PREVENÇÃO CONTRA

GOLPES E FRAUDES

SICOOB
Coopemata

O Sicoob investe continuamente em segurança para garantir a tranquilidade de seus cooperados e colaboradores. Mesmo assim, é importante que você adote algumas medidas ao realizar suas operações financeiras, uma vez que, sua segurança, assim como a dos nossos associados, está sempre em primeiro lugar.

Pensando nisso reunimos nessa cartilha as melhores dicas do Sicoob, para a prevenção contra golpes e fraudes. A informação ainda é a melhor forma de se proteger contra criminosos.

SUMÁRIO

Fraudes financeiras em celulares roubados

Imagine que você está na rua, respondendo uma mensagem no celular, quando de repente alguém rouba seu aparelho. Ainda que o App Sicoob seja seguro e confiável, é fundamental que você adote alguns cuidados para manter sua conta bancária protegida caso tenha o celular roubado. Siga essas dicas e evite que suas informações pessoais e financeiras sejam usadas por pessoas mal-intencionadas.

Por isso, **jamais compartilhe suas senhas por aplicativos de mensagens ou as guarde em bloco de notas**, e quando precisar compartilhar, lembre-se de apagar as conversas que contenham senhas e/ou dados pessoais. Outra dica fundamental é **evitar usar a mesma senha em contas diferentes**, evite também andar na rua usando o celular e tenha cuidado ao volante sempre que usar aplicativos como Waze ou Google Maps.

Ativar o bloqueio de tela com senha diferente das demais, também é uma forma de se prevenir, além de usar o "duplo fator de autenticação" nas plataformas que você utiliza. Uma dica que vale ouro no Sicoob é **nunca usar a opção "salvar senha" em navegadores e sites**, e lembre-se de manter o IMEI do seu aparelho anotado em casa ou em algum lugar seguro.

Foi vítima? Saiba como você deve agir:

- Avise sua cooperativa imediatamente ou ligue 0800 724 4420 (opção 5) e peça para desabilitar o acesso à sua conta;
- Envie um comando para apagar os dados do seu aparelho remotamente (recurso disponível para Android e iOS);
- Avise sua operadora e solicite o bloqueio da linha e do IMEI do aparelho;
- Faça um B.O. na delegacia mais próxima ou pela internet;
- Avise seus familiares e amigos.

Golpe do falso empréstimo

O golpe do falso empréstimo é a oferta de empréstimos para pessoas negativadas com a promessa de não consultar órgãos de proteção ao crédito. Utilizam anúncios em outdoors, rádios, jornais, internet, mídias sociais, entre outros, em que se oferecem empréstimos sem consulta aos órgãos de proteção ao crédito. Ao receber o contato dos interessados em tomar o empréstimo, e após dar maiores informações sobre as condições contratuais, os golpistas solicitam pagamento antecipado de taxas administrativas e seguros prestamistas e, quando recebem o pagamento, que geralmente é por TED, cortam o contato com a vítima.

Sempre desconfie das facilidades ofertadas e não efetue qualquer pagamento antecipado de taxas administrativas ou seguros prestamistas. Essa não é a prática adotada por instituições financeiras sérias. E lembre-se, **o Sicoob nunca pede pagamento antecipado de taxas administrativas ou seguros prestamistas para liberar empréstimos.**

Golpe do falso sequestro ou do falso parente

A vítima recebe um telefonema informando que um parente próximo está em poder de sequestradores (o que é mentira) e solicitam o pagamento de resgate imediato através de transferência ou depósito; ou um falso parente telefona para a vítima solicitando um “empréstimo” imediato para arcar com despesas de uma eventualidade inesperada. Após contatar a vítima, os golpistas passam informações bancárias de conta corrente para a qual a transferência deve ser realizada. Desconfie sempre!

Ao receber este tipo de telefonema, **não fale o nome do parente em nenhum momento.** Desligue o telefone e contate seu parente para certificar-se de que ele está seguro. Se conseguir, anote os dados bancários fornecidos pelo golpista e avise a polícia. Sempre desconfie de ligações comunicando sequestros. Desligue o telefone e tente contatar o suposto sequestrado.

Golpe do DDA

Consiste no envio de falso e-mail informando sobre um boleto com desconto. Assim, os fraudadores solicitam que a vítima desconsidere o pagamento do DDA e realizem o pagamento do novo boleto enviado pelo e-mail. Dessa forma, os recursos são desviados para outra pessoa. A quitação da obrigação prevista no DDA não será realizada e, assim, a dívida permanecerá.

Se você aderiu ao DDA, se receber um boleto para pagamento por e-mail desconfie e confirme junto ao beneficiário a legitimidade do documento antes de efetuar qualquer pagamento.

Golpe do falso leilão

Consiste em um site de leilão falso criado com o intuito de roubar dados dos consumidores. Nestes casos, a página falsa aparenta ser apenas mais uma opção oficial e legítima dentre tantas outras de leilões online, com uma diferença importante: o produto nunca será entregue.

Outra técnica utilizada pelos golpistas para trazer ainda mais confiança ao site de leilões é criar uma página no Reclame Aqui (www.reclameaqui.com.br), como se fosse uma empresa constituída. Neste site, os próprios golpistas colocam comentários como se fossem clientes do suposto leilão, mas com reclamações pouco graves, como por exemplo, um retrovisor quebrado em um veículo adquirido ou algum outro dano pequeno. Essas interações buscam dar a impressão de que houve um problema com aquela pessoa, mas que ela de fato recebeu o veículo.

Além disto, existe a pressão do tempo contra a vítima. Por se tratar de um leilão, a pessoa não pode demorar muito para decidir, ela precisa dar o lance e comprar rápido, antes que outro o faça. A partir daí, e uma vez que a vítima consegue dar um lance e é vencedora do suposto leilão, ela recebe um boleto para pagamento. No momento em que a quadrilha identifica que o pagamento foi de fato efetuado, bloqueia todos os contatos e a vítima não consegue mais falar com a suposta “empresa”.

Veja algumas dicas para se proteger desse tipo de golpe

- Desconfie de preços muito abaixo do praticado no mercado;
- Nunca faça cadastros em sites de leilões antes de pesquisar sobre sua reputação;
- Na dúvida, nunca envie dados bancários ou documentos pessoais;
- Confirme no site do Detran se o leilão está sendo processado na plataforma do leiloeiro designado pelo órgão.

Golpe do Motoboy

Fraudadores ligam para o cliente e questionam uma suposta compra no cartão. Pedem as senhas para supostamente bloquear o cartão e oferecem mandar um motoboy ao cliente para recolher o cartão para “perícia”.

ATENÇÃO!

O Sicoob não envia motoboys ou funcionários a seu endereço residencial ou comercial, mesmo quando o cartão precisa ser substituído após transações suspeitas e nem pedimos celulares ou digitação de senha.

Nunca informe seus dados bancários e senhas por telefone. Se alguém ou alguma empresa se oferecer para buscar o cartão, cuidado, pode ser golpe. Se não for mais usar o cartão, danifique o chip, pois assim, seu reuso é evitado.

Golpe por QrCode

O fraudador, se passando por empregado da Central de Suporte ou da cooperativa, induz o cooperado, por telefone, a realizar uma atualização de segurança e solicita à vítima que acesse uma falsa aplicação do internet banking, na qual o cooperado informa todos os dados de acesso à conta, incluindo a senha.

De posse dos dados capturados, o fraudador acessa o App Sicoob do seu celular para cadastrá-lo na conta do cooperado e, ainda na ligação telefônica, solicita ao cooperado que acesse o App Sicoob para realizar a leitura do QR Code de liberação de dispositivo. Uma vez liberado o celular do fraudador, ele passa a efetuar transações financeiras até o limite disponível do cooperado.

O Sicoob não solicita atualização do internet banking por telefone ou envio de QR Code. Nunca faça transferências, TEDs, DOCs ou pagamentos em sua conta corrente para fazer um teste após suposta atualização do Internet Banking. Sempre confira todas as informações contidas na tela do celular após leitura do QR Code.

Pirâmide financeira

A pirâmide é uma das mais antigas fraudes financeiras conhecidas, mas que continua fazendo vítimas. Começa com um negócio que promete retorno rápido e lucro alto. Você investe um valor inicial e, em seguida, precisa recrutar novos participantes para faturar uma comissão mais alta. No entanto, o lucro nunca vem. Em algum momento alguém desaparece e todo o sistema entra em colapso.

Nestes tempos de internet, o esquema se atualizou. Agora existem páginas anunciando “dinheiro fácil sem sair de casa” ou “aplicações com rentabilidade de mais de 20%”, um valor muito acima de qualquer produto financeiro tradicional. Alguns até aparecem com o nome de marketing digital, nome diferente, mas com as mesmas características de uma pirâmide. Melhor pensar duas vezes antes de investir o seu dinheiro suado numa roubada dessas.

Malware

Uma nova página inicial surgiu sem sua permissão? Há uma barra de ferramenta ou atualizações que brotou em seu navegador? Tentou acessar um site e foi redirecionado para outro? Suas ferramentas de proteção foram desativadas? Contatos de e-mails e rede sociais avisaram que você mandou conteúdo estranho? Se sim, provavelmente você carrega um malware.

Se a velocidade, tanto em navegadores na internet quanto na execução de programas, ficar visivelmente debilitada repentinamente é outro sinal. Um malware costuma interferir no desempenho por usar parte do potencial de sua máquina para outros fins. Isso também causa travamentos.

Ao receber um e-mail suspeito, com erros de português, links de ofertas incríveis ou imagens de celebridades, **não clique no link.** Delete o e-mail. Procure ter sempre as versões mais atuais do seu navegador para contar com mecanismos de segurança aprimorados. Evite realizar movimentações utilizando conexões wi-fi de locais públicos. E lembre-se de manter seus sistemas e aplicativos sempre atualizados, e verifique se o antivírus está instalado, atualizado e ativo.

Mensagens falsas e ataques pela internet

Phishing é uma técnica usada por fraudadores para roubo de informações pessoais via e-mail, SMS, telefonemas ou redes sociais. Ao clicar no link recebido, você é direcionado para um site falso, muito parecido com o verdadeiro. Porém, quando você informa seus dados, o fraudador os copia sem você perceber.

Atenção ao receber mensagens de SMS que informam sobre bloqueio de acesso ou que pedem atualização de dados pessoais, alguns possuem erros de português no conteúdo e tentam te convencer a clicar no link e informar seus dados. Outro ponto de atenção é que grande parte dos SMS falsos vem de números particulares e não de empresas.

O ataque pela internet acontece quando o usuário recebe um link ou arquivo por e-mail que, ao ser clicado, altera uma configuração de segurança do computador, permitindo acesso remoto por fraudadores. Por isso, é importante se atentar ao receber mensagens e lembre-se de **não abrir links de SMS suspeitos e nunca informe seus dados bancários e senhas.**

Golpe do WhatsApp

No Golpe do WhatsApp, o fraudador cadastra indevidamente o número de telefone do usuário em outro dispositivo e, após esse processo, um SMS contendo um código de liberação de acesso é enviado para o celular da vítima. Por meio da engenharia social, a vítima é induzida a fornecer esse código ao criminoso e, em seguida, a sua conta de WhatsApp é bloqueada. Nisso, o golpista passar a enviar mensagens para os contatos da vítima pedindo dinheiro no nome dela.

Outra modalidade de clonagem de contas do WhatsApp tem como alvo pessoas que publicam anúncios em sites de vendas e disponibilizam um número de celular. Com a informação, os autores do golpe enviam uma mensagem se passando pela empresa que hospeda o anúncio, alertando a vítima sobre uma suposta necessidade de manter o anúncio ativo com o envio de um código.

Na verdade, o código é para instalação do WhatsApp e, caso a pessoa o envie, seu acesso ao aplicativo é cancelado e a conta é transferida para o outro aparelho. Assim, mesmo com número diferente, os cibercriminosos terão acesso ao histórico de mensagens da vítima para ajudá-los a aplicar os golpes.

A dica para se proteger é ativar a verificação em duas etapas do WhatsApp. É muito fácil:

1. **Acesse as Configurações ou Ajustes do Whatsapp, em seguida clique em Conta e Confirmação/Verificação em duas etapas;**

2. **Forneça seu endereço de e-mail e em seguida cadastre um PIN de 6 dígitos. Periodicamente o WhatsApp irá solicitá-lo.**

Fique atento! Se alguém te mandar mensagem pedindo dinheiro emprestado, desconfie! Sempre ligue por outro canal e confirme se é a pessoa, de fato.

E, para que a sua foto não seja utilizada indevidamente, você pode exibi-la apenas para seus contatos salvos. Esse cuidado vai evitar que golpistas usem a sua imagem e se passem por você para enganar seus conhecidos. E lembre-se de nunca fornecer o código de confirmação recebido pelo SMS para um terceiro. E essa dica vale para qualquer outro aplicativo em meios digitais.

Boleto falso

O golpe do boleto falso geralmente ocorre de forma eletrônica no momento da impressão da segunda via, alterando apenas a linha digitável do boleto, permanecendo as demais características do documento. Assim, com os dados incorretos o dinheiro será desviado para uma conta diferente daquela que deveria recebê-lo.

Esse tipo de fraude utiliza-se de um vírus que pode entrar no computador da vítima disfarçado como um programa comum e legítimo, através de anexos de e-mail, imagens, fotos, pen-drives; páginas falsas acessadas, etc. Portanto, os softwares não são instalados nos sites dos bancos, pois eles são protegidos e sim na máquina do usuário.

A detecção da fraude é realizada através da análise visual do boleto, onde você precisa conferir:

- O nome e a logomarca do banco emissor devem ser coincidentes;
- O número do banco deve corresponder ao banco contido na logomarca e no campo nome do banco. Em caso de dúvida acesse http://www.buscabanco.org.br ;
- Os três primeiros caracteres da linha digitável devem ser iguais ao número do banco e correspondente ao nome do banco e sua logomarca.

Os números contidos nos campos: Agência, Código cedente e nosso número devem de alguma forma estar contidos na linha digitável, independente do banco emitente do boleto e da localização destas informações na linha digitável. Elas devem estar em algum lugar do campo livre da linha digitável, sendo os dados de um campo por inteiro e não partes, lembrando de excluir os DV (dígitos verificadores) no momento da conferência.

Golpe do e-mail

Para manter a relação com nossos cooperados sempre próxima, enviamos e-mails sobre promoções e benefícios, mas nunca solicitamos a realização de transações, dados pessoais, bancários ou senhas. Desconfie das ofertas mirabolantes que chegam a sua caixa de entrada.

Antes de abrir ou clicar em algum link, verifique a veracidade das promoções e a reputação da empresa. Desconfie de e-mails que solicitam o cadastramento ou atualização de suas informações. Nesses casos, contate a empresa solicitante ou acesse o site oficial para confirmação.

ATENÇÃO!

O Sicoob não envia por e-mail:

- **Arquivos de instalação (.exe);**
- **Solicitação de dados cadastrais e de senhas;**

Golpe da engenharia social

A engenharia social é uma técnica aplicada por golpistas para induzir usuários desavisados a repassarem dados confidenciais, como senhas e dados de cartões ou abrir links para sites infectados. Não é necessário o uso de muito tecnologia para aplicar esse golpe, apenas manipulação psicológica com o usuário, convencendo-o de passar as informações solicitadas.

Os golpistas se passam por funcionários da instituição e 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.

Outra forma de aplicar a engenharia social é quando o criminoso escolhe uma vítima, pega sua foto em redes sociais, e, de alguma forma, consegue descobrir números de celulares de contatos da pessoa. Com um novo número de celular, manda mensagem para amigos e familiares da vítima, alegando que teve de trocar de número devido a algum problema, como, por exemplo, um assalto. A partir daí, pede uma transferência via Pix, dizendo estar em alguma situação de emergência.

Golpe do falso funcionário

O fraudador entra em contato com a vítima se passando por um falso funcionário do banco ou da cooperativa com a qual o cliente tem um relacionamento ativo. O criminoso oferece ajuda para que o cliente cadastre a chave Pix, ou ainda diz que o usuário precisa fazer um teste com o sistema de pagamentos instantâneos para regularizar seu cadastro, e o induz a fazer uma transferência bancária.

É importante ressaltar que os dados pessoais do cooperado jamais são solicitados ativamente pelo Sicoob Coopemata, tampouco funcionários de cooperativas ligam para clientes e cooperados para fazer testes com o Pix. Na dúvida, sempre procure a cooperativa para obter esclarecimentos.

O Sicoob Coopemata busca sempre estar em contato com os cooperados, porém, não solicitamos:

- Acesso a senhas e códigos bancários;
- Acesso ao APP com dados pessoais;
- Atualização de Dispositivos.

CUIDADOS COM O PIX

Com a Lei Geral de Proteção de Dados Pessoais, suas informações têm ainda mais valor. Mesmo contando com o sistema de segurança do Banco Central e do próprio Sicoob, você também precisa tomar alguns cuidados para não ser enganado ao cadastrar, atualizar ou confirmar sua chave Pix.

- Fraudadores podem entrar em contato se passando pelo Sicoob por meio do WhatsApp, ligação telefônica ou links de sites falsos recebidos por e-mail ou mensagem de texto. Para o suposto cadastramento da chave Pix, eles solicitam informações como sua senha, dados pessoais e da conta corrente;

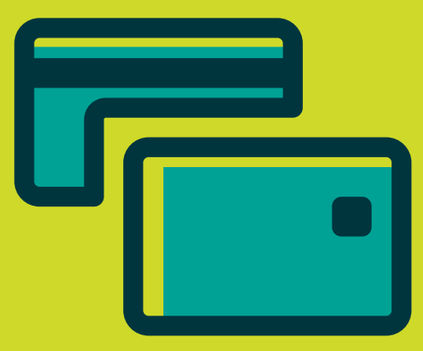
- Apesar de o Pix ser um serviço de conta corrente, o fraudador também pode solicitar dados de cartão de crédito. Nunca forneça senha nem dados como código CVV, número e validade em ligações ou mensagens que receber para cadastramento, atualização ou confirmação da chave Pix ou para qualquer outra finalidade;

- Nunca faça transferências, TEDs, DOCs ou pagamentos em sua conta para fazer um teste para utilização do Pix;

- Não solicitamos que acesse seus dispositivos remotamente para habilitar o Pix;

- Na hora de realizar sua transação utilizando a Chave PIX, sempre confira os dados do “recebedor” da transação, seja pessoa ou estabelecimento;

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



PREVINA-SE CONTRA GOLPES COM CARTÕES

- O Sicoob não envia motoboys ou funcionários à sua residência para retirar cartões destruídos. Se alguém ou alguma empresa se oferecer para isso, cuidado, pode ser golpe;

- Não perca seu cartão de vista, mantenha-o com você e aguarde a chegada da maquininha ou acompanhe a pessoa até ela;

- Ao efetuar uma transação, observe se o cartão devolvido é o mesmo entregue ao funcionário do estabelecimento e confira seu nome. Isso evita que seu cartão seja trocado;

- Não informe o número do seu cartão em sites desconhecidos, ou links recebidos por e-mail ou SMS.

- Sempre confira o extrato de conta corrente e/ou fatura pela internet e, caso tenha alguma despesa que não reconheça, mantenha contato imediatamente com a central de atendimento ou com a sua cooperativa;

- Mantenha os telefones e demais dados cadastrais atualizados, especialmente o número do celular, pois esse é importante para o recebimento de SMS ou contato da área de prevenção e segurança;

- Ao receber um SMS informando sobre uma transação, caso a desconheça, faça contato imediatamente com a central de atendimento ou cooperativa, evitando que novas transações indevidas sejam realizadas;

- Em caso de perda ou roubo do cartão, comunique imediatamente a central de atendimento ou cooperativa para evitar que o seu cartão seja usado indevidamente;

- Não guarde o cartão e a senha juntos, pois em caso de perda ou roubo, quem tiver acesso poderá utilizar o cartão indevidamente.

PRINCIPAIS DICAS

- Mantenha seus dados, principalmente endereço, telefones e e-mails, sempre atualizados em sua cooperativa;

- Cancele todas as contas inativas, tanto bancárias quanto de cartão de crédito. Elas podem ser utilizadas para operações fraudulentas;

- Nunca responda e-mails, telefonemas ou SMS que peçam seus dados bancários, como número de conta, agência e senhas. Na dúvida, ligue para a Central de Atendimento do Sicoob;

- Quando realizar compras pela Internet, fique atento à procedência do site, preferindo sempre lojas conhecidas;

- Preferencialmente, utilize um cartão virtual ao realizar compras online;

- O Sicoob envia apenas e-mail marketing aos seus associados. E lembre-se: o Sicoob nunca solicitará suas senhas/ assinaturas eletrônicas por e-mail;

- Sua senha é pessoal, inequívoca e intransferível. Jamais revele sua senha a terceiros, nem mesmo para um empregado do Sicoob ou para alguém de sua confiança;

- Alguns aplicativos criados para redes sociais podem ser usados como armadilhas para extrair informações. Pesquise sempre a procedência e o que dizem sobre o app antes de autorizá-lo no seu perfil;

- Evite receber cheques de terceiros e não os aceite se possuírem rasuras, borrões e aspecto envelhecido.

Fonte: https://www.sicoob.com.br/web/sicoob/principais-golpes

Conhecendo os principais golpes, é menos provável que você entre numa roubada. Em caso de dúvidas ou suspeitas entre em contato com o Sicoob Coopemata.

WWW.SICOOBCOOPEMATA.COM.BR

SICOOB
Coopemata