente, exiba somente para seus contatos de confiança.**

iOS: no WhatsApp, acesse Ajustes > Conta > Privacidade > Foto de Perfil > Meus contatos

Android: no WhatsApp, acesse Menu > Configurações > Conta > Privacidade > Foto de perfil > Meus contatos

- Se receber alguma solicitação para realizar transações, **confirme a legitimidade do pedido da transferência** ou pagamento ligando para a pessoa e fazendo perguntas pessoais. Mesmo que a foto do contato seja da pessoa que você conhece, faça a confirmação antes de realizar a transação.

- **Ao realizar um pagamento de boleto,** certifique se a linha digitável está de acordo com o logo da instituição financeira, além do Beneficiário - Cedente e Pagador – Sacado.

- **Atenção aos sites** que possuem domínio **.com** e produtos com valores muito abaixo do praticado.

- Ao acessar sites, **procure sempre digitar o endereço no navegador.** Evite clicar em links.

- **Proteja seu computador,** não abra arquivos de fontes desconhecidas.

- **Nunca forneça senha** ou dados pessoais a terceiros, principalmente por telefone.

Voltar ao menu

- **Desconsidere mensagens** de instituições financeiras com os quais você não tem relação, especialmente quando solicitarem seus dados pessoais ou a instalação de módulos de segurança.

- **Não faça transações bancárias** a partir de equipamentos de terceiros ou redes Wi-Fi públicas.

- **Nunca entregue seu cartão** a outra pessoa. Nenhuma instituição financeira faz coleta de cartões.

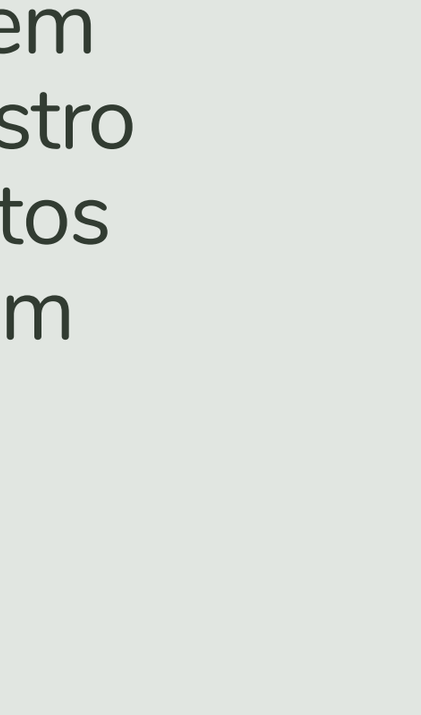
- **Sempre corte o chip** do cartão ao descartá-lo.

- Ao utilizar o recurso de login por biometria, **esteja ciente que toda biometria cadastrada em seu celular terá acesso aos aplicativos** em que você utiliza essa funcionalidade. Em caso de perda ou roubo do celular, comunique imediatamente sua instituição financeira para solicitar o bloqueio da conta e acesso ao aplicativo, evitando assim a utilização indevida por terceiros.

- **Específico para cooperativas:** ativação do dispositivo de segurança por telefone. Certifique-se da legitimidade do associado que está contatando, pedindo o código de ativação. Desligue o telefone, informe que fará as análises necessárias, entre em contato através do telefone que consta no cadastro e faça confirmações sobre a utilização de produtos que ele possui. Essas são evidências que auxiliam na identificação positiva.

- **Ao fazer uma negociação,** confirme o efetivo recebimento do dinheiro em sua conta antes de entregar a mercadoria. Tenha atenção a comprovantes falsos, comprovantes de agendamento ou comprovante de depósito feitos em caixa eletrônico utilizando um envelope vazio.

Voltar ao menu



Seguindo essas dicas e cuidados, você vai ficar muito mais protegido e pronto para orientar associados, amigos e familiares.