

# Segurança – Alerta a Fraudes

Quando se trata de segurança, precisamos estar sempre atentos a vários fatores, pois as ameaças de ações ilícitas podem estar em qualquer lugar.

No intuito de evitar às ações de fraudadores, os cooperados devem atentar-se aos procedimentos listados abaixo, no que se refere a:

- I. Atendimento na Cooperativa;
- II. Terminal de auto-atendimento (ATM);
- III. Internet;
- IV. Uso de cheques;
- V. Cartão magnético;
- VI. Pagamento de boletos;
- VII. Cuidados com uso de senhas; e
- VIII. Prevenção à lavagem de dinheiro.

## I. Atendimento na Cooperativa

Para garantirmos a segurança dos nossos associados disponibilizamos uma moderna estrutura.

- Porta giratória com detectores de metais que impede a entrada de pessoas armadas;
- Circuito interno de televisão que permita a observação e gravação eletrônica das imagens dos ambientes internos da cooperativa;
- Fechadura de retardo de tempo: impede a abertura imediata de cofres ou caixas-fortes que ocorre apenas nos horários programados, protegendo os valores guardados em seu interior;
- Alarme contra roubo e intrusão: aciona imediatamente a polícia ou a empresa de monitoramento em caso de ocorrência de roubo ou furto durante e fora do horário normal de expediente;
- Vigilância ostensiva nas entradas e em pontos estratégicos de observação durante o horário de expediente.

## 2 - Cuidados quando estiver na cooperativa:

- Evite conversar com estranhos, afinal, não é possível saber se o seu interlocutor é uma pessoa honesta ou não;
- Estando na fila, cuidado com as cortesias;
- Proteja bem seu dinheiro ou os cheques ao ir à cooperativa;
- Não se preste a receber créditos de pessoas desconhecidas em sua conta. Propostas desse tipo são geralmente feitas por golpistas;
- Desconfie de vantagens financeiras ou dramas familiares que lhe sejam apresentados por desconhecidos;
- Ao fazer pagamentos, confira se todos os canchotos foram autenticados pelo caixa;
- Ao retirar seu extrato, verifique os lançamentos e, em caso de dúvidas, procure imediatamente o seu gerente;
- Guarde seu extrato em lugar seguro ou rasgue e jogue-o em uma lixeira, se possível, fora da cooperativa.

3 - Cuidados nas grandes retiradas de dinheiro e após realizar operações na cooperativa:

Os fraudadores observam os associados na cooperativa ou no PAC, para identificar aqueles que efetuam grandes retiradas de dinheiro nos guichês ou ATM's.

Você pode ser seguido e abordado por criminosos ao sair da cooperativa que exigirão a entrega do dinheiro retirado.

Orientações:

- Retire valores em dinheiro apenas quando for extremamente necessário;
- Evite pagar suas contas com dinheiro em espécie. Procure efetuar os pagamentos pela internet, débito em conta ou nos ATM's;
- Se tiver dúvidas quanto à melhor maneira de realizar saques elevados, consulte seu gerente;
- Não saia da cooperativa com pacote nas mãos, pois chama a atenção dos criminosos;
- Evite contar dinheiro em público.

## II. Terminal de auto-atendimento (ATM)

Na hora de utilizar os terminais de auto-atendimento, se você tomar alguns cuidados, pode favorecer ainda mais a sua segurança pessoal e possibilitar operações tranquilas:

- Fique atento a pessoas suspeitas perto do terminal;
- Mantenha o corpo próximo à máquina para impedir que outras pessoas vejam o que você digita ou as informações na tela;
- Não solicite ou aceite ajuda de estranhos. Caso precise procure um funcionário da cooperativa;
- Procure utilizar caixas automáticos instalados em locais de grande movimentação e, se possível, em ambientes internos, como shopping centers;
- Realize saques em horário comercial quando o movimento de pessoas é maior. Evite os horários noturnos caso seja necessário, procure ir acompanhado até o terminal;
- Não anote suas senhas, memorize-as;
- Se após digitar a senha o sistema demorar a concluir a operação, não saia de perto do terminal até que a situação se regularize. Caso persista o problema, tecla "anula" ou "cancela";
- Após o uso certifique que a operação foi finalizada.

## III. Internet

1 - Cuidado com os vírus de computador:

- Eles são instalados e funcionam sem que o usuário perceba;
- Estão por todos os lados na Internet;
- Podem roubar senhas e apagar informações preciosas de seu computador;
  - Ao perceber que foi infectado por um vírus, desligue seu computador e acione a equipe de informática da sua empresa ou procure ajuda de um profissional da sua confiança;
- Vírus e outros *malwares* se disseminam de diversas formas, tais como:
  - Acessando sites suspeitos;
  - Embutidos em arquivos ou programas baixados pela Internet, anexados a e-mails ou recebidos por meio de sites de relacionamento e redes sociais;

- Utilizando dispositivos infectados: disquetes, CD, pen-drives ou cartões de memória.

## 2 - Dicas para manter seu computador seguro

- Instale um bom programa de antivírus e, pelo menos uma vez por semana, faça uma verificação completa do computador;
- Use sempre cópia original do programa de antivírus, pois as cópias “piratas” geralmente já estão infectadas e não funcionam corretamente;
- Configure seu antivírus para procurar por atualizações diariamente;
- Use seu antivírus para verificar todo arquivo baixado antes de abri-lo ou executá-lo pela primeira vez;
- Cópias originais do Windows são mais seguras e são atualizadas periodicamente pela Microsoft;
- Mantenha o sistema operacional do seu computador e seus programas sempre atualizados para protegê-los contra as falhas de segurança, que são descobertas todos os dias;
- Somente instale programas de fontes confiáveis. Evite os serviços de compartilhamento (por exemplo: Kazaa, Bittorrent, Limeware, Emule, etc.). Eles são uma das principais fontes de disseminação de programas nocivos;
- Não abra e-mails e arquivos enviados por desconhecidos;
- Não abra programas ou fotos que dizem oferecer prêmios;
- Cuidado com os e-mails falsos de bancos, lojas e cartões de crédito;
- Jamais abra arquivos que terminem com PIF, SCR, BAT, VBS e, principalmente, os terminados com EXE e COM;
- Se você desconfiar de um e-mail recebido, mesmo quando enviado por pessoa conhecida, cuidado, pois pode ser um e-mail falso: não abra. Apague-o e não utilize o contato.

## 3 - Fique atento aos endereços acessados no seu navegador

- Verifique se o endereço que está aparecendo em seu navegador é realmente o que você queria acessar;
- Não confie em tudo o que vê ou lê;
- O navegador não garante sozinho a segurança de informações pessoais, senhas e dados bancários;
- Não autorize instalação de software de desconhecidos ou de sites estranhos;
- Antes de clicar em um link, veja na barra de status do navegador se o endereço de destino do link está de acordo com a descrição do mesmo;
- Sempre desconfie de ofertas e sorteios dos quais não tenha prévio conhecimento.

## 4 - Compras e Pagamentos

- Ao realizar compras pela Internet procure por sites reconhecidamente seguros;
- Se for utilizar o seu cartão de crédito ou tiver que fornecer dados da instituição financeira, verifique se a página acessada utiliza tecnologia de criptografia:
  - O endereço da página acessada deve começar com “https”;
  - Verifique se aparece o ícone do cadeado na barra de status (parte inferior) ou à direita da caixa do endereço, dependendo do navegador;
- Confie em seus instintos. Se você desconfiar de um site de compra, deixe-o de lado e compre em outro lugar.

## 5 - Nunca abra e-mails ou execute arquivos enviados por desconhecidos

- Pode haver muitas informações falsas e golpes nas mensagens;
- E-mail é o método mais utilizado para a disseminação de vírus;
- Não clique em links recebidos por e-mail e, caso seja necessário clicar, fique atento para ver aonde ele irá levar;
- Atenção com cartões virtuais. Não abra quando o nome do arquivo tiver a extensão “exe” no final, pois podem ser programas de invasão;
- Não acredite em todos os e-mails sobre vírus, principalmente aqueles de origem duvidosa que trazem anexo arquivo para ser executado, prometendo solucionar o problema;
- Jamais acredite em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado pessoal por e-mail. Comunique-se por telefone com a instituição que supostamente enviou o e-mail e confira o assunto.

## 6 - Cooperativas não enviam e-mails não solicitados a seus cooperados

- Fraudadores geralmente enviam e-mails falsos solicitando que você informe seus dados ou senhas de acesso as contas;
- Muitas vezes falsos e-mails levam você a clicar em links que podem causar situações perigosas, como:
  - Levá-lo a um site falso de sua Cooperativa para capturar o número da sua conta e senha;
  - Instalar um programa malicioso em sua máquina para roubar suas informações, monitorar suas atividades ou mesmo obter o controle de seu computador.

## 7 - Fique atento ao utilizar programas como MSN, Google Talk, Skype, etc

- Esses programas estão sempre conectados a um servidor central e podem ser atacados por pessoas mal-intencionadas;
- Nunca aceite arquivos de pessoas desconhecidas, principalmente se tiverem a extensão “exe” e “doc”, pois podem conter vírus ou outro *malware*;
- Caso haja necessidade de aceitar algum tipo de arquivo, tenha um antivírus atualizado instalado em sua máquina e tenha certeza da pessoa que está enviando.

## 8 - Utilização de Internet Banking

- Procure pelos sinais de segurança:
  - Assegure-se de que o site em que você realizará suas operações bancárias utiliza tecnologia segura. O endereço do navegador deve começar com “https”, onde o “s” significa “seguro”;
  - É importante localizar o ícone do cadeado que, dependendo do navegador, estará localizado à direita da caixa da URL, como no Internet Explorer:



Ou na barra de status (parte inferior), como no Firefox:



- Normalmente a página utiliza a tecnologia segura somente quando você for realizar transações confidenciais, ou seja, a partir da tela em que você informa o número da conta e a senha;
- Navegue diretamente na URL de sua cooperativa
- Evite acessar sua cooperativa clicando em links de outros sites. NUNCA acesse clicando em um link recebido por e-mail. Geralmente trata-se de um site fraudulento destinado a obter sua conta e senha;
- A forma mais segura de visitar o site de sua cooperativa é escrever sempre o endereço diretamente no seu navegador, por exemplo: <http://www.sicoobnet.com.br>.
  
- Não realize operações financeiras em lugares públicos
- Computadores públicos (como os de lan-houses e bibliotecas) muitas vezes contêm códigos maliciosos, instalados por pessoas mal-intencionadas, capazes, por exemplo, de registrar tudo o que você digitar no teclado, facilitando a quebra de sigilo dos seus dados confidenciais.
  
- Mantenha a salvo sua identidade eletrônica
- É importante ter o cuidado especial de não divulgar sua identidade (senhas e códigos de acesso) eletrônica a ninguém, pois uma pessoa mal-intencionada que disponha de sua identidade eletrônica poderá entrar em suas contas, ver seus saldos, solicitar transferências, comprar produtos, enfim, fazer tudo o que você mesmo faria sem que a instituição financeira tenha como saber que não é você que está fazendo tudo isso.
  
- Troque suas senhas com certa frequência
- É uma boa prática trocar sua senha periodicamente para reduzir a possibilidade de que alguém venha a sabê-la e possa usá-la no futuro.
  
- Cadastramento de computadores
- O SicoobNet dispõe de uma ferramenta de segurança que cadastra e identifica o computador do usuário, aumentando a segurança das transações realizadas pela Internet. Essa identificação permite evitar que sua conta seja movimentada a partir de computadores de terceiros;
- Somente operações de consulta podem ser realizadas a partir de computadores não cadastrados para sua conta.
  
- Relate qualquer irregularidade a sua cooperativa
- Verifique sempre seus saldos e extratos bancários para certificar-se de que não contenham transações suspeitas ou desconhecidas, caso em que você deve contatar sua cooperativa e solicitar esclarecimentos;
- Para contatos com a cooperativa utilize os números de telefone encontrados no cartão, nas correspondências da instituição financeira, no talão de cheque ou nas páginas amarelas. Não utilize números de telefones encontrados em sites suspeitos na Internet ou recebidos por e-mail, pois pode ser outra fraude.

#### **IV. Uso dos Cheques**

A cooperativa busca aperfeiçoar a tecnologia de emissão do cheque para torná-lo cada dia mais seguro e confiável. Você associado, com algumas atitudes no uso dos cheques, pode minimizar ou até mesmo impedir a ação de fraudadores.

Como eles agem na falsificação ou adulteração de cheques:

- Fraudadores aproveitam de seu descuido na hora de guardar seu talão de cheques e se apoderam de algumas folhas avulsas ou do talão por completo. Com seu cheque em mãos, a pessoa mal intencionada pode causar muitos prejuízos.
- Após receber um cheque como pagamento de algum produto ou serviço, o fraudador se aproveita do seu descuido no momento do preenchimento do cheque e adultera os valores. Isso pode acontecer adicionando palavras (e números) nos espaços deixados em branco, ou caso você tenha utilizado caneta cedida por terceiro mal intencionado com tinta especial, os valores podem ser apagados e alterados.

1 - Cuidados que você deve ter ao utilizar os cheques:

- Não use caneta emprestada de pessoas desconhecidas para preencher cheques;
- Guarde os talões em local seguro;
- Evite a guarda dos talões de cheques junto a documentos pessoais;
- Ao preencher cheques deixe o menor espaço possível entre as palavras e risque os espaços sem preenchimento;
- Emita sempre cheques nominais e cruzados;
- Ao receber um novo talão, confira os dados impressos e verifique a quantidade de cheques. Se houver alguma divergência, comunique seu gerente;
- Preencha todos os campos e evite rasuras;
- Não empreste seu cheque para outras pessoas;
- Não desconte cheques com estranhos, utilize apenas as instituições financeiras ou os postos autorizados;
- Na perda ou roubo, comunique imediatamente a sua cooperativa e à delegacia de polícia mais próxima;
- Evite circular com talões de cheques. Leve apenas a quantidade de folhas que pretende utilizar no dia;
- Efetue a baixa de cheques inutilizados.

2 - Cuidados que você deve ter ao receber os cheques;

- Confira sempre os dados pessoais do emitente solicitando a apresentação do documento de identificação e o cartão da instituição financeira;
- Verifique se o documento de identificação não apresenta sinais de adulterações (foto, data de nascimento aparentemente divergente da fisionomia do emitente, data de emissão recente etc);
- Anote no verso do cheque o número do RG e telefone do emitente;
- Não aceite cheques rasurados, borrados ou com manchas;
- Desconfie de cheques com aspecto desgastado ou envelhecido;
- Não receba cheques de terceiros;
- Consulte sempre serviços que disponibilizam bases de dados de cheques sustados, cancelados por roubo, etc.

## **V. Cartão Magnético**

O fraudador para agir primeiramente ele tem que obter o cartão magnético da vítima, o verdadeiro ou o clonado, e obter a senha.

## 1 - Como os fraudadores agem para obter o cartão magnético e a senha:

- O fraudador oferece ajuda ao cooperado, e quando o associado entrega o cartão ao falso “atendente”, este troca os cartões sem que o associado perceba. Por isso, nunca aceite ajuda de estranhos;
- O fraudador esbarra no associado enquanto está segurando o cartão, se o cartão cair, ele tenta pegá-lo e devolve ao associado, pedindo desculpas pelo esbarrão. Mas sem que você perceba, troca os cartões e fica com o cartão do associado;
- Para obter a senha o fraudador fica de olho no associado enquanto este utiliza o atendimento automático, sem que você perceba, o fraudador observa as teclas que o usuário digita;
- O fraudador passa por um falso atendente, diz que é funcionário e pede alguns dados do associado, como data de nascimento e senha do cartão, para verificar o funcionamento do atendimento automático. Se o associado der estes dados ao “falso atendente”, este terá as informações necessárias para fraudar o associado. Por isso nunca aceite ajuda de estranhos e lembre-se que os funcionários nunca pedem as senhas do associado e estão devidamente identificados.

## 2 - Como os fraudadores agem de posse do cartão eletrônico e da senha do associado:

- Pode realizar operações no atendimento automático;
- Fazer compras em estabelecimento que aceita o cartão.

## 3 - Cuidados que você deve ter com seu cartão magnético:

- Confira seu saldo e transações listadas no extrato;
- Fique sempre atento a movimentações financeiras e, em caso de suspeita de irregularidade, informe imediatamente o seu gerente e troque todas as suas senhas;
- Após uma compra, é importante que você verifique se o cartão devolvido realmente é o seu e, após devidamente conferidos, os recibos devem ser jogados no lixo;
- Ao utilizar seu cartão em um caixa eletrônico, ou em um estabelecimento comercial, é recomendável agir com discrição. Se for exigida a digitação da senha, procure fazê-lo de forma que outra pessoa não veja o que você está digitando no teclado;
- Ao utilizar seu cartão para compras na Internet, certifique-se de que está na área segura do site (verifique a existência de um pequeno cadeado fechado na tela do programa de navegação e que no início do campo “endereço” surgem as letras “https”);
- Não forneça ou compartilhe com ninguém as suas senhas;
- Em viagem, se não for usar o cartão, deixe-o guardado no cofre do hotel;
- Não anote as suas senhas. Memorize-as.

## **VI. Pagamento de Boletos**

Uma pessoa mal intencionada adultera os documentos relacionados ao pagamento de títulos, boletos ou tributos, ou até mesmo os substituem por outros, desviando o recurso para um terceiro que não é o de origem.

Geralmente este tipo de fraude acontece durante o transporte do documento até o posto de atendimento para pagamentos com cheques ou autorização para débito em conta.

Cuidados com pagamento de boletos:

- Encarregue o transporte dos documentos e valores a uma pessoa de sua inteira confiança;
- Preencha os cheques ou autorizações para débitos em conta corrente com os dados detalhados da operação: natureza, valores e finalidade.

## **VII. Orientações sobre senhas**

A senha é sua assinatura eletrônica, portanto você deve ter o maior cuidado com ela. Uma pessoa mal intencionada de posse da sua senha pode causar uma grande dor de cabeça.

Cuidados que deve ter com sua senha:

- Evite deixar suas senhas anotadas. Elas não devem ser anotadas em locais de fácil acesso, como agendas e carteiras;
- Decore as senhas e depois destrua a anotação;
- Troque suas senhas regularmente;
- Ao criar sua senha, não utilize números que tenham relação com você, como RG, CPF, telefones, datas etc, pois isso pode facilitar a ocorrência de práticas ilícitas;
- Evite números seqüenciais ou repetitivos;
- Nunca digite qualquer senha com pessoas estranhas observando;
- Proteja o teclado com o corpo ao digitar sua senha;
- Não forneça ou compartilhe com ninguém as suas senhas.

## **VIII. Prevenção à Lavagem de Dinheiro**

Os criminosos usam técnicas tão sofisticadas e audaciosas que pessoas inocentes podem se tornar vítimas fáceis do esquema da lavagem de dinheiro.

Cuidados para não cair nesse golpe:

- Não empreste sua conta corrente para receber depósitos e transferir dinheiro para outras contas;
- Não empreste seu cartão para que outras pessoas façam transações em terminais de auto-atendimento, mesmo que sejam somente depósitos para outras contas;
- Não se preste a receber créditos de pessoas desconhecidas em sua conta. Propostas desse tipo são feitas por golpistas, nas proximidades de caixas automáticas e de postos de atendimento;
- Desconfie de vantagens financeiras ou dramas familiares que lhe sejam apresentados por desconhecidos na fila do caixa automático, especialmente propostas de utilização de sua conta para transferência de valores.