



CARTILHA

GOLPE & FRAUDE

Quando o assunto é **se proteger**,
não podemos **pagar para ver**.



O Sicoob Sacramento investe continuamente em tecnologia e segurança para garantir a tranquilidade de seus cooperados e empregados.

Ainda assim, é fundamental que você adote alguns cuidados ao realizar suas operações financeiras, pois a sua segurança, assim como a dos nossos cooperados, está sempre em primeiro lugar.

Pensando nisso, reunimos nesta cartilha as principais dicas do Sicoob para a prevenção contra golpes e fraudes. A informação continua sendo a melhor forma de proteção contra a ação de criminosos.

Boa leitura!



GOLPE OU FRAUDE?

Você sabe qual é a diferença?

Golpe

É quando o criminoso engana a vítima para que ela mesma entregue informações ou dinheiro.

Exemplo: alguém se passando por um funcionário do banco pede sua senha ou código. A vítima participa sem perceber, acreditando que é uma situação legítima.

Resumo: envolve manipulação e engano.

Fraude

É quando o criminoso usa seus dados ou acessa sua conta sem sua autorização.

Exemplo: clonagem de cartão ou invasão de conta bancária. A vítima não participa diretamente da ação.

Resumo: envolve uso indevido de dados ou acesso ilegal.

A informação ainda é a melhor forma de se proteger contra criminosos. Conheça os principais golpes e não entre numa roubada.



Cuidados com você e com a sua empresa!



Golpe Spoofing



Falsa Agência Investigada



Golpe do site falso – phishing



Golpe da falsa oferta



Golpe do falso empréstimo



Golpe "Bença tia"



Golpe do DDA



Malware



Golpe do QR Code



Golpe da mão fantasma



Golpe do Falso Advogado



Golpe do estorno do Pix



Roubo ou furto de celular



Golpe do falso sequestro ou do falso parente



Golpe do falso leilão



Roubo de dados por meio de mensagens falsas – Phishing ou Smishing



Golpe do falso boleto



Golpe do WhatsApp



Golpe da falsa central ou do falso funcionário



Golpe do motoboy

Golpe Spoofing

Como é:

É quando os golpistas usam técnicas de falsificação de identidade digital e se passam por fontes confiáveis, por meio de ligações, e-mails e sites parecidos ou iguais aos canais oficiais do Sicoob. O objetivo é obter informações confidenciais e induzir a vítima a clicar em links maliciosos.

Para se proteger de golpes fique atento às dicas:

- Nunca confie apenas na identificação da chamada;
- Desconfie sempre de pedidos urgentes;
- Não clique em links desconhecidos.



Falsa Agência Investigada

Golpistas, geralmente por telefone, se passam por policiais ou representantes de bancos. Eles dizem que a agência ou gerente da vítima está sob investigação e que o dinheiro corre risco de ser roubado. Para “proteger” os valores, orientam a transferência para uma suposta conta segura, que na verdade pertence aos próprios criminosos.

Para se proteger de golpes fique atento às dicas:

- Desconfie de contatos que pedem transações ou dados pessoais/bancários.
- Instituições como o Sicoob nunca solicitam transferências ou pagamentos em investigações.
- Não compartilhe dados pessoais por telefone, e-mail ou mensagens.
- Em caso de suspeita, procure a instituição pelos canais oficiais.
- Desconfie de urgência: golpistas pressionam para decisões rápidas.
- Informe-se sobre golpes e compartilhe com familiares e amigos.
- Nunca faça transações a pedido de terceiros: você é responsável pela sua conta.



Golpe do site falso – phishing

O golpe do site falso, também conhecido como phishing, é uma técnica que redireciona os usuários para páginas falsas, com o objetivo de obter informações pessoais. Os golpistas podem se passar por instituições legítimas, como bancos e provedores de e-mail, para atrair as vítimas.

Para se proteger de golpes fique atento às dicas:

- Desconfiar de produtos com descontos muito grandes;
- Verificar se o site é verdadeiro antes de fazer qualquer compra;
- Consultar se existem reclamações ou denúncias sobre o vendedor;
- Não pagar por Pix em links enviados;
- Solicitar o código de rastreamento ao vendedor.

Golpe da falsa oferta



O golpe acontece quando golpistas indicam links de sites falsos com ofertas de valores muito atrativas, mas que exigem pagamento exclusivamente por PIX ou boleto, em um falso anúncio em redes sociais. Por isso, o consumidor deve sempre desconfiar de preços muito abaixo do mercado, especialmente em momentos em que o item está sendo muito procurado.

Para se proteger de golpes fique atento às dicas:

- Desconfie de preços muito abaixo do mercado.
- Recebeu promoção? Confira direto no site oficial.
- Cuidado com sites falsos; verifique se começa com "https".
- Prefira cartões virtuais (único para compras e recorrente para assinaturas).
- Evite salvar dados do cartão online e confirme a segurança do site.
- Ative notificações do banco para acompanhar movimentações e identificar suspeitas.

Golpe do falso empréstimo

É a oferta de empréstimos com muitas facilidades, inclusive a promessa de não consultar órgãos de proteção ao crédito ou de oferecer condições mais vantajosas que as do mercado. Geralmente, são divulgados por SMS, WhatsApp, ligações telefônicas, internet, redes sociais, outdoors, rádios e jornais.

Após o contato de interessados e a definição das condições, os golpistas solicitam o pagamento adiantado de taxas (como administrativas ou seguros), sob o pretexto de liberar o crédito. Depois de receberem o dinheiro, eles interrompem o contato com a vítima.

Para se proteger de golpes fique atento às dicas:

- Desconfie de ofertas “fáceis”.
- Nunca faça pagamentos antecipados — instituições não cobram para liberar crédito.
- O Sicoob não pede adiantamentos nem transferências para pessoas físicas.
- Não compartilhe informações do empréstimo nas redes sociais.
- Confirme ofertas apenas nos canais oficiais da cooperativa.
- Se pedirem taxas ou depósitos como garantia, cancele.
- Não forneça dados pessoais a desconhecidos.

Golpe “bença, tia”

Um falso parente telefona para a vítima e muitas vezes quando a vítima atende o telefone o criminoso diz “bença tia”, como se fosse da família. O criminoso cria e conta uma história e solicita um “empréstimo”, uma ajuda imediata para arcar com despesas de uma eventualidade

Assim, o criminoso passa informações bancárias para o envio do recurso, para que a transferência seja realizada.

Para se proteger de golpes fique atento às dicas:

- Não fale o nome da pessoa que poderia ser seu provável parente, dessa forma você evita passar para os criminosos informações que eles podem usar para deixar o golpe mais realista.
- Desconfie de ligações solicitando ajuda financeira. Sempre ligue para a suposta pessoa de outro telefone ou peça a alguém para ligar e confirmar.



Golpe do DDA

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

O DDA é o boleto de forma eletrônica, assim qualquer correção ou alteração no boleto refletirá no DDA.

Malware

Malware é a abreviação de “software malicioso” (malicious software) e se refere a programas criados para infectar o computador de um usuário e causar danos de diferentes formas.

Alguns sinais de infecção incluem mudanças sem permissão, como nova página inicial, barras de ferramentas ou atualizações no navegador, redirecionamento para sites desconhecidos, desativação de proteções e envio de mensagens estranhas para seus contatos. Além disso, queda repentina de desempenho, lentidão e travamentos também podem indicar a presença de malware, que consome recursos do sistema para fins indevidos.

Para se proteger de golpes fique atento às dicas:

- Uma das formas mais comuns de propagação de malware é por e-mail, que pode se passar por empresas conhecidas (como bancos) ou até por contatos pessoais.
- Desconfie de mensagens que pedem senhas ou que trazem links com frases curtas, como “Veja que interessante!”.
- Ao receber e-mails suspeitos, com erros de português, ofertas muito vantajosas ou conteúdos chamativos, não clique em links e exclua a mensagem.
- Mantenha sempre seu navegador, sistema operacional, aplicativos e antivírus atualizados.
- Evite realizar operações importantes em redes Wi-Fi públicas.
- Não clique em links recebidos de desconhecidos por e-mail, SMS, WhatsApp ou outros aplicativos de mensagem.
- Não instale programas ou aplicativos de fontes não confiáveis ou que você não precisa.

Golpe do QR Code

O fraudador, se passando por (funcionário do Sicoob), induz o cooperado, por telefone, a realizar a leitura de um QR Code. Ele cria uma historinha para convencê-lo, contudo o QR Code é para realização de uma transação financeira ou e até mesmo de liberação de dispositivo que foi por ele cadastrado.

Para se proteger de golpes fique atento às dicas:

- O Sicoob nunca solicita atualização do internet banking, assim como não envia QR Code ou links em mensagens de texto.
- Nunca faça transferências, TEDs, PIX ou pagamentos em sua conta corrente com o pretexto de realização de teste.
- Sempre confira todas as informações contidas na tela do celular após leitura de QR Code.



Golpe da mão fantasma

O golpe da “mão fantasma” faz a vítima acreditar que há alguém controlando seu celular remotamente. Os criminosos entram em contato por SMS, e-mail, WhatsApp ou ligação, se passando por funcionários do Sicoob e alegando a necessidade de atualizar um aplicativo.

A partir daí, os golpistas realizam transações em tempo real, como transferências para contas de terceiros, pagamento de boletos e contratação de empréstimos.

Para se proteger de golpes fique atento às dicas:

- Analise as mensagens que receber e não acredite em tudo que lê ou escuta na internet, principalmente em mensagens com códigos ou links que você não sabe porque está recebendo.
- Sempre cheque as informações com sua cooperativa de relacionamento. Se receber alguma ligação ou mensagem, não faça nada. Desligue e, depois, ligue de outro aparelho para o número oficial do Sicoob e confirme a informação.
- O Sicoob não solicita baixa de aplicativos de segurança ou de atualizações.

Golpe do Falso Advogado

O golpe do falso advogado ocorre quando criminosos se passam por advogados ou assistentes, usando dados reais de processos para enganar vítimas. Por telefone ou WhatsApp, informam falsamente a liberação de valores e enviam documentos falsos. Em seguida, solicitam depósitos antecipados com justificativas como taxas ou despesas e, após o pagamento, desaparecem.

Para se proteger de golpes fique atento às dicas:

- Nunca faça pagamentos antecipados sem confirmar com seu advogado de confiança e verifique se a conta é realmente dele.
- Desconfie de contatos inesperados, especialmente com urgência ou linguagem técnica.
- Confirme o profissional pelo ConfirmADV ou canais oficiais do escritório.
- Não compartilhe dados pessoais ou bancários sem validar o contato.
- Lembre-se: advogados não pedem PIX para liberar valores de processos.



Golpe do estorno do pix

Neste golpe, o criminoso realiza um Pix para o cooperado e, em seguida, liga para ele solicitando que devolva o valor para a conta de uma terceira pessoa.

Depois disso, o golpista aciona o Mecanismo Especial de Devolução (MED), alegando que o Pix foi feito por engano. Assim, ele consegue reaver o dinheiro diretamente com a instituição financeira, obtendo uma devolução dupla.

Para se proteger de golpes fique atento às dicas:

- Sempre realize devoluções de Pix diretamente no extrato, utilizando a opção "Devolver".
- Desconfie de solicitações suspeitas e verifique o seu extrato cuidadosamente.
- Nunca forneça informações pessoais ou financeiras para quem está na ligação.

Golpe do falso boleto

O golpe ocorre em transações financeiras entre fornecedores e clientes, geralmente envolvendo o pagamento via boleto bancário. O fraudador se infiltra no processo enviando um e-mail falso que imita o do fornecedor original. Esse e-mail contém um boleto bancário adulterado, quase idêntico ao original, mas com mudanças estratégicas, como na data de vencimento, no código de barras e na sequência numérica. Assim, o cliente é induzido a pagar o valor para a conta do fraudador.

Para se proteger de golpes fique atento às dicas:

- Desconfie de boletos recebidos fora do padrão e confirme com o beneficiário antes de pagar.
- Nunca emita segunda via em sites que não sejam oficiais da instituição financeira.
- Verifique se a logomarca da instituição financeira corresponde aos três primeiros dígitos da linha digitável (ex.: Sicoob = 756).
- Desconfie de boletos com descontos incomuns.
- Negocie sempre pelos canais habituais do beneficiário.
- Em contas de consumo (água, luz, telefone, etc.), confira se a linha digitável começa com 8; caso contrário, não pague.

Roubo ou furto de celular



Imagine estar na rua usando o celular quando ele é roubado. Além da perda do aparelho, há risco de prejuízos financeiros, pois ele guarda dados importantes que podem ser usados em golpes. Embora o App Sicoob seja seguro, é essencial adotar cuidados para proteger sua conta nesses casos. Siga as orientações e evite que suas informações pessoais e financeiras caiam em mãos erradas.

Para se proteger de golpes fique atento às dicas:

- Não salve nem anote senhas no celular e nunca as compartilhe por mensagens ou bloco de notas.
- Evite usar a mesma senha em diferentes contas ou apps.
- Ative bloqueio de tela com senha única e use sempre o duplo fator de autenticação.
- Não utilize a opção “salvar senha” em sites e navegadores.
- Tenha cautela ao usar o celular na rua ou ao volante.
- Guarde o IMEI em local seguro.
- Apague mensagens e fotos com informações sensíveis.

Golpe do falso sequestro ou do falso parente

Criatividade é o que não falta para os criminosos. Eles sempre inventam novas maneiras para extorquir dinheiro das vítimas, muitas vezes apelando para as nossas emoções. O golpe do falso sequestro é um dos mais “tradicionais” da categoria.

A vítima recebe um telefonema de um número desconhecido, informando que um parente próximo está em poder de sequestradores (o que é mentira), algumas vezes chama você de mãe ou pai, e então os criminosos solicitam o pagamento de resgate imediato através de transferência ou depósito. Após contatar a vítima, os golpistas passam informações bancárias de conta corrente para a qual a transferência ou o depósito devem ser realizados.

Para se proteger de golpes fique atento às dicas:

- Não fale o nome da pessoa que poderia ter sido sequestrada. Dessa forma você evita passar para os criminosos informações que eles podem usar para deixar o golpe mais realista.
- Desconfie de ligações comunicando sequestros. Peça para alguém ligar para a pessoa que estaria sendo sequestrada, sem deixar que os criminosos percebam.
- Não passe nenhuma informação pessoal sua ou de seus familiares, não diga, por exemplo, onde mora, o seu nome, quanto ganha, quanto tem na sua conta bancária ou onde tem conta.
- Se conseguir, anote os dados bancários fornecidos pelo golpista e avise a polícias.

Golpe do falso leilão

É um golpe sofisticado e difícil de identificar, exigindo atenção a cada orientação para prevenção. Trata-se de sites falsos que se passam por leiloeiros, anunciando veículos, imóveis ou equipamentos com preços abaixo do mercado para atrair vítimas. Além da falsa venda, há roubo de dados. A página parece legítima, mas o produto nunca é entregue. A pressão do tempo típica de leilões leva a decisões rápidas: ao dar o lance, a vítima “vence”, realiza o pagamento e, após a confirmação, o golpista desaparece e interrompe o contato.

Para se proteger de golpes fique atento às dicas:

- Desconfie de preços muito abaixo do mercado, mesmo em leilões.
- Não faça depósitos para terceiros, como “representantes” ou “parceiros”. Leilões brasileiros usam “.com.br”; sites com “.com” ou “.com/br” podem ser falsos.
- Pesquise a reputação do site antes de se cadastrar.
- Na dúvida, não informe dados bancários ou documentos pessoais.
- Consulte listas confiáveis em sites como Aleibras e Leilão Seguro antes de comprar.
- Verifique no Detran se o leilão está sendo realizado pelo leiloeiro oficial indicado.

Roubo de dados por meio de mensagens falsas (Phishing ou Smishing)

Smishing é uma variação do phishing, mas que se diferencia pelo meio de abordagem: o texto chega por mensagem de SMS no telefone que terá um link malicioso, que leva as vítimas a um formulário usado para roubar as informações.

Para se proteger de golpes fique atento às dicas:

- Atenção ao receber mensagens de SMS que informam sobre bloqueio de acesso ou que pedem atualização de dados pessoais.
- Alguns conteúdos possuem erros de português 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.
- Não abra links de SMS suspeitos e nunca informe seus dados bancários e senhas.ável começa com o dígito 8, do contrário, não pague o documento.



Golpe da falsa central ou do falso funcionário

O golpista se passa por pessoa conhecida ou parente da vítima (normalmente pelo WhatsApp, Telegram, Instagram, Facebook) e alega uma situação de urgência. O cooperado realiza transferências ou pagamentos para conta de terceiros indicados pelo golpista.

Principais tipos de golpes:

- **Conta clonada:** criminosos acessam o WhatsApp da vítima e pedem dinheiro aos contatos.
- **Perfil falso:** criam um número novo com foto de alguém conhecido e solicitam valores.
- **Mensagem de urgência:** pedidos rápidos de dinheiro, Pix ou pagamento de contas.

Como se proteger:

Ative a verificação em duas etapas no aplicativo.

Nunca compartilhe seu código de segurança.

Desconfie de contatos com número diferente, mesmo com foto conhecida.

Confirme sempre pelo número salvo na agenda ou por chamada de vídeo.

Evite transferências solicitadas apenas por mensagem, principalmente para terceiros.



Golpe da falsa central ou do falso funcionário

Golpistas fingem ser da Central de Atendimento do Sicoob e simulam o número de telefone por meio de recursos tecnológicos, como gravações e menus para aumentar a sua confiança. A partir dessa abordagem, solicitam senhas, atualização de sistemas ou liberação de equipamentos ou realização de transferências.

Para se proteger de golpes fique atento às dicas:

- O Sicoob nunca solicita atualização ou cadastramento de módulo de segurança em computadores, celulares ou senhas e nem a instalação de softwares ou componentes em navegadores via telefone. Por isso, nunca passe essas informações pra ninguém.
- E lembre-se: o telefone da Central de Atendimento do Sicoob é um número para você ligar. O Sicoob não realiza ligações a partir desse número.



Golpe do motoboy

O fraudador liga para o cliente se passando por um falso funcionário e questiona sobre uma suposta compra no cartão. O criminoso, então, pede as senhas para supostamente bloquear o cartão, solicita que corte o cartão ao meio e informa que mandará um motoboy para recolher o cartão para "perícia".

Atenção: O Sicoob não envia motoboys ou funcionários para recolher seu cartão, mesmo quando ele precisa ser substituído devido a transações suspeitas ou não, e também não pede celulares ou digitação de senha.

Para se proteger de golpes fique atento às dicas:

- As instituições financeiras nunca recolhem os cartões dos clientes, mesmo que eles estejam vencidos ou bloqueados.
- Ao se desfazer de um cartão, corte o chip ao meio.
- Nenhum atendente do Sicoob solicita informações sensíveis por telefone.
- Nunca informe seus dados bancários e senhas por telefone.
- Se alguém ou alguma empresa se oferecer para buscar o seu cartão, cuidado, pode ser golpe.
- Se não for mais usar o cartão, danifique o chip (corte-o em algumas partes), pois assim seu reuso é evitado.

ATENÇÃO ATENÇÃO ATENÇÃO

Se você cair no golpe, siga as instruções abaixo:



Entre em contato imediatamente com sua cooperativa de relacionamento ou ligue para o **SAC pelo número 0800 724 4420, opção 5;**

Registre um **Boletim de Ocorrência (BO)** para sua segurança e para formalizar a situação.

Lembre-se: segurança começa com você. Um clique pode custar caro!

Fique atento. Previna-se. Compartilhe essa dica!

No Sicoob, cooperamos pela segurança das suas finanças.

Selecione um item abaixo para conferir as dicas de segurança:



Celulares



Sistema de Valores a Receber



Internet Banking



Pix



Caixas Eletrônicos



Boletos



Cartões



E-mail



Compras



Redes Sociais



Senhas



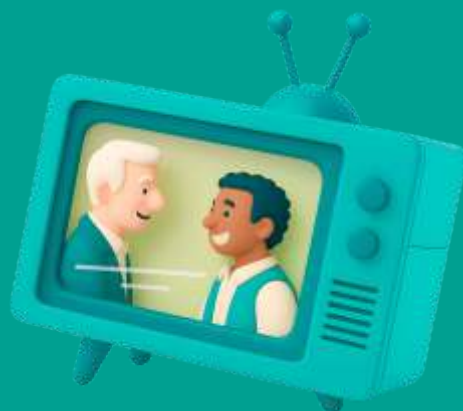
Internet



Cheques



Glossário da Segurança Digital



Cuidados no uso do celular para evitar golpes

Fique por dentro: como se proteger

O uso do celular para consultas e transações bancárias já faz parte da rotina. Por isso, é essencial adotar alguns cuidados para proteger seus dados.

Ligações e contatos

- Nunca informe dados pessoais ou bancários por telefone.
- Em contatos suspeitos do Sicoob, procure a cooperativa.
- Confirme dados com descrição e use canais oficiais.
- Verifique a origem de mensagens e evite links suspeitos.
- Antes de enviar dinheiro, confirme por ligação.
- Desconfie de números diferentes, mesmo com fotos conhecidas.

Segurança no celular

- Use biometria, senha e bloqueio automático.
- Evite salvar contatos como “mãe” ou “pai”. Não empreste seu celular nem use aparelhos de terceiros.
- Instale antivírus, ative rastreamento e baixe apps só de lojas oficiais.
- Anote o IMEI (*#06#) e não guarde fotos de cartões.
- Mantenha tudo atualizado e oculte notificações na tela bloqueada.
- Utilize o programa Celular Seguro.

Senhas e acessos

- Não salve nem compartilhe senhas.
- Evite guardar dados sensíveis em anotações.
- Use senha exclusiva para apps financeiros.
- Crie senhas fortes e evite informações óbvias.
- Ative a autenticação em duas etapas e não use redes sociais para login.

Como se proteger ao movimentar sua conta na internet.

Contar com o internet banking do Sicoob é ter à disposição uma ferramenta moderna e segura para cuidar do seu dinheiro. Ainda assim, você deve seguir algumas dicas na hora de movimentar sua conta na internet.

- Ao acessar o internet banking – <https://ib.sicoobnet.com.br/inetbank/login.jsp> – um cadeado fechado aparecerá após você digitar cooperativa e conta, ao lado da URL. Ele indica que temos um certificado para garantir um acesso seguro. Fique de olho: caso não apareça, cancele imediatamente a operação.
- A senha de efetivação ou QR Code são utilizados apenas para concluir transações financeiras solicitadas por você.
- A senha de efetivação e o QR Code não são solicitados para atualizações de segurança ou instalações de arquivos.
- O Sicoob não solicita atualizações de programas por e-mail, celular, SMS ou internet.
- Ao realizar uma transação via QR Code, confira no visor do seu celular se os dados batem com as informações apresentadas no computador.
- Sempre verifique a data de seu último acesso. Caso note alguma irregularidade, ligue imediatamente para a Central de Atendimento.



Tome alguns cuidados ao utilizar os terminais

- O Sicoob disponibiliza caixas eletrônicos em diversos locais no Brasil, mas por estarem em áreas públicas, é essencial ter cuidado ao utilizá-los.
- Não aceite ajuda de estranhos nem permita aproximação durante o uso. Proteja sua senha ao digitá-la e nunca a compartilhe. Ao finalizar, confira se o cartão é realmente o seu para evitar golpes de troca, que podem ocorrer com distrações ou falsas ajudas.
- Evite aceitar propostas envolvendo sua conta ou transferências suspeitas. Não filme, fotografe ou compartilhe QR Codes nem realize videochamadas durante o uso do caixa.
- Sempre finalize a operação usando a tecla “Sair” e não retorne ao terminal se alguém solicitar. Fique atento ao redor, especialmente em saques, para evitar o “golpe da saidinha”, em que criminosos observam e abordam clientes após retiradas.
- Se precisar de ajuda, procure apenas pessoas de confiança ou funcionários identificados. Não se afaste do terminal antes de concluir a operação e redobre a atenção à noite, quando o risco é maior.
- Solicitar o código de rastreamento ao vendedor.

Previna-se contra golpes, no débito ou no crédito.

< VOLTAR

O Sicoobcard oferece praticidade, mas exige cuidados para evitar fraudes.

O Sicoob não envia pessoas para retirar cartões em sua casa, desconfie. Nunca perca seu cartão de vista, confira se ele devolvido é o seu e não o empreste nem compartilhe dados (número, validade, código ou senha).

Evite informar dados em sites ou links desconhecidos. Prefira usar o cartão presencialmente e mantenha sua senha em sigilo. Utilize o App Sicoobcard para acompanhar movimentações, ativar notificações e controlar limites e funções.

Para se proteger de golpes fique atento às dicas:

- Desconfie de ofertas “fáceis”.
- Nunca faça pagamentos antecipados — instituições não cobram para liberar crédito.
- O Sicoob não pede adiantamentos nem transferências para pessoas físicas.
- Não compartilhe informações do empréstimo nas redes sociais.
- Confirme ofertas apenas nos canais oficiais da cooperativa.
- Se pedirem taxas ou depósitos como garantia, cancele.
- Não forneça dados pessoais a desconhecidos.

Aprenda a não entrar em roubadas

Fique por dentro

Antes de comprar, pesquise a reputação da empresa, verifique canais de atendimento e avaliações de clientes.

Use apenas dispositivos seguros — evite computadores públicos. Nunca forneça dados pessoais ou do cartão sem confirmar a autenticidade do site. Prefira páginas com <https://> e cadeado de segurança.

Desconfie de ofertas muito vantajosas e confirme sempre o valor da compra e a proteção da senha (asteriscos). Destrua recibos com dados sensíveis.

Para mais segurança online, use cartões virtuais:

- **Compra única:** válido para uma única transação.
- **Recorrente:** ideal para assinaturas e fácil de cancelar em caso de fraude, sem afetar o cartão físico.



Proteja essas informações para não sair no prejuízo

Sua senha é só sua: é ela que garante o acesso seguro à sua conta. Por isso, é muito importante seguir algumas dicas e recomendações para criar senhas fortes e mantê-las protegidas.

- Sua senha é pessoal e intransferível — não compartilhe com ninguém.
- O Sicoob nunca pede sua senha.
- Proteja sua digitação — evite olhares de terceiros.
- Memorize a senha — não anote nem salve em dispositivos.
- Crie senhas fortes (misture letras, números e símbolos); evite dados pessoais e sequências óbvias.
- Não informe senhas em sites suspeitos ou links recebidos por mensagens.
- Acesse apenas o site oficial: www.sicoob.com.br
- Troque sua senha regularmente e imediatamente em caso de suspeita.
- Não reutilize senhas antigas.

Aprenda a cuidar bem dos seus talões

Fraudes com cheques provocam prejuízo financeiro e muita dor de cabeça. Folhas de cheques são documentos pessoais e, como tal, devem ser tratados com cuidados especiais para que você não pague a conta.

- Em caso de roubo, furto ou extravio entre em contato com sua cooperativa de relacionamento para efetuar o bloqueio provisório das folhas.
- Guarde as folhas de cheque em local seguro e fora do acesso de outras pessoas.
- Evite emprestar suas folhas de cheques para outras pessoas.
- Ao emitir um cheque, tome o cuidado de cruzá-lo e colocar o nome do beneficiário.
- Inutilize os talões/folhas de cheques de contas encerradas.
- Mantenha seu cadastro atualizado para possibilitar agilidade no contato e confirmação das informações em caso de dúvidas.
- Acompanhe regularmente seu extrato e os cheques debitados.
- Não permita que outras pessoas preencham seu cheque.
- Utilize sua própria caneta com tinta azul ou preta. Tome cuidado com canetas oferecidas por outras pessoas.
- Evite receber cheques de terceiros e não os aceite se possuírem rasuras, borrões e aspecto envelhecido.

Conheça os termos e os respectivos significados sobre a segurança da informação

- **Antivírus / Firewall:** protegem o computador contra ameaças e acessos não autorizados.
- **Malware / Vírus / Cavalo de Troia / Keylogger:** programas maliciosos que roubam dados ou danificam sistemas.
- **Criptografia / HTTPS / SSL:** tecnologias que protegem informações durante a navegação.
- **Conexão segura (cadeado):** indica que os dados estão protegidos em um site.
- **Phishing / Scam / Engenharia social:** golpes que tentam enganar o usuário para roubar informações.
- **Spam / Correntes:** mensagens não solicitadas, muitas vezes usadas para golpes ou vírus.
- **Site / URL / Domínio / IP:** formas de identificar e acessar páginas na internet.
- **Browser (navegador):** programa usado para acessar sites (ex: Chrome, Firefox).
- **Download / Upload:** baixar ou enviar arquivos pela internet.
- **Link:** acesso que leva a outra página ou site.
- **Wi-Fi / Roteador / Banda larga:** formas de conexão à internet.
- **Servidor / Rede:** sistemas que armazenam e compartilham dados.
- **E-commerce / Loja virtual / Internet Banking:** serviços online para compras e operações bancárias.
- **Cookies:** arquivos que armazenam informações de navegação.
- **Atualizações (update/upgrade):** melhorias de segurança e desempenho de sistemas.



Saiba como utilizar o Sistema de Valores a Receber com segurança

O Banco Central lançou uma plataforma para consultas, pelos cidadãos e pelas empresas, de valores a receber. Havendo saldo a ser restituído, o usuário será informado da data em que poderá ter acesso ao valor e solicitar a devolução.

Para que você aproveite essa novidade com segurança, reunimos algumas informações que podem te ajudar a se prevenir de golpes. Confira:

É verdade que:

- O único site para consulta ou solicitação de valores é o valoresareceber.bcb.gov.br. **Qualquer outro link é golpe, não clique.**
- O usuário precisará de um login Gov.br, nível prata ou ouro, para acessar o Sistema Valores a Receber.
- Não serão enviados links e não haverá contato do Banco Central com os usuários. Fique atento e nunca compartilhe seus dados.

É fraude:

- Qualquer solicitação de pagamento para receber os valores. Fique atento para não ficar no prejuízo.
- Links suspeitos enviados por e-mail, SMS, WhatsApp ou Telegram. Nunca clique e nem forneça suas informações.



Entenda os cuidados que você precisa ter com a nova funcionalidade

Mesmo com os sistemas de segurança do Banco Central e do Sicoob, é importante que você tome alguns cuidados ao cadastrar, atualizar ou confirmar sua chave Pix.

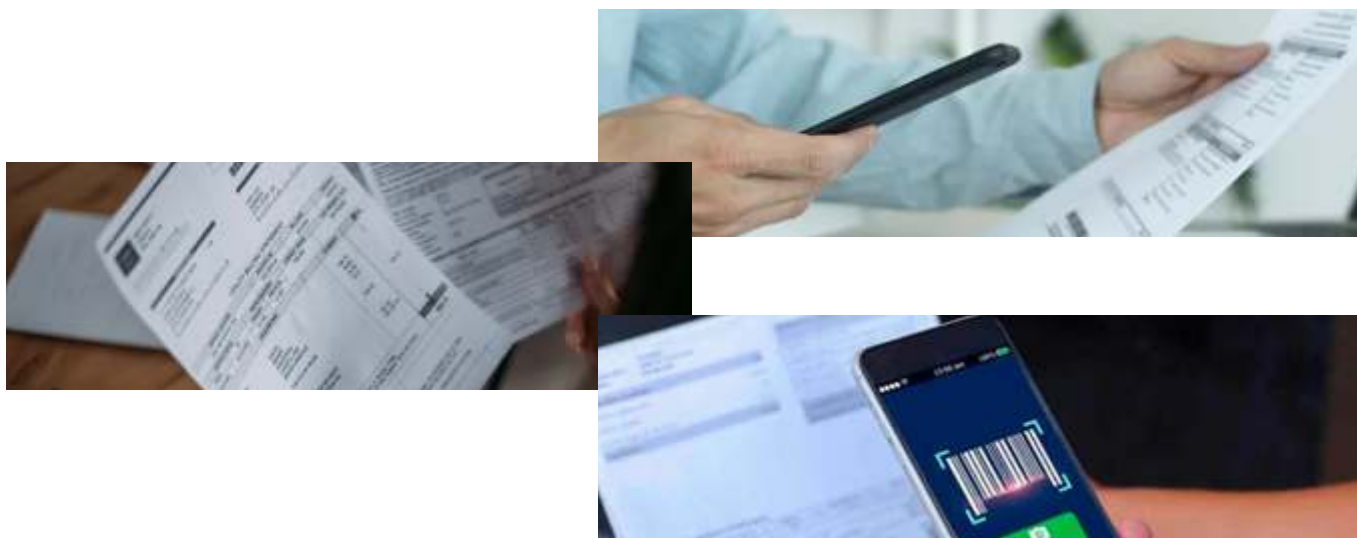
Golpistas podem tentar se passar por atendentes do Sicoob por meio de ligações, mensagens ou links falsos, solicitando dados pessoais e bancários.

Fique atento:

- O Sicoob não pede senha nem dados do cartão (como CVV, número ou validade). Não faça transferências ou testes para ativar o Pix.
- O Sicoob não acessa seu celular ou computador remotamente.
- Evite clicar em links recebidos por mensagens ou redes sociais.

Boas práticas:

- Cadastre sua chave Pix somente pelo App Sicoob.
- Sempre confira os dados do recebedor antes de confirmar a transação.
- Verifique se o site é oficial antes de inserir qualquer informação.
- Mantenha as notificações do app ativas para acompanhar movimentações.
- Lembre-se sempre que o cadastramento da Chave Pix é realizado pelo App Sicoob.



Aprenda a identificar boletos fraudulentos

Fique atento ao pagar boletos para evitar fraudes. Desconfie sempre que receber um boleto por um canal incomum e confirme sua autenticidade com o beneficiário antes de pagar.

Emita a segunda via apenas no site oficial da instituição financeira.

Verifique se a logomarca corresponde aos três primeiros números da linha digitável (ex.: Sicoob = 756).

Desconfie de boletos com descontos inesperados ou enviados fora do padrão habitual. Sempre utilize o canal de comunicação já conhecido com o beneficiário.

Em contas de serviços (água, luz, telefone, internet), confira se a linha digitável começa com o número 8; caso contrário, não efetue o pagamento.

Saiba como identificar mensagens maliciosas

Para manter a proximidade com os cooperados, enviamos e-mails sobre promoções e benefícios, mas nunca solicitamos senhas, dados pessoais, bancários ou transações.

- Desconfie de mensagens com erros, ofertas “imperdíveis”, imagens de celebridades ou remetentes desconhecidos. Não clique em links e exclua o e-mail.
- Se receber mensagens em nome do Sicoob com links ou anexos, encaminhe para denunciefraude@sicoob.com.br e apague. Não acesse o conteúdo, pois pode conter vírus.
- E-mails que pedem atualização de dados também são suspeitos. Nesses casos, confirme diretamente com a empresa ou pelo site oficial.

No âmbito dos golpes praticados diante de engenharia social que são crescentes no mercado brasileiro, sugerimos as seguintes atenções:

- Nenhuma solicitação de cadastramento ou inclusão de dados pessoais é enviada aos cooperados, seja por e-mail ou por meio das redes sociais.
- Não informe o número do seu cartão e senha nas páginas direcionadas pelos links recebidos por e-mail, pois eles podem direcionar para uma página falsa de cooperativa ou de algum parceiro.

Curta as amizades, mas evite os fraudadores



O uso das redes sociais cresce a cada ano, atraindo também criminosos em busca de aplicar golpes.

Evite clicar ou compartilhar links de promoções “imperdíveis” ou notícias sensacionalistas, pois podem conter vírus e ameaças. Não divulgue dados pessoais como endereço, telefone ou e-mail.

Se receber mensagens suspeitas de amigos, confirme a autenticidade antes de interagir; caso contrário, exclua.

Não salve senhas nos dispositivos e sempre faça logout ao sair. Além disso, pesquise a procedência de aplicativos antes de autorizá-los, pois podem ser usados para roubar informações.

Descubra como navegar em segurança

Quando você sai de casa, provavelmente toma cuidados para se proteger de assaltos e outros perigos. Na internet, é igualmente importante colocar em prática alguns procedimentos de segurança.

- Mantenha todos os navegadores atualizados, pois as versões atuais contêm mecanismos de segurança mais aprimorados.
- Mantenha o antivírus atualizado e adquira apenas software originais. Faça sempre uma varredura em arquivos baixados e anexos recebidos por e-mail.
- Não acesse o site do Sicoob através de links recebidos por e-mail, SMS ou redes sociais. Sempre digite o endereço www.sicoob.com.br no seu navegador. Observe se o endereço começa com <https://> e se há um cadeado ao lado; isto significa que suas informações estão protegidas.
- Não realize consultas ou transações financeiras em computadores públicos, principalmente em lan houses e cyber cafés.
- Nunca realize transações em sites cuja url não comece com <https://> e que não possua um cadeado no navegador.

ATENÇÃO ATENÇÃO ATENÇÃO

Se você cair no golpe, siga as instruções abaixo:



Entre em contato imediatamente com sua cooperativa de relacionamento ou ligue para o **SAC pelo número 0800 724 4420, opção 5;**

Registre um **Boletim de Ocorrência (BO)** para sua segurança e para formalizar a situação.

Lembre-se: segurança começa com você. Um clique pode custar caro!

Fique atento. Previna-se. Compartilhe essa dica!



SICOOB
Sacramento