CARTILHA DE SEGURANÇA DA INFORMAÇÃO

SICOOB
Credivertentes

INTRODUÇÃO

Quase 4,5 bilhões de transações já são realizadas por canais digitais do Sicoob todos os anos. Isso significa que associados de todo o país fazem 78% de suas movimentações econômicas via aplicativos ou Internet Banking. Um marco para o maior sistema cooperativista financeiro do país.

Afinal, nosso Propósito é justamente "conectar pessoas para promover Justiça Financeira e prosperidade". Algo que requer, além de inclusão com produtos e serviços em portfólio completo, a oferta de ferramentas tecnológicas, modernas e dinâmicas para integrar instituições a seus públicos.

Você já ouviu falar em Engenharia Social?

O termo, em Segurança da Informação, diz respeito a estratégias e manipulações para obter dados importantes de possíveis vítimas em ciberataques. Todo esse contexto pode envolver conversas informais (aproveitando da ingenuidade das pessoas); exploração de confiança e vontade de ajudar; jogos psicológicos sugerindo problemas urgentes a serem resolvidos.

O alerta e o conhecimento de como funcionam esses crimes podem protege-lo. Confira:

· Geralmente, o golpista se faz passar por outra pessoa ou finge ser um profissional de determinada empresa ou área;

· O indivíduo mal intencionado usa o telefone, e-mail, salas de bate-papo, sites de relacionamento e mesmo o contato pessoal para conseguir as informações que procura;

· Desconfie de abordagens de pessoas que ligam e se identificam como técnicos ou funcionários de determinada firma, solicitando dados sobre sua empresa, sobre o ambiente, sobre você, etc.;

· Evite fazer cadastros pela Internet, especialmente fornecendo seus dados pessoais. Se necessário, somente o faça se confiar no site;

· Nunca forneça informações sensíveis, pessoais ou da empresa, por telefone ou outros meios, quando a iniciativa do contato não seja sua;

· Nunca forneça sua senha por telefone, e-mails ou outros meios que não sejam o acesso normal aos aplicativos utilizados, ao site do seu banco ou às máquinas de auto-atendimento;

· O lixo pode ser uma fonte de informações para pessoas malintencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou corporativas antes de descartá-los no lixo;

· Seja cuidadoso com as informações que você disponibiliza em blogs e redes sociais. Elas podem ser usadas por malfeitores para confirmar os seus dados cadastrais, descobrir dicas e responder perguntas de segurança.

NOSSOS SISTEMAS DIGITAIS

Caixas Eletrônicos

Sicoobnet

Cedente

APLICATIVOS NO GOOGLE PLAY OU NA APP STORE

Sicoob

Faça Parte

SicoobCard

Sicoob
MINHAS FINANÇAS

Sipag

Sicoob Mapas

Coopcerto

Sicoob Moob

1. SEGURANÇA

Via Sicoobnet ou qualquer um de nossos aplicativos, você realiza várias operações disponíveis nas agências físicas do Sicoob Credivertentes. E o melhor: sem enfrentar filas ou com restrições* nos horários de atendimento.

Tudo rápido, prático e dinâmico, a poucos cliques. Isso sem falar, claro, em estruturas seguras de Tecnologia de Informação – aperfeiçoadas e fortalecidas por cuidados básicos que os usuários devem ter em seus dispositivos. É sobre eles que falaremos nesta cartilha.

Fique atento(a):

Fraudar dados em um servidor institucional não é fácil. Assim, golpistas usam artimanhas maliciosas para conseguir informações sensíveis das potenciais vítimas ou convencê-las a ações como executar códigos maliciosos e acessar páginas falsas (Phishing). Portanto, cuidado:

1. O Sicoob não solicita informações de identidade digital (login e senha) fora de seus sistemas (no atendimento de agências, nos caixas eletrônicos e Internet Banking) ou aplicativos onde ocorrem transações. Desconfie, portanto, de ligações telefônicas, e-mails, mensagens de Whatsapp ou chats de redes sociais como Facebook e Instagram com essa finalidade.

2. Outros temas comuns na tentativa de enganar usuários são atualização de cadastros e de senhas de cartão; lançamento e atualização de módulos de proteção; comprovante de transferência e depósito; cadastro/recadastro de computadores; suspensão de acessos; sincronização de tokens.

3. Em qualquer contato feito virtualmente envolvendo o nome do Sicoob Credivertentes, certifique-se de conhecer o(a) interlocutor(a). Havendo dúvidas, entre em contato com sua agência de relacionamento. O mesmo vale para supostos representantes de empresas voltadas a manutenção de computadores, celulares ou tablets.

*Vale lembrar que, embora as transações possam ocorrer a qualquer momento via sistemas digitais, elas continuam sujeitas a parâmetros de compensação estabelecidos pelo Banco Central. É o caso de TEDs, por exemplo, que têm compensação no mesmo dia de transferência se ela for feita entre 6h e 17h.

2. PRINCIPAIS GOLPES

Boletos Falsos:

O boleto falso pode ser recebido por e-mail, com falsa oferta de desconto no DDA, entregue fisicamente na residência do cooperado ou ainda ser adulterado durante a emissão na internet (caso, por exemplo, algum vírus esteja instalado no computador ou dispositivo móvel). Ao efetuar o pagamento desse novo boleto, o recurso é desviado e a quitação da obrigação não é realizada. Se o boleto foi recebido fora de sua rotina, confirme sua autenticidade com a empresa emissora ou solicite a segunda via no site oficial da instituição.

Falso Empréstimo:

Oferta de empréstimo com condições facilitadas onde é solicitado pagamento antecipado de taxas administrativas, seguros e outras. Não efetue qualquer pagamento antecipado e desconfie das facilidades. Caso ouça, leia ou veja alguma oferta via meios de comunicação como jornais, revistas, sites, e-mails, rádios ou redes sociais, entre em contato com sua agência de relacionamento para confirmar a veracidade da mesma.

Mensagens Falsas:

Os fraudadores nesse caso conseguem seu endereço de e-mail ou número de telefone e enviam uma mensagem como se fosse o Sicoob, solicitando seus dados pessoais e senhas ou alertando sobre transações indevidas ou bloqueios da conta ou cartão. Ao clicar, você será direcionado a uma página falsa, criada para capturar suas informações ou permitir a instalação de softwares maliciosos (malwares), que podem alterar a configuração de segurança do computador e possibilitar o acesso remoto. Nunca clique no link ou responda a mensagens desse tipo. Em caso de SMS, encaminhe-o para o número 7726, para bloqueio de SPAMS.

Falso Depósito:

O fraudador informa que efetuou depósito indevido e, após enviar o comprovante falso, solicita que o cooperado devolva o valor ou a diferença. Mas quando o envelope depositado é conferido, está vazio. Desconfie de contatos desta natureza e, antes de agir, confirme se os valores estão desbloqueados em sua conta.

Outras formas de golpes são:

- Disponibilizar aplicativos maliciosos que, se instalados, podem coletar seus dados;
- Explorar possíveis vulnerabilidades em seu computador ou dispositivo móvel para instalar códigos maliciosos;
- Explorar possíveis vulnerabilidades em equipamentos de rede, como senhas fracas ou padrão;
- Coletar informações sensíveis que estiverem trafegando na rede sem criptografia (redes não seguras).

Cuidado com documentos:

A maioria das fraudes acontece com o uso de documentos roubados, furtados ou extraviados. Se você foi vítima de uma destas situações, registre um Boletim de Ocorrência (BO).

3. RISCOS

A rede mundial de computadores é uma teia de conteúdos e informações cheia de possibilidades via computadores, smartphones ou tablets. É com esses dispositivos, conectados, que você pede comida em casa, consegue transporte rápido, compartilha fotos, divulga opiniões, lê jornais e livros, assiste aos filmes favoritos e, claro, realiza suas transações financeiras. É importante, no entanto, se proteger contra alguns riscos:

Perdas financeiras:
Sua conta corrente pode ser usada para ações maliciosas e fraudulentas, como transferências indevidas de dinheiro e pagamentos de contas de outras pessoas.

Invasão de privacidade:
Alguém que tenha acesso indevido a sua conta pode obter informações pessoais sobre suas movimentações econômicas e até violar seu Sigilo Bancário (um direito seu, garantido na Constituição).

Ações simples e efetivas:

- Instale programas Antivírus, Antispyware, Antispam, etc. em seu computador e mantenha-os sempre atualizados – bem como o próprio sistema operacional da sua máquina. Em seu celular e tablet, tenha aplicativos (também com atualizações em dia!) de proteção do sistema. Além disso, não ignore os alertas de alguns navegadores quanto a sites suspeitos.
- Troque suas senhas periodicamente utilizando variação de caracteres (letras, números, símbolos). Evite aquelas que remetam a dados pessoais como nomes, sobrenomes, datas ou quaisquer outros que possam ser facilmente coletadas. Atenção: não use a mesma senha do Sicoobnet ou de aplicativos mobile para acessar outros sites.

4. NAVEGAÇÃO E COMPRAS PELA INTERNET

Tenha cuidado com links postados na internet ou enviados a você por mensagens, e-mails e chats. Verifique na barra de status do navegador, antes de clicar, se o destino está de acordo com a descrição do mesmo*. Em caso de redes sociais, opte por acessar aqueles divulgados em nossos perfis oficiais (sicoob.credivertentes, no Facebook; e @sicoob_credivertentes, no Instagram).

Não autorize a instalação de softwares de desconhecidos ou de sites estranhos;

Desconfie de ofertas e sorteios anunciados fora de canais oficiais de qualquer empresa;

Ao realizar compras online, procure por sites reconhecidamente seguros. Uma dica importante: o endereço da página acessada deve começar com "https". Além disso, o ícone de cadeado estará visível na Barra de Status (parte inferior) ou à direita da caixa do endereço, dependendo do navegador;

Antes de utilizar o seu cartão de crédito ou fornecer dados bancários, confirme se a página acessada utiliza tecnologia de criptografia.

*A recomendação é válida, aliás, para os sites da Confederação (www.sicoob.com.br) e do próprio Sicoob Credivertentes (www.credivertentes.com.br).

5. INTERNET BANKING

O Sicoob investiu mais de R$700 milhões em tecnologia entre 2016 e 2019. Tudo para tornar mais prático o cotidiano de seus associados, facilitar transações, dinamizar relações com a economia e ampliar possibilidades de negócios.
Uma das soluções tecnológicas oferecidas pelo sistema nesse sentido é o Sicoobnet, serviço de Internet Banking que, aliás, foi pioneiro no setor cooperativista. Para utilizá-lo com segurança:

1. Acesse o site com o seguinte endereço no seu navegador:

www.sicoob.com.br/sicoobnet

2. Observe que logo depois ele passa a ser precedido por "https", sinal de que realizará suas operações com tecnologia segura. Além disso, haverá o ícone do cadeado na Barra de Status (parte inferior), ou à direita da caixa da URL;

3. Siga sempre essas orientações. Evite acessar o Sicoobnet ou qualquer serviço de Internet Banking via links de outros sites ou com resultados obtidos em pesquisa na web.

4. Também não use dispositivos móveis/computadores de terceiros (como de lan houses e bibliotecas) ou conexões Wi-Fi públicas (em lanchonetes, cafés, etc) para acessar sua conta;

Cadastramento de computadores

O SicoobNet dispõe de uma ferramenta que cadastra e identifica o computador do usuário, aumentando a segurança das transações realizadas pela web. Essa identificação permite evitar que sua conta seja movimentada a partir de equipamentos que não sejam seus. Lembre-se: somente operações de consulta podem ser realizadas a partir de dispositivos não cadastrados.

Efetivação em dois passos

O SicoobNet também dispõe da Efetivação em Dois Passos, que proporciona mais segurança na confirmação e autorização das suas transações financeiras. Em vez da sua senha, você vai digitar um código de seis dígitos, que pode ser gerado por meio de QR Code ou informado pelo Cartão de Segurança. Você escolhe.

Funcionalidades como Bluetooth podem tornar seu aparelho mais vulnerável e suscetível a ataques. Recomenda-se manter tais funcionalidades desabilitadas!

Em qualquer máquina ou dispositivo, use **SEMPRE** a opção "Sair" quando terminar **QUALQUER** operação e deixar de usar seu Sicoobnet.

Verifique periodicamente o extrato da sua conta e as movimentações no seu Sicoobcard. Em caso de dúvidas ou problemas, entre imediatamente em contato com sua agência de relacionamento ou seu gerente.

6. DISPOSITIVOS MÓVEIS

Quantos aplicativos você tem no seu smartphone? Vários, certo? De joguinhos aparentemente corriqueiros a e-mails e apps de redes sociais, diferentes soluções ocupam espaço no seu aparelho – uma mistura de computador pessoal a plataforma de entretenimento –, incluindo os voltados a movimentações financeiras.
Antes de baixá-los e utilizá-los, vale ter atenção a pontos importantes de segurança:

1. Instale aplicativos de fontes confiáveis, como lojas oficiais ou sites de fabricantes dos seus dispositivos. Ao fazer o download, verifique se as permissões solicitadas para a instalação e execução são coerentes com a finalidade do app;

2. Nas configurações do seu aparelho, escolha opções de Bloqueio de Tela com o menor tempo possível. Essa é uma tática importante e simples para proteger suas informações em caso de perda ou roubo;

3. Seja cuidadoso ao permitir que os aplicativos acessem seus dados pessoais;

4. Mantenha o dispositivo atualizado com as versões mais recentes de todos os apps instalados;

5. Cadastre uma senha para o aparelho e configure o bloqueio na tela inicial, para que seja ativado quando o smartphone ou tablet não estão em uso;

6. Ao se desfazer de um dispositivo móvel, apague os dados e restaure as configurações de fábrica.

PROTOCOLO DE ENTREGA

Declaro que recebi para fins de informação e consulta a "Cartilha de Segurança da Informação - 3ª edição", elaborada pelo SICOOB Credivertentes para seus associados. O conteúdo deste material foi desenvolvido baseado nas informações da "Cartilha de Segurança da Informação" disponibilizada pelo Sicoob Confederação.

Nome completo: _____

RG/CPF: _____

Agência: _____

Assinatura: _____

Local e data: _____

PROTOCOLO DE ENTREGA

EDIÇÃO

3ª edição / 2020

PRODUÇÃO

Produzido pelo SICOOB Credivertentes e baseado na Cartilha de Segurança da Informação do Sicoob Confederação

DIAGRAMAÇÃO

Mapa de Minas Comunicação Integrada

IDENTIFICAÇÃO

Razão Social: Cooperativa de Crédito de Livre Admissão Campos das Vertentes Ltda.

CNPJ: 22.724.710/0001-05

Endereço: Rua Carlos Pereira, 100 - Centro

CEP: 36.350-000 São Tiago - MG

Telefone: (32) 3376-1386

www.credivertentes.com.br

SICOOB
Credivertentes