SICOOB Credimil

CARTILHA

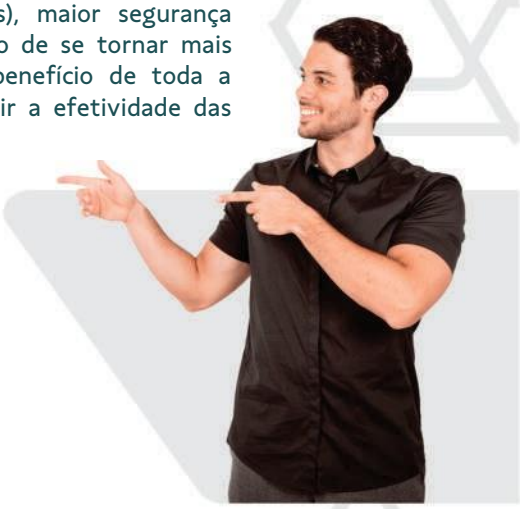
COMO EVITAR GOLPES E FRAUDES FINANCEIRAS

Sumário

1 – Apresentação

Esta **Cartilha de Prevenção a Golpes e Fraudes Financeiras** (1ª Edição) foi desenvolvida pelo Sicoob Credimil com o intuito de ampliar a conscientização de seus associados e clientes quanto às principais formas de fraudes e/ou golpes usualmente praticados.

Pautada em seu compromisso com **o desenvolvimento de ações em benefício social**, o Sicoob Credimil visa proporcionar ao leitor (e, indiretamente, a sua rede de contatos), maior segurança financeira em suas transações, prevenindo-o de se tornar mais uma vítima e ainda contribuindo para o benefício de toda a sociedade à medida em que ajuda a diminuir a efetividade das ações criminosas.



De modo geral, o que se percebe é que com o crescimento e a agilidade no uso das soluções digitais, criminosos identificaram "oportunidades" para aplicação de golpes, com as mais variadas técnicas, observando forte destaque para a manipulação psicológica da vítima (modelo conhecido como Engenharia Social).

Os modelos de golpes apresentados nas páginas a seguir, **infelizmente, não são exaustivos,** haja vista que novas modalidades de golpes estão sendo utilizadas a cada dia. Entretanto, com a leitura atenta, criar-se-á uma boa base de conhecimento que instigará no leitor, um **sentimento de desconfiança** para aquelas situações que fugirem o mínimo da normalidade.

Em qualquer situação, a **informação é a melhor ferramenta preventiva!** Então, seja também, um multiplicador! Repasse essas informações ao maior número de pessoas possíveis.

A todos uma excelente e proveitosa leitura!

2 – Comece protegendo seus Dados Pessoais

Sabemos que os criminosos estão à espreita, criando meios e esperando qualquer brecha para entrarem em ação. Por isso, antes de mais nada, devemos fazer a nossa parte, cuidando de um bem muito precioso: nossos Dados Pessoais!

Os dados pessoais são a sua representação na sociedade, por isso, são parte da sua personalidade. Eles devem ser usados de forma leal e segura, conforme as legítimas expectativas.

O excesso de exposição pode comprometer sua privacidade e dar aos golpistas a oportunidade de usar seus dados para tentar se passar por você, inclusive. Já pensou nisso?

Por isso, adote uma **postura preventiva,** diminuindo sua exposição e usando medidas de segurança. Confira a seguir alguns cuidados importantes para garantir proteção dos seus dados e acessos.

2.1 – De olho em suas Redes Sociais

Com o número cada vez mais crescente de usuários de redes sociais, os criminosos virtuais enxergam nessas plataformas uma grande chance de aplicar diferentes golpes. **FIQUE ATENTO!**

a. Evite exposição desnecessária na internet. Muitas vezes, a vítima é escolhida a partir da coleta de informações que ela mesmo publica em suas redes sociais;

b. Configure sua conta como privada, quando possível. Aceitar qualquer contato facilita a ação de pessoas mal-intencionadas;

c. Ajuste o público-alvo das informações que compartilha;

d. Cuidado com o fundo das fotos. Procure não fazer postagens que exibem a frente da sua casa, a placa de seu veículo, as informações anotadas naquele quadro atrás de você no trabalho, ou a imagem do seu filho com o uniforme da escola, por exemplo;

e. Ative alertas e notificações de tentativas de acesso em suas contas;

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

g. Alguns aplicativos criados para redes sociais (como jogos, testes de personalidade e edição de imagens) podem ser usados como armadilhas para extrair informações pessoais. Leia os termos de uso e privacidade, pesquise sempre a procedência e o que dizem sobre o aplicativo antes de autorizá-lo no seu perfil;

h. 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.

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

2.2 – Cuide de suas senhas e acessos

a. Utilize sempre senhas fortes: combine aleatoriamente letras maiúsculas e minúsculas, números e caracteres especiais (*, #, @, !, >, <, por exemplo);

b. Jamais use como senha informações como datas de aniversário própria ou de familiares, números de telefone ou qualquer outra facilmente identificável a partir de seus dados pessoais;

c. Troque suas senhas com frequência;

d. Utilize diferentes senhas em diferentes serviços ou aplicativos, principalmente os financeiros;

e. Nunca use a opção “salvar senha” ou “lembrar senha” em navegadores, sites e aplicativos instalados no dispositivo;

f. Nunca, em hipótese alguma, compartilhe suas senhas com terceiros;

g. Jamais compartilhe senhas por meio dos aplicativos do celular, pois muitos aparelhos têm recursos que permitem pesquisar tudo o que já foi transmitido, dando o acesso à senha ao criminoso;

h. Jamais salve ou anote suas senhas ou outras informações sensíveis no próprio celular (bloco de notas, por exemplo). Deixar uma senha salva elimina toda a segurança proporcionada por um sistema protegido;

i. Não use perfis das redes sociais para fazer login em outros sites ou aplicativos;

j. Faça uso do "duplo fator de autenticação" nas plataformas que você utiliza;

k. Troque imediatamente suas senhas se desconfiar que vazaram ou foram usadas em um dispositivo infectado;

l. Habilite notificações de login, sempre que possível.

2.3 - Mais cuidado com o mundo virtual

a. Utilize sempre conexões seguras, evitando redes públicas de Wi-Fi, principalmente, para realizar transações financeiras;

b. Deixe sua conexão Wi-Fi mais segura com pequenas atitudes: não deixe o nome de fábrica, troque-o; desative a conexão automática, porque assim você não corre o risco de ser conectado automaticamente a redes abertas desconhecidas e potencialmente perigosas.

c. Proteja sua máquina ou celular de ataques virtuais. Instale um bom programa de antivírus, mantenha-o sempre atualizado e, pelo menos uma vez por semana, faça uma verificação completa em seus dispositivos;

d. Nunca acesse sites e links desconhecidos, principalmente, aqueles cuja legitimidade não possa ser verificada;

e. Verifique se o endereço que está aparecendo em seu navegador é realmente o que você deseja acessar (confira as letras e caracteres do endereço, um mínimo detalhe faz diferença);

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

g. **Desconfie** de e-mails que solicitam o cadastramento ou atualização de suas informações. Nesses casos, contate a empresa solicitante através de seus canais oficiais para confirmação.

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

i. **Desconfie** de situações e solicitações anormais, sempre buscando meios seguros de confirmar a identificação da pessoa que estiver do outro lado da linha.

2.4 – Realize suas compras com segurança

a. Pesquise 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);

b. Faça compras em computadores seguros. Nunca use um computador público ou de um estranho para efetuar operações que exigem o fornecimento de dados bancários ou senhas;

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

d. 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;

e. Ao realizar compras pela internet, procure por sites reconhecidamente seguros (ao digitar seus dados, observe se a URL (endereço do site) começa com https:// (observe a letra "s" no endereço) e se aparece um cadeado fechado ao lado, identificando que o ambiente é seguro;

f. Nas compras e pagamentos, se for utilizar seu cartão de crédito ou seus dados bancários, verifique se a página acessada utiliza tecnologia de criptografia;

g. Ofertas e promoções imperdíveis são golpes comuns na internet. Para não correr riscos, descarte as mensagens imediatamente;

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

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

j. Opte por utilizar o cartão virtual para compras online. A utilização do cartão de forma online (e não na loja física) é menos segura e envolve maior exposição dos dados. Por isso, sempre que realizar uma compra na internet, proteja o seu cartão físico e crie um cartão virtual. Ele pode ser dedicado para as seguintes situações:

- ✔ Compra única: caso precise realizar apenas uma compra naquele site, crie um cartão virtual de compra única. Assim, caso o dado do cartão vaze, não será possível que o fraudador o utilize, pois ele já terá sido cancelado.
- ✔ Compra recorrente: já para sites que oferecem serviço de assinatura ou outras compras que acontecem todo mês, crie um cartão virtual recorrente. Caso o cartão virtual seja fraudado, será necessário apenas abrir um chamado de contestação e cancelamento do cartão virtual, não sendo necessária a reposição do cartão físico.

2.5 – Cuidados no uso do celular

a. Use a biometria facial ou digital para desbloqueio da tela inicial do celular (essas alternativas são mais fortes que as opções de desbloqueio por desenho ou PIN);

b. Ative o bloqueio temporário de tela com senha diferente das demais;

c. Evite salvar seus contatos no aparelho celular com apelidos como: pai, mãe, irmã, tia, tio etc. (isso facilita a ação de pessoas mal-intencionadas);

d. Jamais empreste seu telefone celular para pessoas desconhecidas;

e. Da mesma forma, nunca use celulares de terceiros para acessar as suas contas;

f. Mantenha o sistema operacional do celular atualizado, assim como os aplicativos financeiros;

g. Faça o download de um antivírus adequado para seu dispositivo;

h. Habilite a função de rastreio do celular para conseguir apagar os dados do seu aparelho e localizá-lo remotamente, se necessário;

i. Baixe aplicativos somente nas lojas oficiais;

j. Anote o código IMEI (International Mobile Equipment Identify) assim que comprar um aparelho, pois com ele será mais fácil bloquear seu celular em caso de perda, roubo ou furto. Basta digitar *#06# no celular e o número aparecerá;

k. Mantenha o código IMEI do seu aparelho anotado em casa ou em algum lugar seguro.

l. Não guarde fotos de cartões de crédito;

m. Apague mensagens e fotos com dados sensíveis.

n. Desative a leitura das notificações na tela inicial quando o celular estiver bloqueado.

o. Usar sempre uma configuração de bloqueio da tela de início do celular e optar pela opção de bloqueio automático mais rápida;

p. Evite andar na rua usando o celular e tenha cuidado ao volante sempre que usar aplicativos como Waze ou Google Maps;

q. Quando usar serviços via telefone em ligações, seja discreto. Isso impede que suas informações sejam ouvidas e usadas por pessoas mal-intencionadas.

3 – Golpes mais Comuns

Como absolutamente ninguém está livre de se tornar uma vítima dos fraudadores, a melhor forma de todos se protegerem é através da INFORMAÇÃO!

Por isso, confira abaixo alguns dos tipos de golpes mais comuns e aprenda como não cair em suas armadilhas.

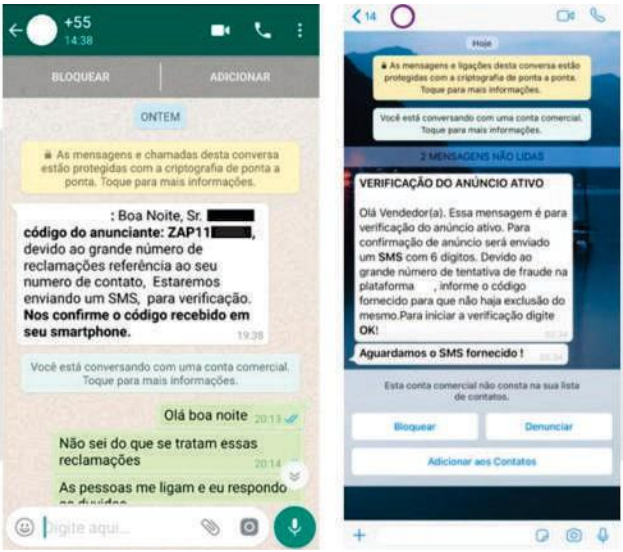
3.1 – Golpe do WhatsApp

Como variações diferentes do Golpe do WhatsApp, podemos encontrar a Clonagem do *WhatsApp* e o Perfil *Fake*. Confira:

COMO FUNCIONA: No **primeiro tipo**, 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 passa a enviar mensagens para os contatos da vítima pedindo dinheiro em nome dela.

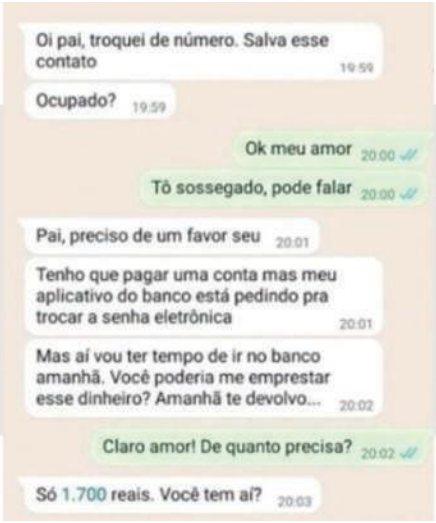
Outra modalidade de clonagem de contas do WhatsApp tem como alvo pessoas que publicam anúncios em sites de vendas e disponibilizam um número de celular. Com a informação, os autores do golpe enviam uma mensagem se passando pela empresa que hospeda o anúncio, alertando a

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 informe, 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.

Um **terceiro tipo** de golpe é por meio da criação de uma conta fake no WhatsApp: os criminosos criam um perfil fake no WhatsApp, com a foto de um usuário, mas com um número de telefone diferente. Nestes casos, o golpista já possui os dados pessoais da vítima (coleta fotos de suas redes sociais, por exemplo), assim como os contatos no aplicativo. Utilizando o perfil fake, o fraudador envia mensagens aos contatos da vítima, dizendo ter trocado de número e alegando alguma emergência. A partir daí, solicita transferência de valores ou pagamento de boletos. Observe o exemplo:



PROTEJA-SE!

1. **Desconfie** de pessoas pedindo dinheiro, pagamento de boletos ou seus dados por aplicativos de mensagem. Geralmente os golpistas apelam para alguma urgência falsa e pedem depósitos e transferências via Pix para contas de terceiros ou então para pagar alguma conta. Por isso, não faça transferências ou pagamentos por solicitação feita apenas por mensagem, principalmente se o destinatário for uma terceira pessoa.

2. **Desconfie** de contatos do WhatsApp que utilizam foto de conhecidos, mas com número diferente.

3. Ao receber mensagens com solicitação de transferência ou empréstimo de algum conhecido e antes de realizar qualquer transação financeira, certifique-se buscando outros meios de entrar em contato com a pessoa que supostamente está fazendo a solicitação (faça uma chamada de vídeo ou ligue por outro canal para confirmar a solicitação ou se é a pessoa, de fato).

4. É fundamental a comunicação imediata da clonagem ou da existência de um perfil falso para o maior número de conhecidos, para que eles não façam transferências ou pagamentos solicitados em seu nome e assim não se tornem outras vítimas.

5. Caso algum contato tenha realizado transferências ou pagamentos solicitados pelos criminosos, oriente-o a registrar um boletim de ocorrência e a comunicar imediatamente a instituição financeira de origem dos recursos para tentativa de recuperação do valor.

6. Não deixe público o seu número de telefone pessoal em redes sociais.

7. Para evitar que sua foto seja utilizada indevidamente, você pode exibí-la apenas para seus contatos de confiança. Com esse cuidado, você diminuirá as chances de os golpistas usarem sua imagem e se passarem por você para enganar seus conhecidos. Para ativar essa opção, acesse: **CONFIGURAÇÕES** ou **AJUSTES do WhatsApp**, em seguida clique em **PRIVACIDADE** e **FOTO DO PERFIL** (desmarque a opção TODOS, caso esteja ativada e selecione a opção que desejar (Meus Contatos, por exemplo).

8. Outra dica para se proteger é ativar a verificação em duas etapas do WhatsApp: Acesse as **CONFIGURAÇÕES** ou **AJUSTES do WhatsApp**, em seguida clique em **CONTA** e **CONFIRMAÇÃO/VERIFICAÇÃO EM DUAS ETAPAS** (siga os comandos e cadastre um PIN de 6 dígitos). Periodicamente o WhatsApp irá solicitá-lo.

3.2 – Golpe da Tarefa ou da Renda Extra

COMO FUNCIONA: Usando aplicativos de mensagens, como o WhatsApp, os golpistas prometem pagamentos por tarefas aparentemente simples, por exemplo, curtir publicações, seguir perfis ou fazer comentários. Em algum momento, os golpistas podem pedir um investimento inicial para "liberar" ou "aumentar" os ganhos, ou solicitam informações pessoais e dados bancários sob o pretexto de pagamento. Mas o valor prometido pelo

bandido nunca é enviado. Ao contrário, a cada pagamento realizado pela vítima, novos depósitos são solicitados.

Observe um exemplo de abordagem suspeita:

PROTEJA-SE!

Sempre **desconfie** de uma proposta de trabalho que seja preciso pagar antes de receber qualquer valor, bem como, de promessas de vantagens exageradas. Se algo parece bom demais para ser verdade, provavelmente é golpe!

3.3 - Golpe do Falso Leilão

COMO FUNCIONA: Golpistas criam sites falsos com o intuito de se passar por um leiloeiro, promovendo supostos leilões de veículos, imóveis, maquinários etc., com preços geralmente abaixo do mercado, atraindo a atenção de pessoas que navegam e buscam um bom negócio. Além da falsa venda e do falso leilão realizados, também roubam 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!

Por se tratar de um leilão, existe a pressão do tempo contra a vítima. A pessoa não pode demorar muito para decidir, ela precisa dar o lance e comprar rápido, antes que outro o faça. Ao dar o lance, a vítima é vencedora

do suposto leilão e precisa realizar o pagamento, no entanto, quando o criminoso identifica que o pagamento foi de fato realizado, bloqueia os contatos e a vítima não consegue mais falar com a suposta "empresa".

PROTEJA-SE!

1. **Desconfie** de preços muito abaixo do praticado no mercado, mesmo que se trate de um leilão.
2. Não realize depósitos para terceiros, sejam eles "representantes comerciais" ou "parceiros do leiloeiro".
3. Sites de leilões brasileiros sempre terminam com: '.com.br", porque precisam estar hospedados no Brasil. Já os leilões falsos, normalmente usam o final ".com" e, para enganar, eles colocam: ".com/br", porque são hospedados no exterior.
4. Nunca faça cadastros em sites de leilões antes de pesquisar sobre sua reputação e idoneidade.
5. Antes de comprar, visite o site da Aleibras – Associação da Leiloaria Oficial do Brasil (www.aleibras.org.br/leilao-seguro) ou visite o site www.leilaoseguro.org.br e analise o leilão que você deseja participar;
6. Confirme no site do Detran se o leilão está sendo processado na plataforma do leiloeiro designado pelo órgão;
7. Confira o CNPJ do leiloeiro;
8. Na dúvida, nunca envie dados bancários ou documentos pessoais;
9. Nunca faça transações em sites que não tenham o cadeado de segurança no navegador.

3.4 – Golpe do Falso Boleto

COMO FUNCIONA: A vítima poderá receber um boleto falso para pagamento por meio de falsa correspondência (bancária, de um vendedor, prestador de serviço ou de uma loja, por exemplo) ou em formato eletrônico (tais como mensagens de SMS, WhatsApp ou e-mail). Quando o cooperado efetua o pagamento de um boleto adulterado, o valor é direcionado para a conta do suposto fraudador ao invés do verdadeiro credor. Como resultado, o credor continua a efetuar as cobranças à vítima ou não envia o produto.

PROTEJA-SE!

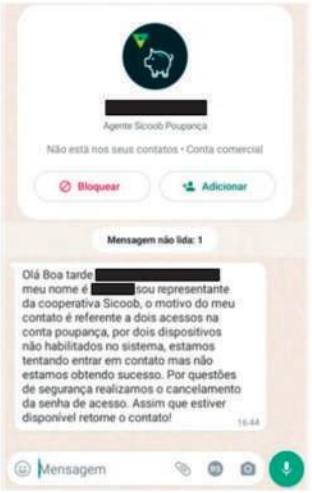
1. Quando receber um boleto para pagamento de forma não usual, ou seja, de forma diferente da que costumeiramente o recebe de seu fornecedor, **desconfie!** Confirme junto ao beneficiário a legitimidade do documento antes de efetuar o pagamento;
2. Nunca emita segunda via de boleto em site que não seja o da instituição financeira emissora do boleto. Você provavelmente emitirá um documento fraudado que não quitará sua dívida com o beneficiário;
3. 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;
4. Confira os dados do beneficiário do boleto antes de concluir o pagamento e só efetive a transação quando tiver certeza de que o dinheiro irá para o destinatário correto;
5. **Desconfie** sempre de descontos concedidos com o envio de uma segunda via de boleto.
6. Entre em acordo com o beneficiário do boleto pelo canal de comunicação pelo qual os boletos são costumeiramente enviados.

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

8. Para maiores esclarecimentos, consulte a **CARTILHA DE PREVENÇÃO A FRAUDES EM BOLETOS** disponível no site do Sicoob (www.sicoob.com.br).

3.5 – Golpe da Falsa Central ou do Falso Funcionário

COMO FUNCIONA: O criminoso entra em contato com a vítima por meio de aplicativos de mensagens ou ligação, passando-se por um funcionário da Cooperativa (ou fingindo ser da Central de Atendimento do Sicoob) no intuito de obter informações confidenciais. Também podem oferecer ajuda no cadastramento de chave PIX ou de quaisquer outros serviços. A partir dessa abordagem, solicitam senhas, atualização de sistemas, liberação de equipamentos ou realização de transferências. Observe um exemplo:



Há casos em que os golpistas simulam o número de telefone por meio de recursos tecnológicos, como gravações e menus para aumentar a sua confiança, dando mais veracidade ao golpe.

PROTEJA-SE!

1. A Cooperativa NUNCA entra em contato solicitando informações pessoais e confidenciais. Tampouco 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 para ninguém.

2. Nessa situação, desligue e entre em contato com a Cooperativa, por outro aparelho, ou em outro horário, através dos canais oficiais. Desta forma, você evita que a golpista "prenda" sua linha telefônica e você volte a falar com o criminoso, acreditando estar falando com a Central de Relacionamento oficial de sua instituição.

3. 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 por meio dos números disponibilizados no site oficial www.sicoob.com.br.

4. JAMAIS forneça seus dados pessoais e bancários, como senhas, códigos e números de cartão por meio de ligação, e-mails, SMS ou aplicativos de mensagens. Caso receba algum contato suspeito em nome do Sicoob, converse com a Cooperativa.

5. 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.

3.6 - Golpe do Falso Empréstimo

COMO FUNCIONA: É a oferta de empréstimos com muitas facilidades, inclusive com a promessa de não consultar órgãos de proteção ao crédito, ou com condições mais vantajosas em relação às praticadas no mercado. No geral, são ofertados por SMS, WhatsApp, contatos telefônicos, anunciados na internet, mídias sociais, em outdoors, rádios, jornais etc.

Após receberem o contato dos interessados em tomar o empréstimo e acertarem as condições contratuais, os golpistas solicitam uma

antecipação de valor, que pode ser um pagamento antecipado de taxas administrativas, seguros prestamistas ou outra desculpa para liberarem o crédito e, quando recebem o pagamento, interrompem o contato com a vítima.

PROTEJA-SE!

1. **Desconfie** das facilidades ofertadas. Quanto mais atraente for a oferta, maiores as chances de golpe. Fique atento!
2. Nunca faça pagamentos antecipados à liberação do empréstimo. Nenhuma instituição financeira pede ou pode receber pagamentos adiantados para liberação de crédito.
3. Não divulgue os detalhes do seu pedido de empréstimo em redes sociais.
4. Se alguém lhe oferecer empréstimo em nome do Sicoob, procure o canal oficial da **Cooperativa**. Somente ela poderá oferecer e realizar o empréstimo.
5. Se pedirem pagamento de taxa, depósito ou transferência como garantia, cancele a negociação.
6. Não passe dados pessoais e documentos para desconhecidos.
7. Sempre confira a origem das mensagens ao receber e-mail marketing ou outros se passando pela instituição financeira. Nunca clique em links super vantajosos.

3.7 – Golpe do 0800

COMO FUNCIONA: Neste golpe, os bandidos enviam uma mensagem por SMS para a vítima, se passando pela Cooperativa e informando sobre uma transação suspeita de transferência ou uma compra no cartão de crédito, pedindo para a pessoa entrar em contato com uma suposta central de atendimento para receber auxílio. A mensagem em questão é enviada por um número 0800, para passar confiança à vítima. No contato, a vítima é

induzida a fornecer dados pessoais e fazer uma transação para "regularizar" a situação ou baixar algum software espião que pode dar aos criminosos acesso completo ao seu celular.

COOPERATIVA: Parabéns! Compra aprovada com sucesso no valor de R$ 3.760,00 12/06/2023. Caso não reconheça contate a Central 0800 ** 2588.

PROTEJA-SE!

Jamais ligue para os números de telefone (0800) recebidos através de SMS ou por outras mensagens. Na dúvida, ligue sempre para a Cooperativa ou para seu gerente. A Cooperativa nunca solicitará dados como senhas e outros dados pessoais via ligação, tampouco irá solicitar transferências, Pix ou qualquer tipo de pagamento, ainda mais para supostamente regularizar problemas na conta. **Desconfie!**

3.8 - Golpe do Acesso Remoto

COMO FUNCIONA: Neste golpe, também conhecido como **Golpe da Mão Fantasma,** o golpista também pode entrar em contato com a vítima se passando por um falso funcionário da Cooperativa. O criminoso usa várias abordagens para enganar a vítima e diz que vai enviar um link para a instalação de um aplicativo para solucionar um suposto problema ou proceder com alguma atualização de segurança. Por SMS, e-mails falsos ou aplicativos de mensagens, induzem o usuário a clicar em links maliciosos enviados, os quais instalam um malware (um software maligno), concedendo ao golpista o acesso remoto ao celular da vítima.

A partir daí, os criminosos conseguem então acessar qualquer coisa no aparelho, como configurações, aplicativos e fazer login na conta do banco, principalmente se a sua senha fica salva em algum bloco de notas, por exemplo. Assim, em tempo real, começam a movimentar o dinheiro com transferências para contas de terceiros, pagam boletos e solicitam empréstimos. O golpe faz com que a vítima sinta que tem uma mão invisível mexendo no seu celular, por isso o nome "mão fantasma".

PROTEJA-SE!

1. Use a autenticação em duas etapas nos principais aplicativos.
2. 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 por que está recebendo.
3. Sempre cheque as informações com seu gerente 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.
4. Só baixe aplicativos em fontes confiáveis. Além dos links maliciosos, os golpistas costumam solicitar que você instale um aplicativo com a desculpa de melhorar a segurança. Na verdade, esse aplicativo funcionará como a porta de entrada para os golpistas.
5. Lembre-se: a Cooperativa nunca liga para o associado solicitando a instalação de nenhum tipo de aplicativo em seus dispositivos (celulares ou computadores) para supostamente regularizar um problema na conta. Tampouco, envia mensagens SMS ou e-mails com essa mesma finalidade.

3.9 - Golpe do IPVA

COMO FUNCIONA: Os fraudadores criam páginas muito bem elaboradas, que imitam a linguagem gráfica (layout) dos sites oficiais. Podem ser ainda oferecidos "cupons de desconto", normalmente através de links maliciosos

enviados por aplicativos de mensagens, e-mails ou redes sociais. Ao clicar nesses links, a vítima é direcionada a um site clonado, idêntico ao da Secretaria de Fazenda. Na página fraudulenta, são solicitados os dados do veículo e, em seguida, gerado um QR Code, para o usuário realizar a transferência. Nesse momento, o valor é enviado diretamente a uma conta bancária controlada pelos golpistas.

PROTEJA-SE!

1. A Secretaria de Fazenda não oferece descontos além do benefício regulamentar para o pagamento do IPVA em cota única, tampouco para regularizar os débitos pendentes. Portanto, se receber alguma oferta de desconto, saiba que é golpe.
2. Se receber alguma mensagem informando sobre pendências no pagamento do IPVA, confira sua situação nos canais dos Órgãos Oficiais.
3. Nunca clique em links recebidos em aplicativos de mensagens, redes sociais ou e-mails. A Secretaria de Fazenda não envia tais mensagens.
4. É importante também verificar os dados bancários do destinatário do pagamento.

4.0 – Na prática

4.1 – Fui abordado(a)

Se você foi abordado por WhatsApp, SMS ou Ligação e conseguiu perceber a tempo de não transferir suas valiosas economias ao criminoso, **denuncie!** Assim, você segue se protegendo e ainda presta seu apoio às outras pessoas. Veja como:

I – Abordagem por SMS ou Ligação:

a. Envie uma mensagem com qualquer texto (ou até mesmo vazia) para o número 7726 (serviço das operadoras de telefonia para bloqueio de telefone por pirataria/fraude)

b. A sua operadora responderá sua mensagem solicitando o envio do número do telefone que você deseja denunciar (DDD + número completo)

c. Informe o número para que o contato seja analisado e, possivelmente, bloqueado.

II – Abordagem por Whatsapp:

a. Abra a conversa com o usuário que você deseja denunciar

b. Toquem em MAIS OPÇÕES ⋮ > Mais > Denunciar
Selecione a caixa exibida para bloquear o usuário e apagar as mensagens da conversa

c. Toque em DENUNCIAR.

4.2 – Caí em um Golpe... E agora?

Todas as informações contidas aqui, se bem observadas e praticadas no dia a dia, reduzirão (E MUITO!) as chances de você se tornar uma vítima dos golpistas e/ou fraudadores.

Mas se ainda assim, você foi vítima de um golpe ou de uma fraude, saiba que sua **ação rápida pode fazer toda a diferença!** Isso porque não são raros os casos em que o criminoso pode enviar dinheiro para outras contas, dificultando a recuperação do valor.

Informações, dúvidas, reclamações e comunicação de ocorrência de fraude

0800 724 4420

Atendimento 24 horas

Por isso, ligue **IMEDIATAMENTE** para o número **0800 724 4420,** para que o Sicoob possa agir e te ajudar a reaver seus recursos.

Logo em seguida, registre um **Boletim de Ocorrência** na delegacia mais próxima ou pela internet e **entre em contato com a Cooperativa** para maiores orientações sobre o restante da documentação que será necessária para o andamento de sua demanda.

Inclusive, se você utilizou o PIX nas transações, o Sicoob acionará a ferramenta MED (Mecanismo Especial de Devolução) do Banco Central, solicitando o bloqueio dos valores que estejam mantidos na conta do suposto golpista. Caso não haja saldo suficiente para a devolução total dos valores, a conta recebedora será monitorada por 90 (noventa) dias da transação original e, surgindo recursos, serão realizadas as devoluções parciais para a vítima, aumentando o sucesso de recuperação dos valores.

Reforçamos: É importante agir com **RAPIDEZ!**

4.3 – Perdi ou Roubaram meu Celular!

Novamente nesta situação, a **Rapidez** pode fazer a diferença! Veja como agir:

1. Avise imediatamente sua cooperativa ou ligue **0800 724 4420** e peça para desabilitar o acesso à sua conta. Somente ela pode impedir que seu dispositivo seja utilizado caso o criminoso descubra suas senhas.
2. Caso possua relacionamento com outras instituições financeiras, avise-as também imediatamente.
3. Avise sua operadora e solicite o bloqueio da linha e do IMEI do aparelho.
4. Caso faça uso de carteira digital (Apple Pay, Samsung Pay ou Google Pay) no seu cartão de crédito, ela também deve ser bloqueada.
5. Envie um comando para apagar os dados do seu aparelho remotamente (recurso disponível para Android e iOS).

6. Faça um Boletim de Ocorrência na delegacia mais próxima ou pela internet.
7. Avise seus familiares e amigos.
8. Você também pode utilizar o aplicativo ***Celular Seguro*** para denunciar a perda, roubo ou furto de seu celular de modo mais ágil. Acesse: https://celularseguro.mj.gov.br/. Mas **confira antes** se todas as instituições financeiras com as quais você mantém relacionamento faz parte da relação das instituições parceiras do programa.

Fique por Dentro:

O Sicoob foi uma das primeiras instituições financeiras do Brasil a integrar-se ao serviço do **Celular Seguro** – aplicativo lançado pelo Governo Federal que permite às pessoas denunciarem a perda, roubo ou furto de seus aparelhos através do portal Gov.br. O aplicativo faz a integração com as instituições participantes, permitindo o compartilhamento de dados com operadoras de telefonia brasileiras para a suspensão do dispositivo e dos serviços financeiros ligados às instituições financeiras integrante. **Mas atenção**: a denúncia no aplicativo NÃO dispensa o registro do Boletim de Ocorrência. Saiba mais em https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/celular-seguro.

5.0 – Você Sabia?

5.1 – Receber PIX por engano e não devolver é crime!

Nesses casos, por não se tratar de uma fraude ou golpe, a Cooperativa não poderá intervir, mesmo sendo o associado emitente ou recebedor do PIX.

No entanto, a não devolução do valor recebido por engano pode levar a um acionamento judicial por apropriação indébita, com pena de detenção e multa, além de gerar a devolução do valor acrescido de perdas e danos, juros e despesas processuais.

Se você recebeu um pix por engano em sua conta na Cooperativa, pelo App Sicoob você consegue proceder a devolução facilmente. Abra seu extrato, localize e clique na transação do PIX recebida por engano e, em seguida, acione DEVOLVER.

Mas, **fique atento**! Só devolva o valor para a conta de quem lhe enviou (conta de origem), **NUNCA** para conta de pessoa diferente do emissor!

5.2 – O Registrato te mostra quais contas estão abertas em seu nome

Se não cair em golpes é o desejo de todos, ter seus dados envolvidos em transações fraudulentas também não é nada agradável e pode lhe dar uma dor de cabeça daquelas.

Lembra que iniciamos essa Cartilha falando sobre a proteção de seus Dados Pessoais? Já pensou ter conta aberta em seu nome em alguma instituição financeira por aí, que você nem sabe que existe, recebendo recursos de atividades criminosas?

Através das informações do **Sistema Registrato** (Banco Central), você consegue, por exemplo, verificar **gratuitamente** se existe conta bancária, dívida ou chave Pix em seu nome que você não contratou. Sempre que possível, verifique suas informações através do serviço.

Se você não reconhecer alguma informação, procure imediatamente a instituição financeira em que a conta foi aberta (ou o serviço contratado) e solicite orientações.

Saiba mais em:
https://www.bcb.gov.br/meubc/registrato

6 – Quando o assunto é Proteção, Informação nunca é demais!

Quanto mais você aprende, mais você se protege e protege seus amigos e familiares!

Você encontrará as principais dicas desta Cartilha (e outras mais) em sicoob.com.br/principais-golpes e sicoob.com.br/web/sicoob/dicas-seguranca. Acesse e conheça!

Além disso, fique ligado nos treinamentos gratuitos que o Sicoob disponibiliza através do Aplicativo Sicoob Moob:

App Sicoob Moob

Acesse o menu de Opções ☰ e, em seguida, selecione **Universidade**.

Além de inúmeros outros treinamentos, dos mais variados temas, você encontrará:

Baixe o aplicativo Sicoob Moob no Google Play ou AppStore e aproveite!!!

Ainda está com dúvidas? Estamos à disposição através de nossos Canais de Atendimento oficiais para auxiliar você!

7 – Reforce seu Conhecimento!

Passe o tempo reforçando seu conhecimento.

7.1 – Passatempo

Cruzadinha

a. **Atualize-se:** a informação é a melhor forma de se prevenir!

b. **Mude** suas **senhas** regularmente. E não se esqueça de usar senhas fortes, ok?

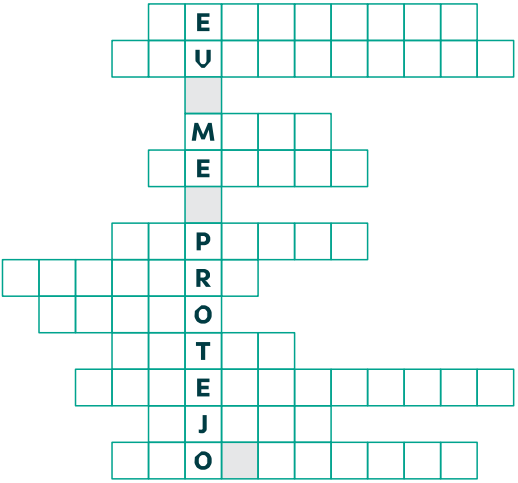
c. **Desconfie** sempre! "Não há almoço grátis"!

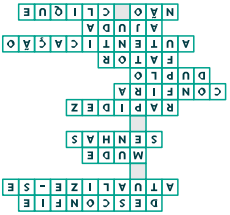
d. **Confira** os endereços de e-mails, a procedência dos sites, das pessoas e empresas que entraram em contato com você e, principalmente, o destinatário dos recursos para o qual você esteja transferindo recursos ou efetuando pagamentos (no caso de boletos, por exemplo).

e. Utilize o **duplo fator** de **autenticação** para acessar suas redes sociais e aplicativos: eles são uma camada extra de segurança.

f. Na dúvida, **não clique** em links desconhecidos, não retorne ligações utilizando o mesmo telefone e, sobretudo, peça **ajuda!**

g. Se você foi vítima de um golpe ou fraude, haja com **rapidez:** ligue para 0800 724 4420 e procure sua Cooperativa.

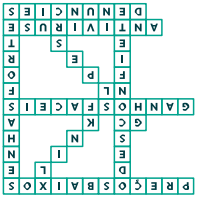




Caça Palavras

ANTIVIRUS / DESCONFIE / GANHOS FACEIS/ LINKS / DENUNCIE / GOLPES
PREÇOS BAIXOS / SENHAS FORTES

P	R	E	Ç	O	S	B	A	I	X	O	S
W	I	R	D	D	M	Y	F	D	L	A	E
D	E	I	N	E	L	S	T	I	I	O	N
Y	D	B	O	S	Y	A	N	S	R	I	H
E	Y	D	G	C	P	K	B	U	A	I	A
G	A	N	H	O	S	F	A	C	E	I	S
T	F	B	E	N	L	A	S	D	V	E	F
L	I	R	E	F	T	P	L	R	T	G	O
E	F	T	I	I	U	A	E	W	P	U	R
T	E	R	A	E	N	I	C	S	E	R	T
E	T	A	N	T	I	V	I	R	U	S	E
S	A	S	D	E	N	U	N	C	I	E	S



8 – Considerações Finais

Caro Leitor,

Se você chegou até aqui, passando por uma leitura atenta do conteúdo desta Cartilha e pela prática das inúmeras formas de prevenção que aqui deixamos registradas, arriscamos a dizer (sem medo de errar!) que você já está mais protegido do que quando iniciou esta jornada. Parabéns!!!

Pautado em seus Princípios Cooperativistas, o Sicoob Credimil se alegra em poder demonstrar mais uma vez seu interesse pela comunidade ao ampliar a disseminação de informações tão relevantes para a segurança financeira de todos e, em especial, de seus associados e clientes.

Reforçamos, pois, nosso compromisso em prestar serviços financeiros pautados na Ética, Solidariedade e Responsabilidade Social.

Lembrem-se: a **Informação** é a melhor forma de **Prevenção!**

Excelentes e **Seguros** Negócios a todos vocês!

9 – Referências

Principais Golpes – Nacional – Sicoob, disponível em:
https://www.sicoob.com.br/web/sicoob/principais-golpes

Dicas Segurança – Nacional – Sicoob, disponível em:
https://www.sicoob.com.br/web/sicoob/dicas-seguranca

Febraban – Segurança Digital, disponível em:
https://antifraudes.febraban.org.br/

FAQs (bcb.gov.br), disponível em:
https://www.bcb.gov.br/meubc/faqs/p/o-que-e-e-como-funciona-o-mecanismo-especial-de-devolucao-med

Registrato (bcb.gov.br), disponível em:
https://www.bcb.gov.br/meubc/registrato

Publicações da ANPD — Autoridade Nacional de Proteção de Dados (www.gov.br), disponível em:
https://www.gov.br/anpd/pt-br/documentos-e-publicacoes

Fascículos – Cartilha de Segurança para Internet (cert.br), disponível em:
https://cartilha.cert.br/fasciculos/

Você já protege seus dados? — LGPD – Lei Geral de Proteção de Dados Pessoais | Serpro, disponível em:
https://www.serpro.gov.br/lgpd/cidadao/voce-ja-protege-seus-dados-pessoais

Celular Seguro — Ministério da Justiça e Segurança Pública (www.gov.br), disponível em:
https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/celular-seguro

O que é Celular Seguro e como cadastrar seu aparelho [agora mesmo] – Meu Bolso em Dia, disponível em:
https://meubolsoemdia.com.br/Materias/celular-seguro

Termo de Recebimento

Declaro que recebi a primeira edição da **Cartilha de Prevenção a Golpes e Fraudes Financeiras** na data abaixo especificada, conforme:

Data:

Nome:

Agência: **Número da Conta:**

( ) Ciente

Assinatura


SICOOB
Credimil