QUEM AVISA, AMIGO É.

Alerta contra golpes e fraudes.

Por onde começar?

Para ficar cada vez mais protegido, **conheça algumas dicas** que você pode implementar na sua rotina a partir de hoje:

Senha

- Crie senhas fortes sempre: maiúsculas, minúsculas, números e caracteres especiais.
- Jamais use como senha informações fáceis de adivinhar, como datas de nascimento, sequências de teclado, placa de carro ou números de telefone.
- Não compartilhe suas senhas ou use a opção "salvar senha" em dispositivos, navegadores, sites e apps.
- Não utilize o bloco de notas do seu celular para anotar senhas ou informações confidenciais.
- Ative o segundo fator de autenticação dos seus apps de mensagens, redes sociais e e-mails.

Cartões

- Não empreste seu cartão a outras pessoas.
- Não informe o número do seu cartão em sites desconhecidos ou links recebidos por e-mail/ SMS.
- Em caso de perda, roubo ou transações não reconhecidas, comunique imediatamente a central de atendimento ou a sua cooperativa.
- Ao pagar, não entregue o cartão para alguém inserir na maquininha, faça você mesmo este processo.

Celular e mensagens

- Instale o aplicativo "CelularSeguro", ele possibilita que vítimas de furto e roubo possam bloquear o aparelho e seus aplicativos em poucos cliques.
- Use a biometria facial ou digital para desbloqueio da tela inicial do celular.
- Evite salvar seus contatos no aparelho celular com apelidos, como: pai, mãe, irma, tio, tia etc.
- Nunca use celular de terceiros para acessar as suas contas.
- Habilite a opção de rastreio e bloqueio do celular remotamente.
- Baixe aplicativos somente nas lojas oficiais.
- Não guarde fotos de cartões de crédito.
- Não clique em links suspeitos ou que apresentem vantagens exageradas.
- Anote o IMEI do telefone. Com ele será mais fácil bloquear o celular em caso de roubo ou furto. Basta digitar *#06# no celular e o número aparecerá.

Ligações

- Nunca forneça seus dados pessoais e bancários, como senhas, códigos e números de cartão por meio de ligação.
- Muito cuidado ao receber ou fazer ligações para centrais de atendimento. Contate o Sicoob somente por meio dos números disponibilizados no site oficial www.sicoob.com.br.

Compras

- Verifique sempre o site a reputação da empresa da qual pretende fazer compras online.
- 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.
- Sempre que realizar uma compra na internet, proteja o seu cartão físico e crie um cartão virtual.

ATENÇÃO

O SICOOB NUNCA...

- **Entra em contato** para informar tentativas de acesso em sua conta e compras suspeitas realizadas nos seus cartões.
- **Solicita acesso remoto** aos seus dispositivos.
- **Envia motoboys ou funcionários** à sua residência para retirar cartões destruídos.
- **Pede seus dados** pessoais, bancários, senhas de acesso ou códigos enviados por SMS/E-mail
- **Requer atualizações de segurança** por e-mail, celular, SMS ou internet.
- Pede que você faça **transações financeiras** para assegurar sua conta.

Golpes e fraudes

Saiba como reagir caso passe por um dos golpes ou fraudes a seguir:

Falsa Central de Atendimento/Falso funcionário

Como acontece?

Os criminosos entram em contato por telefone, e-mail ou mensagem de texto, fingindo ser funcionários do Sicoob, e tentam convencer as vítimas a fornecerem dados sigilosos ou realizarem transações financeiras.

O que fazer?

Desconfie de contatos não solicitados, não forneça informações pessoais ou financeiras e entre em contato com o Sicoob pelos canais de atendimento oficiais ou vá até sua agência. Se você foi supostamente alertado sobre compras indevidas no seu cartão, consulte a fatura e as transações recentes no próprio APP Sicoob.

Link falso

Como acontece?

Os golpistas enviam mensagens de e-mail ou texto com links que aparentam ser de empresas conhecidas, como bancos ou lojas online, e solicitam que as vítimas cliquem nesses links para realizar alguma ação, como verificar uma transação suspeita ou atualizar informações de cadastro.

Ao clicar no link, as vítimas são redirecionadas para um site falso, que pode roubar suas informações pessoais, como senhas ou números de cartão de crédito.

O que fazer?

Nunca clique em links suspeitos ou baixe arquivos de fontes não confiáveis. Se receber uma mensagem com um link suspeito, verifique diretamente com o Sicoob pelos canais oficiais de atendimento.

Esteja atento a esses três detalhes no endereço eletrônico: possuir o "https", o cadeado na barra de navegação e a inscrição “site seguro”. Se não encontrar, não compartilhe seus dados pessoais nem financeiros.

Preste atenção em erros ortográficos: um e-mail legítimo de grandes empresas raramente contém erros ortográficos e de gramática.

SICOOB Credcooper

WhatsApp (transferências e empréstimos)

Como acontece?

Os criminosos conseguem informações pessoais das vítimas por meio de redes sociais ou outras fontes e, em seguida, entram em contato pelo WhatsApp, fingindo ser um familiar ou amigo em situação de emergência. Eles inventam histórias convincentes, como acidentes, problemas de saúde ou dificuldades financeiras, e pedem dinheiro emprestado de forma rápida e urgente. Normalmente, os contatos utilizam foto de conhecidos, mas com número diferente.

O que fazer?

Verifique sempre a identidade da pessoa que está solicitando dinheiro, especialmente se o pedido for inesperado ou parecer suspeito. Confirme a história com a pessoa em questão ou mesmo com outros familiares antes de realizar qualquer transação financeira. Além disso, nunca compartilhe informações pessoais ou bancárias por meio de aplicativos de mensagens, mesmo que o pedido pareça legítimo.

- Ajuste a privacidade da sua foto de perfil no WhatsApp, para que seja vista apenas por seus contatos salvos.
- Habilite a "Confirmação em duas etapas" no WhatsApp.

Venda Falsa

Como acontece?

As vendas falsas podem acontecer de diversas formas: sites fraudulentos, falso leilão, anúncios falsos em perfis nas redes sociais, dentro de plataformas de venda, como Mercado Livre, OLX, entre outros.

O que fazer?

O Sicoob nunca envia ninguém para recolher cartões bloqueados e dados bancários, por isso desconfie de qualquer contato inesperado que solicite informações pessoais ou financeiras, especialmente se envolver a entrega ou retirada de cartões bancários. Em caso de dúvidas, entre em contato pelos canais oficiais de atendimento.

- Desconfie de ofertas muito atrativas, que oferecem uma vantagem financeira muito grande
- Observe se o endereço eletrônico possui o "https", o cadeado na barra de navegação e a inscrição de "site seguro".
- Pesquise a reputação do vendedor.
- Não aceite intermediação durante uma negociação.
- Atente-se ao favorecido quando for realizar transferências.

Falso boleto

Como acontece?

Os criminosos geralmente enviam aos destinatários boletos falsificados, que se parecem com os boletos legítimos de empresas ou instituições financeiras. Esses boletos podem ser enviados por e-mail, mensagem de texto ou até mesmo entregues em mãos.

O que fazer?

Para confirmar se um boleto é verdadeiro, faça três verificações: confira se os três primeiros números da linha digitável correspondem ao nome do banco emissor; se os dados do beneficiário são da pessoa ou instituição que você precisa pagar; e se o nome do pagador é o mesmo apresentado no boleto. Fique especialmente atento aos boletos recebidos de forma não usual e com muitos descontos.

Renegociação de dívidas

Como acontece?

Os golpistas entram em contato com vítimas em débito e oferecem opções de renegociação da dívida, com condições especiais e descontos atrativos. Na tentativa de resolver sua situação financeira, as pessoas são persuadidas a fornecer informações pessoais e financeiras, como números de CPF, senhas de acesso a contas bancárias ou dados de cartões de crédito.

O que fazer?

Não forneça informações pessoais ou financeiras por telefone, e-mail ou mensagem de texto, especialmente se você não iniciou o contato. Em caso de dúvida, entre em contato diretamente com o Sicoob pelos canais oficiais de atendimento

Roubo de celular

Teve o celular roubado ou furtado? Confira algumas ações que vão proteger os seus dados e a sua privacidade:

- Informe as autoridades: registre um boletim de ocorrência na delegacia mais próxima em caso de roubo do celular. Isso pode ajudar nas investigações e na recuperação do dispositivo.

- Bloqueie o acesso ao celular: se o seu celular tiver a função de bloqueio remoto, como o "Encontre Meu Dispositivo" para dispositivos Android ou o "Buscar iPhone" para dispositivos iOS, use-a para impedir o acesso ao seu celular imediatamente. Outra opção é o aplicativo do governo "Celular Seguro", que possibilita que vítimas de furto e roubo bloqueiem o aparelho e seus aplicativos em poucos cliques.

- Entre em contato com a operadora: entre em contato com sua operadora de telefonia móvel para bloquear o chip (SIM card) do celular perdido ou roubado. Isso ajudará a evitar que os criminosos façam uso indevido do seu número de telefone.

- Mude as senhas: altere imediatamente as senhas de acesso a aplicativos bancários e outras contas financeiras associadas ao seu celular perdido ou roubado.

- Notifique o banco ou instituição financeira: entre em contato com o seu banco ou instituição financeira para informar sobre a perda ou roubo do celular. Eles podem fornecer orientações específicas sobre como proteger suas informações bancárias e monitorar qualquer atividade suspeita em sua conta.

- Monitore suas contas bancárias: fique atento a qualquer atividade suspeita em suas contas bancárias e histórico de transações. Relate imediatamente ao banco qualquer atividade não autorizada.

O Sicoob tem a sua segurança como prioridade, por isso está sempre buscando novas ferramentas e tecnologias para te oferecer o melhor quando o assunto é proteção e conscientização:

Proteção no ambiente cibernético

O Sicoob implementa proteções cibernéticas em três seções principais: a primeira inclui recursos tecnológicos robustos, como firewalls de última geração, detecção de intrusão, segmentação de redes e monitoração ostensiva. A segunda seção possui controles de segurança avançados, como biometria facial, senha de acesso e segundo fator de autenticação. A terceira seção utiliza inteligência artificial para validar transações, podendo negar operações suspeitas ou exigir nova validação biométrica. Além disso, o Sicoob possui um Centro de Operações de Cibersegurança (SOC) com uma equipe dedicada a monitorar 24 horas por dia e 7 dias por semana tentativas de ataques, fraudes e atividades maliciosas.

Reconhecimento facial e inteligência artificial

O Sicoob implementa a inteligência artificial (IA) no ambiente cibernético através da aplicação *User Behaviour Analytics (UBA)*, que utiliza machine learning e regras pré-definidas para detectar potenciais ameaças relacionadas às contas dos usuários. A IA analisa os hábitos do usuário, incluindo o tipo de dispositivo, rotinas e origem da conexão, atribuindo pontuações com base em seu comportamento. Desde abril de 2020, o reconhecimento facial é utilizado para liberar novos dispositivos remotamente, sem necessidade de comparecimento aos pontos de atendimento. Em transações fora do padrão, os cooperados são submetidos a uma validação avançada da biometria facial. Além disso, os cooperados têm a capacidade de definir limites diferenciados para transações com pessoas desconhecidas ou habituais, ajustando esses limites conforme o horário do dia.

Investimentos e campanhas de conscientização

O Sicoob tem se dedicado continuamente a investir em tecnologia para desenvolver mecanismos que evitem ações de golpistas, ao mesmo tempo em que prioriza a comunicação para educar seus cooperados. Recentemente, lançou a Cartilha de Segurança da Informação, disponível em www.sicoob.com.br/seguranca, oferecendo dicas valiosas de segurança. Além disso, o Sicoob participa ativamente das campanhas nacionais promovidas pela Febraban, contribuindo para conscientizar a população sobre questões de segurança. No aplicativo, os cooperados têm a opção de contratar seguros que cobrem situações em que transações são realizadas por celular sob coação, assim como oferecem ressarcimento de perdas materiais decorrentes de roubos ou furtos qualificados de dispositivos celulares, bolsas, mochilas e seus pertences.

ATENÇÃO

CAIU NO GOLPE?

Faça a contestação do Pix através da funcionalidade "Contestar Pix" no Super App Sicoob ou entre em contato com a Central de Atendimento do Sicoob, na área de prevenção a fraudes, pelo telefone **0800 724 4420**, disponível 24 horas por dia em todos os dias da semana e nos feriados.

Faça um Boletim de Ocorrência: forneça o máximo de detalhes possível sobre o golpe.

Entre em contato com a sua agência para informar o acontecido. Será necessário apresentar o Boletim de Ocorrência.

Redefina suas senhas de contas bancárias, cartões, redes sociais e e-mail, para tentar limitar outros acessos não autorizados.

Se seu celular ou computador foi afetado de alguma forma, é indicado formatar sua máquina.

SICOOB Credcooper

Dicas para fazer compras online com segurança

- Pesquise preços antes de comprar e desconfie de valores muito abaixo da média de mercado.
- Cheque o endereço do site, que deve começar com https:// e ter o cadeado na barra do navegador.
- Evite links recebidos por e-mail, SMS ou redes sociais.
- Confira o histórico de reclamações da loja no Procon e no Reclame Aqui.
- Desconfie de propagandas que usam gatilhos de emergência como "compre antes que acabe", "é só hoje", ou que tenham o timer de contagem regressiva.
- Evite sites que só aceitam pagamento via boleto ou Pix.
- O jeito mais seguro para realizar pagamentos online é criar um cartão virtual de compra única, onde o limite dele será o valor da compra, reduzindo a chance de clonagem e utilização indevida.
- Evite redes Wi-Fi públicas. Prefira conexão segura e privada.

Reforçando:

O Sicoob NÃO solicita dados pessoais, dados bancários e NÃO pede que você faça transações financeiras através de ligações telefônicas e mensagens.
- Nós também NÃO solicitamos que você faça a troca de senha do seu app, reconhecimento facial e atualize o aplicativo, através de contato por telefone.
- Se você receber ligação ou mensagem solicitando essas informações ou ações, desconfie e não corresponda.

Em caso de dúvida, procure sua agência.

sicoob | sicooboficial | @sicoob | sicooboficial | sicoob | sicoob | sicoob

Para mais dicas e orientações, acesse
www.sicoob.com.br/seguranca.

SICOOB Credcooper