

Cartilha de Segurança da Informação



Índice

1. Conceitos de Segurança

- 1.1. O que é Segurança da Informação?
- 1.2. Cuidado com os vírus de computador
- 1.3. Dicas para manter o computador seguro

2. Navegando na Internet com Segurança

- 2.1. Fique atento aos endereços acessados no seu navegador
- 2.2. Compras e pagamentos

3. Utilização do e-mail e programas de mensagem instantânea com segurança

- 3.1. Nunca abra e-mails ou execute arquivos enviados por desconhecidos
- 3.2. Bancos não enviam e-mails não solicitados a seus clientes
- 3.3. Fique atento ao utilizar programas como MSN, Google Talk, Skype etc

4. Utilização de Internet Banking

- 4.1. Procure pelos sinais de segurança
- 4.2. Navegue diretamente na url do seu banco
- 4.3. Não realize operações bancárias em lugares públicos
- 4.4. Mantenha a salvo sua identidade eletrônica
- 4.5. Troque suas senhas com certa frequência
- 4.6. Cadastramento de computadores
- 4.7. Relate qualquer irregularidade ao seu banco

5. Utilização de Caixas Automáticos - ATM

6. Engenharia Social

7. Administração segura de suas senhas

8. Glossário

**O significado é
segurança!**



Conceitos de Segurança



I.1 O que é Segurança da Informação?

Denomina-se Segurança da Informação a proteção existente sobre as informações de uma determinada empresa ou pessoa. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa.

I.2 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.

1.3 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.

2. Navegando na Internet com Segurança



2.1 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.

2.2 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 bancários, 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.

3

Utilização do E-mail e programas de mensagem instantânea com segurança



3.1 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 email e, caso seja necessário clicar, fique atento para ver onde 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.

3.2 Bancos não enviam e-mails não solicitados a seus clientes

- Fraudadores bancários geralmente enviam e-mails falsos solicitando que você informe seus dados ou senhas bancárias;
- Muitas vezes falsos e-mails de bancos levam você a clicar em links que podem causar situações perigosas, como:
 - ❖ levá-lo a um site falso do seu banco 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.

3.3 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.

4 ■ Utilização de Internet Banking



A utilização segura das facilidades oferecidas pelo Internet Banking requer alguns cuidados que recomendamos abaixo:

4.1 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 do banco 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;

4.2 Navegue diretamente na URL do seu banco

- Evite acessar seu banco clicando em links de outros sites. NUNCA acesse seu banco 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 do seu banco é escrever sempre o endereço diretamente no seu navegador, por exemplo: <http://www.sicoobnet.com.br>.

4.3 Não realize operações bancárias 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.

4.4 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.

4.5 Troque suas senhas com certa freqüência

- 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.

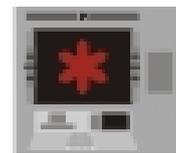
4.6 Cadastramento de computadores

- 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.

4.7 Relate qualquer irregularidade ao seu banco

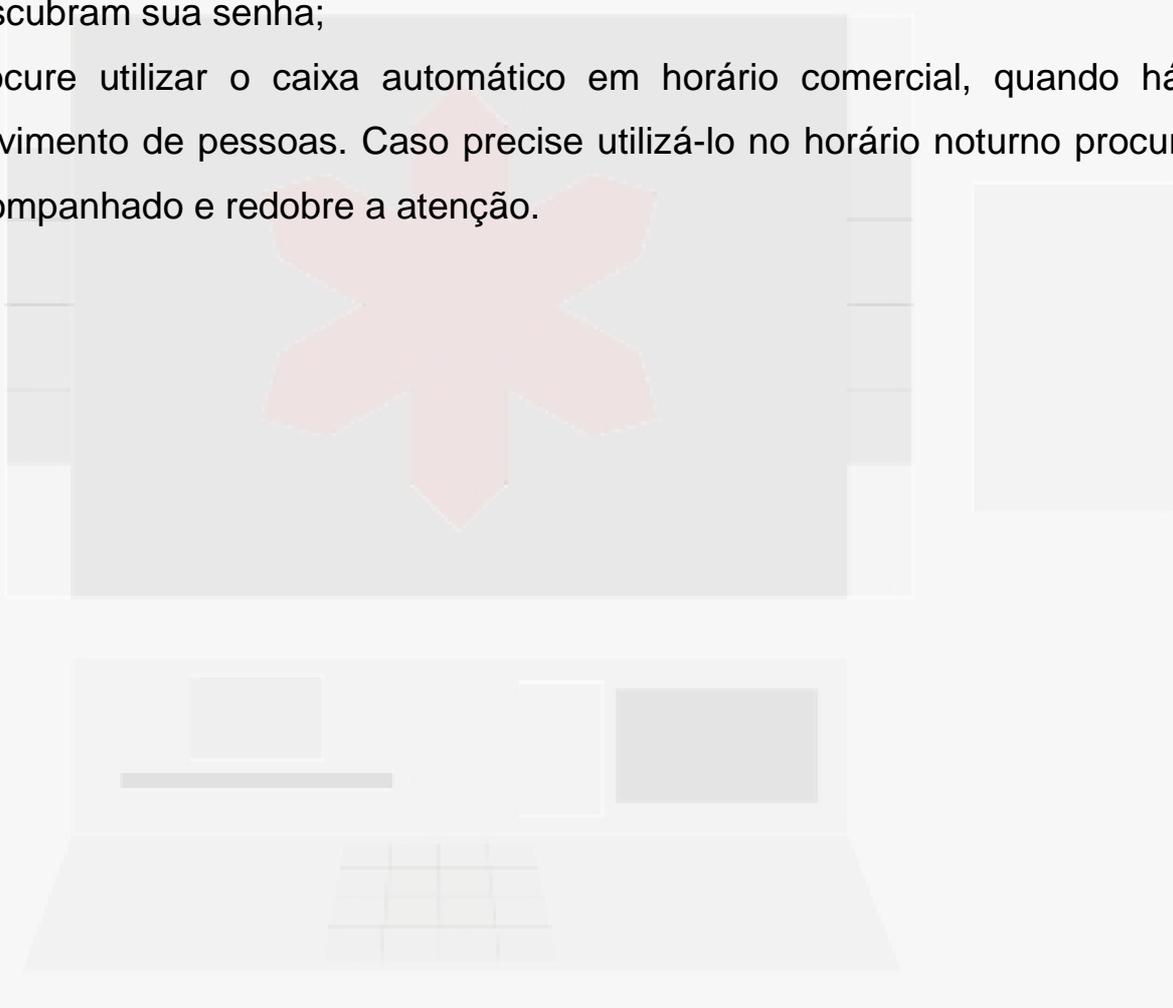
- Verifique sempre seus saldos e extratos bancários para certificar-se de que não contenham transações suspeitas ou desconhecidas, caso em que você deve contatar seu banco e solicitar esclarecimentos;
- Para contatos com o banco utilize os números de telefone encontrados no cartão do banco, nas correspondências bancárias, 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.

5. Utilização de Caixas Automáticas – ATM



Tenha sempre muita atenção ao utilizar os terminais de auto-atendimento:

- Fique atento às pessoas ao seu redor e nunca aceite ajuda de desconhecidos;
- Proteja o teclado com as mãos ou com o corpo, para evitar que outras pessoas descubram sua senha;
- Procure utilizar o caixa automático em horário comercial, quando há maior movimento de pessoas. Caso precise utilizá-lo no horário noturno procure estar acompanhado e redobre a atenção.



6 ■ Engenharia Social



- Consiste da obtenção de informações importantes por meio de uma conversa informal, aproveitando da ingenuidade das pessoas, explorando sua confiança ou a vontade de ajudar;
- 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 mal-intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou corporativas antes de descartá-los no lixo.

7

■ Administração Segura de suas Senhas



- Sua senha é pessoal e intransferível. Compartilhar sua senha é como assinar um cheque em branco;
- Não escreva a senha em local público ou de fácil acesso como, por exemplo, em sua agenda, em um pedaço de papel pregado no seu monitor ou guardado na sua gaveta;
- Troque a senha regularmente ou sempre que suspeitar de quebra de sigilo;
- Não utilize números fáceis de serem descobertos, tais como o número da carteira de identidade, do CPF e de outros documentos ou datas de qualquer espécie, como sua senha bancária.

8 ■ Glossário



Backdoor (Porta dos fundos) – é uma falha de segurança (casual ou intencional) que existe em um programa de computador ou sistema operacional, que permite a um invasor obter total controle da máquina sem que o usuário perceba.

Cavalo de Tróia (*Trojan Horse*) – é um programa que além de executar as funções para as quais foi aparentemente projetado também executa outras funções, normalmente maliciosas, sem o conhecimento do usuário, tais como, furto de senhas, de números de cartões de crédito e outras informações pessoais e, também, inclusão de *backdoors*.

Cracker – é o termo usado para designar quem quebra um sistema de segurança de forma ilegal ou sem ética. *Crackers* utilizam seus conhecimentos para fins como vandalismo, revanchismo, espionagem, roubo ou qualquer prática criminosa em benefício próprio ou corporativo.

Criptografia – é uma técnica capaz de transformar a informação da sua forma original para uma forma ilegível para pessoas não autorizadas.

Download – significa baixar ou descarregar para seu computador, celular ou outro aparelho um arquivo localizado em um computador, site remoto ou em um e-mail recebido. Ao realizar um *download* você transfere para o seu aparelho um arquivo que pode ser uma música, um vídeo, um *programa*, um *malware* etc.

Engenharia Social – conjunto de técnicas utilizadas para conseguir informações privilegiadas e/ou indevidas, persuadindo, manipulando, enganando ou explorando a confiança das pessoas. Essas técnicas são aplicadas por meio do uso de e-mails falsos, telefonemas, salas de bate-papo ou mesmo pessoalmente.

Internet – rede de milhões de computadores de todo o mundo interligados por linhas telefônicas, fibras óticas, rádios e satélites. Além de conectar redes de computadores, interliga milhões de pessoas que formam suas redes de relacionamento e navegam pelas informações disponíveis no espaço virtual, também chamado de Ciberespaço.

Keylogger – programa malicioso que, uma vez instalado no computador, captura o que o usuário digitar, tal como contas bancárias, senhas e outras informações pessoais. As informações capturadas podem ser enviadas para computadores remotos e utilizadas para realizar transações fraudulentas.

Lan House – são centros públicos de acesso à Internet com vários computadores em rede.

Malware – é um termo genérico utilizado para denominar qualquer tipo de código/programa malicioso. Inclui vírus, worms, spywares, trojans, backdoors, rootkits, keyloggers etc.

Spam – e-mail não solicitado pelo remetente, com conteúdo irrelevante ou inapropriado, em geral com propósitos comerciais.

Spyware – programa de computador que, uma vez instalado, coleta informações relacionadas às atividades do usuário e as envia para computadores remotos.

Trojan ou trojan horse – vide cavalo de tróia.

URL (Uniform Resource Locator) – denominação técnica do endereço utilizado para acessar determinado site ou serviço. Ex: <http://www.sicoobnet.com.br>.

Vírus – são programas de computador criados com algum tipo de intenção maliciosa, como roubar dados, danificar ou invadir sistemas.

Worms – são códigos maliciosos que se espalham automaticamente pela rede de computadores sem que sejam percebidos. Um worm pode realizar ações perigosas, como consumir banda de rede e recursos locais, causando sobrecarga dos servidores ou da rede e indisponibilidade dos serviços.

