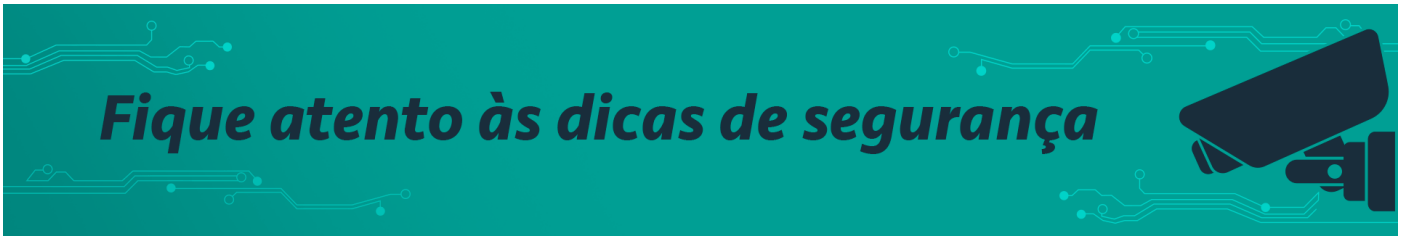

Sicoobnet

- Ao acessar o Sicoobnet - https://ib.sicoobnet.com.br/inetbank/login.jsp - um cadeado fechado aparece 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 é utilizada apenas para concluir transações financeiras solicitadas por você.

- A senha de efetivação não é solicitada 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.

- Sempre verifique a data de seu último acesso. Caso note alguma irregularidade, ligue imediatamente para a Central de Apoio ao Internet Banking.

Senhas

- A senha é pessoal e intransferível, ou seja, você não deve compartilhá-la com ninguém.

- Não permita que ninguém veja você digitando-as, tome cuidado ao utilizar os Terminais de Autoatendimento e ao realizar compras.

- Memorize-as, não anote e nunca as guarde junto com o cartão.

- Não fale sua senha por telefone a ninguém.

- Evite utilizar data de nascimento, telefones, números de documentos ou sequências para criá-las.

- Não as digite em sites desconhecidos, ou em páginas abertas através de links recebidos por e-mail ou SMS.

Acesse o site do Sicoob digitando no navegador o endereço oficial www.sicoob.com.br e evite acessar links patrocinados obtidos através de ferramentas de busca como Google/Yahoo.

- Use senhas diferentes e troque-as com frequência.

Email

- Buscando aprimorar o atendimento e o relacionamento com seus associados e clientes o Sicoob passou a utilizar o e-mail como um canal adicional de comunicação para envio de mensagens informativas sobre promoções e benefícios. Assim, não são enviadas solicitações de dados pessoais, bancários, senhas ou solicitada a realização de transações.

Fique Atento!

- Desconfie de e-mails com erros de português, links com ofertas imperdíveis, imagens de celebridades ou e de remetentes desconhecidos; não clique no link e apague o e-mail.

- Caso receba qualquer mensagem em nome do Sicoob que contenha links ou anexos, encaminhe para denunciefraude@sicoob.com.br e os apague. Não clique nos links ou anexos existentes nestes e-mails, pois podem conter vírus.

- 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.

Internet

- Mantenha os navegadores atualizados com as versões mais atuais.

- Mantenha o antívírus 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.

Telefones

Celular

Utilizar o celular para realizar consultas e transações bancárias já faz parte do dia a dia, mas é preciso tomar alguns cuidados para garantir a proteção dos seus dados e acessos:

- Jamais empreste seu telefone celular para pessoas desconhecidas. Mesmo com senhas de acesso, seus dados podem ficar armazenados, facilitando o acesso indevido.

- Da mesma forma, nunca use celulares de terceiros para acessar a sua conta.

- Existem vírus para celulares. Baixe antivirus adequado para seu celular.

- Quando usar serviços via telefone, seja discreto ao confirmar seus dados cadastrais. Isso impede que suas informações sejam ouvidas e usadas por pessoas mal-intencionadas.

Telefone Fixo

- Muito cuidado ao receber ou fazer ligações para centrais de atendimento. Números falsos são espalhados pela Internet, ou enviados por SMS, e-mail e redes sociais.

- Contate o Sicoob somente dos números do site oficial www.sicoob.com.br.

-Tenha cuidado com ligações recebidas. O Sicoob não liga para cooperados solicitando senhas, número de cartão e dados pessoais e bancários.

Whatsapp e SMS

Caso receba mensagens suspeitas contendo links de Whatsapp, Telegram ou similares, encaminhe para o e-mail denunciefraude@sicoob.com.br.

Caixa Eletrônico

O caixa eletrônico é um canal alternativo de atendimento e atende aos clientes em milhares de pontos espalhados pelo Brasil. Por ficarem em locais de acesso público, é importante que você tome alguns cuidados ao utilizar esses terminais:

Nunca aceite ajuda de estranhos e não permita que estranhos se aproximem quando estiver utilizando um caixa eletrônico e proteja o que está digitando para que ninguém veja.

- Após utilizar o caixa eletrônico, confira se o cartão que está guardando é o seu.

- Nunca aceite propostas, como a transferência de valores para sua conta, tampouco o uso da sua conta por terceiros para transações que não são de seu interesse. Proteja-se de golpes e outros transtornos.

- À noite, redobre o cuidado evite usar Máquinas de Autoatendimento. Nesse período, a circulação de pessoas diminui e você fica mais exposto a riscos.

Cartão

- O Sicoob não envia motoboys ou funcionários à sua residência para retirar cartões.

- 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, confira seu nome. Isso evita que seu cartão seja trocado.

- Não empreste seu cartão a outras pessoas, seu cartão é pessoal e intransferível.

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

- Não empreste o cartão ou fornecer seus dados (Número, código de segurança, validade e senha) a outras pessoas.

- 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.

- Guarde os comprovantes de venda, esse documento comprova que a sua compra foi aprovada. Confira-os mensalmente juntamente com o extrato de conta corrente e/ou fatura, isso ajuda a se recordar das compras que efetuou.

- 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, mantenha 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.

- Caso necessário, ao efetuar um saque, aceite apenas a ajuda de pessoas conhecidas ou de um funcionário da cooperativa identificado pelo crachá.

- Não se ausente do terminal até que o saque seja concluído.

- Caso o cartão fique retido no terminal, solicite a ajuda de um funcionário da cooperativa, sem desviar a atenção do terminal de saque.

Boletos

- Quando receber um boleto para pagamento de forma **não** usual, ou seja, de forma diferente da que costumeiramente o recebe de seu fornecedor, desconfie! Confirme junto ao beneficiário a legitimidade do documento antes de efetuar o pagamento.

- Nunca emita segunda via de boleto em site que **não** seja o da instituição financeira emissora do boleto. Você provavelmente emitirá um documento fraudado que não quitará a tua dívida com o beneficiário.

- Confira sempre se a logomarca da instituição financeira emissora do boleto corresponde ao seu número junto ao Banco Central do Brasil, que são os três primeiros números da linha digitável. Por exemplo, o Sicoob possui o número 756, logo, um boleto com a logomarca do Sicoob e que a linha digitável **não** começa com 756 é um boleto fraudado.

- Desconfie sempre de descontos concedidos com o envio de uma segunda via de boleto.

- Entre em acordo com o beneficiário do boleto quanto o canal de comunicação pelo qual os boletos serão costumeiramente enviados.

- Se for pagar documentos relacionados a contas de convênios, por exemplo, água, luz, telefone, faturas de TV por assinatura e Internet, faturas de operadoras de telefonia celular; verifique se a linha digitável inicia com o dígito 8, do contrário, **não** pague o documento.

- Faça **aqui** o download da cartiha.

Cheques

Folhas de cheques são documentos pessoais e, como tal, devem ter cuidados especiais:

- 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.

Dicas Gerais

1º ACESSO

Para garantir um acesso protegido, é importante reconhecer elementos de segurança e utilizar corretamente nossos dispositivos de segurança, entre outras dicas.

COMPRAS

Na hora de fazer compras, on-line ou não, é importante ser cuidadoso e adotar atitudes mais seguras.

- Recomendamos pesquisar a empresa responsável antes de concretizar sua compra. Observe se há Canais de Atendimento em caso de troca ou reclamação, leia comentários sobre os serviços prestados e se existem políticas de segurança.

- Faça compras em computadores seguros. Se o computador for público, evite comprar e informar suas senhas.

- Só forneça dados do cartão ou dados pessoais após certificar-se da origem e idoneidade do solicitante.

- Ao digitar seus dados, observe se a url começa com https:// e se aparece um cadeado fechado ao lado, identificando que o ambiente é seguro.

- Ofertas e promoções imperdíveis são golpes comuns na Internet. Para não correr riscos, descarte as mensagens imediatamente.

- Confira sempre o valor da sua compra e se a sua senha aparece como asteriscos no visor.

- Os recibos do seu cartão possuem informações pessoais. Por isso, destrua todos antes de jogá-los no lixo.

Redes Sociais

As redes sociais vieram para ficar e devemos tomar cuidados para não cair em armadilhas que podem transitar por estas redes.

- Evite clicar ou compartilhar links de promoções imperdíveis e notícias do tipo: "Você não vai acreditar no que aconteceu" e "Ninguém previa o que estava por vir". Elas podem instalar vírus e outras ameaças que deixarão suas informações vulneráveis.

- Para não colocar a sua segurança em risco,não revele informações pessoais, como endereço, telefone e e-mail. Você pode atrair pessoas mal-intencionadas e até criminosos.

- Se receber uma mensagem estranha de algum amigo, confirme se realmente foi enviada por ele. Caso contrário, não clique em nada e delete imediatamente.

- Não permita que o site salve as suas senhas e sempre dê logout antes de sair do computador ou celular. Assim, você impede o acesso de outras pessoas à sua conta.

- 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.

Principais Golpes

Ataque pela internet

Usuário recebe link ou arquivo por e-mail que, ao ser clicado, altera configuração de segurança do computador, permitido acesso remoto por fraudadores.

Mensagens falsas

Por e-mail ou celular, a pessoa recebe mensagens com link que leva a páginas faldas que capturam informações do cliente.

Phishing

Golpistas enviam mensagens eletrônicas que se passam por comunicação oficial do Sicoob (ou outro site popular); é comum essa mensagem informar que, se a pessoa não fizer os procedimentos que estão naquele e-mail haverá consequência séria, só que ao clicar no link o usuário é redirecionado para uma página falsa do Sicoob.

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 carga 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.

Estelionatários usam WhatsApp como ferramenta para aplicar golpe

Para aplicar o golpe, o criminoso entra em contato, através do WhatsApp, com um amigo próximo ou um parente da vítima que teve o celular clonado, perguntando se a pessoa tem acesso ao banco via computador ou celular. Diante da resposta afirmativa, o golpista pede ao amigo faça uma transferência de urgência, com a promessa de devolver o dinheiro em espécie. Ele passa o número da conta em que o dinheiro deve ser depositado para concretizar o crime. As vítimas acabam acreditando na situação, uma vez que o pedido vem direto do número de telefone da pessoa conhecida. Por isso antes de fazer qualquer transação bancária a pedido de um parente ou amigo, a pessoa entre em contato por telefone ou pessoalmente, com que está fazendo o pedido.

Cuidado com os documentos

A maioria dos documentos acontece com o uso de documentos roubados, furtados ou extraviados. Se você foi vítima de uma destas situações, a primeira atitude a ser tomada é registrar um Boletim de Ocorrência (BO). No primeiro caso (roubo), você deve ir até uma delegacia, nos demais, você pode emiti-lo através do site de Secretaria de Segurança Pública.

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".

Golpe do DDA

Consiste no envio de falso e-mail informando sobre descontou e por isso solicitam que desconsiderem o pagamento do DDA e realizem o pagamento do novo boleto enviado pelo e-mail. Dessa forma, ao efetuar o pagamento desse "novo boleto" os recursos são desviados para outra pessoa, portanto a quitação da obrigação prevista no DDA não será realizada, assim a dívida permanecerá.

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. Forma de ação: Após contatar a vítima nas formas acima descritas, os golpistas passam informações bancárias de conta corrente para a qual a transferência deve ser remetida.

Proteja-se:

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

Falso empréstimo

É a oferta de empréstimos para pessoas negativadas com a promessa de não consultar órgãos de proteção ao crédito. Forma de ação: Anúncios em outdoors, rádios, jornais, Internet, mídias sociais, etc., 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.

Proteja-se:

- Desconfie das facilidades ofertadas.
- Não efetue qualquer pagamento antecipado de taxas administrativas ou seguros prestamistas. Essa não é a prática adotada por instituições financeiras sérias.

- O Sicoob nunca pede pagamento antecipado de taxas administrativas ou seguros prestamistas para liberar empréstimos.

Cadastro de Computadores

Para tornar as suas transações na internet banking (SicoobNet) mais seguras, o Sicoob trabalha com a funcionalidade de segurança "Cadastro de Computadores".

Essa ferramenta identifica o computador do usuário a partir de informações da máquina e com isso evita que terceiros possam movimentar a conta corrente utilizando computadores não cadastrados.

Para maiores informações clique na opção Cadastramento de Computadores.

Teclado Virtual

O teclado virtual é a maneira mais segura de usar o internet banking do Sicoob, pois aumenta a proteção contra diversos tipos de vírus, principalmente aqueles que monitoram a digitação do teclado.

Ao invés de digitar a sua senha no teclado do seu computador, você deverá utilizar o teclado virtual e com o "mouse" clicar nos números correspondentes a sua senha de acesso ao internet banking (SicoobNet).

Com ele, você conta com uma proteção adicional contra vírus ou programas que capturam senhas e podem estar instalados no computador que você utiliza para acessar sua conta corrente.

O teclado virtual é mais uma segurança para você acessar as informações de seu relacionamento conosco. Para mais informações, acesse a opção Teclado virtual.