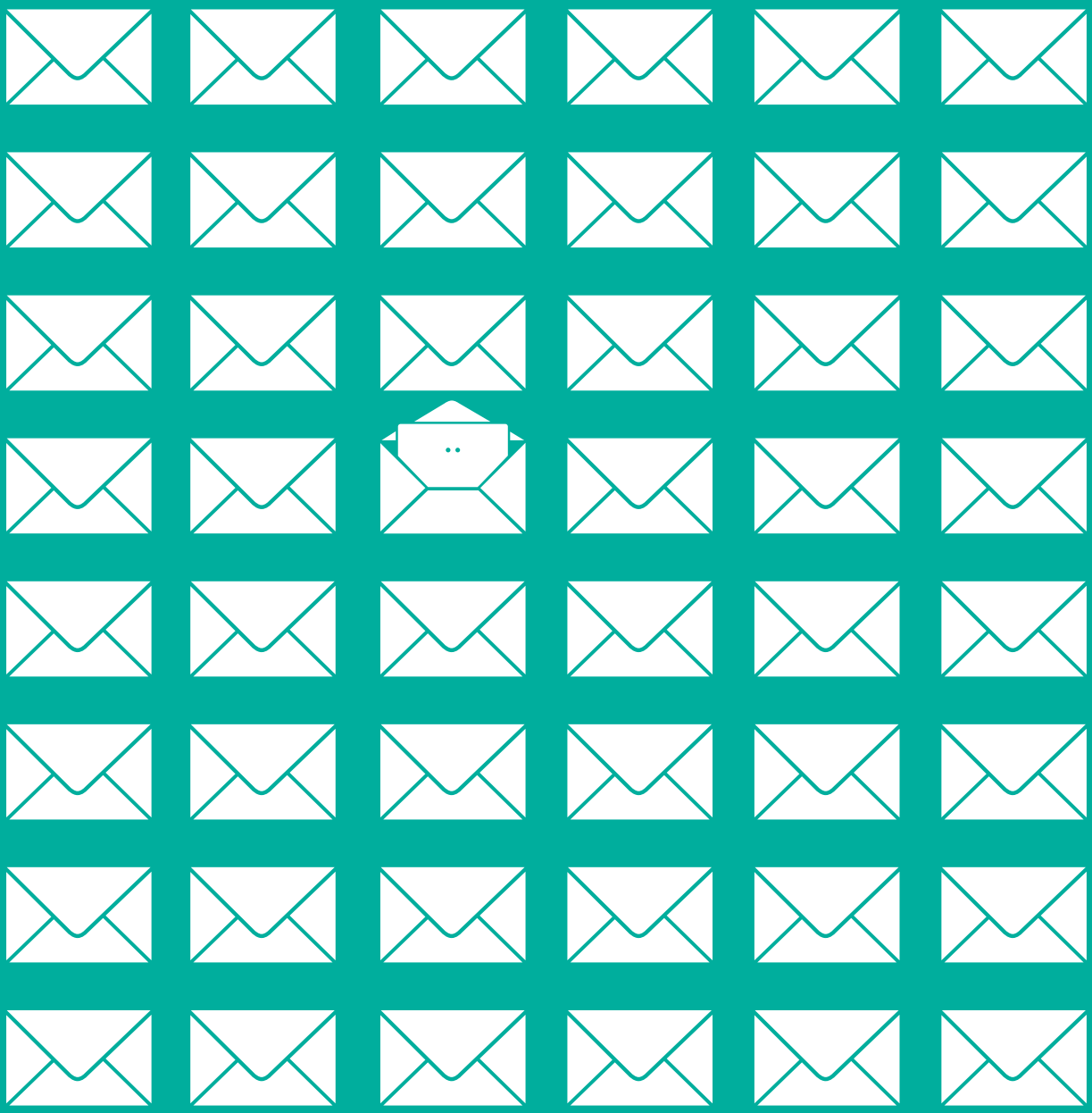

CARTILHA DE SEGURANÇA DA INFORMAÇÃO

SICOOB

Índice

1. Conceitos de Segurança

1.1 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.

1.2 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 páginas Web maliciosas, utilizando navegadores vulneráveis;
    - Embutidos em arquivos ou programas baixados pela Internet, anexados a e-mails ou recebidos por meio de sites de relacionamento e redes sociais;
  - Acessando links patrocinados fraudulentos (Malvertising) obtidos através de ferramentas de busca como Google/Yahoo;
  - Através da exploração de vulnerabilidades existentes em programas instalados.

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 abrí-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 legítimos, de fontes confiáveis, evitando sites de compartilhamento de softwares piratas, pois estes são as 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 as extensões 'PIF', 'SCR', 'BAT', 'VBS', 'CPL', 'COM' e principalmente 'EXE', quando recebidos por e-mail ou de fonte não confiável ou duvidosa. 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.
- Ao adquirir ou alugar equipamentos acessíveis via rede, como roteadores Wi-Fi e modems ADSL (eles podem estar configurados com senha padrão, facilmente obtida na Internet). Altere as senhas padrão para evitar o acesso não autorizado aos equipamentos.
- Caso necessite utilizar computadores de terceiros, utilize o modo de navegação anônima, isso evita que os dados fiquem registrados no computador.
- Ao compartilhar recursos do seu computador, estabeleça senhas para os compartilhamentos e permissões de acesso adequadas.

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 deseja 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;
- 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;
- Desconfie de e-mails do tipo 'Cartão virtual', 'Intimação da Polícia Federal', 'atualização cadastral do banco', 'Seu computador está infectado'. Os e-mails podem conter anexos ou links que podem infectar a máquina quando acessados. 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 Sicoob não envia e-mails aos seus associados

- 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 serviços de mensagem instantânea como Skype, Google talk, Facebook messenger etc Fique atento ao utilizar programas como Google Talk, Skype etc.

- Caso haja necessidade de aceitar algum tipo de arquivo, tenha um antivírus atualizado em sua máquina e tenha certeza da identidade da pessoa que está enviando. 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;
- Desconfie de contatos de desconhecidos que alegam ser representantes de instituição financeira, suporte de computadores etc. e que solicitam dados pessoais e/ou sigilosos.

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 na barra de status (parte inferior), ou à direita da caixa da URL, dependendo do navegador;
- 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 sua instituição financeira através de links de outros sites ou resultados obtidos através de sites de busca. Sempre acesse sua conta usando a página ou o aplicativo fornecido pela própria instituição;
- A forma mais segura de visitar o site do seu banco é escrever sempre o endereço diretamente no seu navegador, por exemplo: https://www.sicoob.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 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.

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 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 na internet. 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.
- Como não exige conexão de dados ativa, funcionará também em locais sem cobertura de operadoras de celular ou em falhas desta cobertura.

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.

Tenha sempre muita atenção ao utilizar os terminais de autoatendimento:

- 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.

4.8 Segurança no uso do SicoobNet Celular

- Não utilize aparelhos de outras pessoas para acessar aos serviços do Sicoobnet Celular ou efetuar transações por meio deste canal, pois seus dados podem ficar armazenados na memória do celular;
- Funcionalidades de conectividade sem fio como Bluetooth podem tornar seu aparelho mais vulnerável e suscetível a ataques, envio de vírus e arquivos maliciosos. Recomenda-se manter tais funcionalidades desabilitadas;
- Exclua ou bloqueie o celular da lista de permissão de cadastro de computadores utilizados, caso você troque de número ou de aparelho;
- Desconfie de mensagens solicitando recadastramento de dispositivos, atualização cadastral, ou solicitando informações pessoais, pois pode se tratar de uma tentativa de fraude.

5. *Utilização de Caixas Automáticos – 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;
- Caso perceba algo estranho no terminal de autoatendimento, ou característica diferente da usual, não utilize o equipamento e comunique à cooperativa.

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;
- 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.

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. *Dispositivos Móveis*

- Evite usar redes Wi-Fi públicas para acessar sua instituição financeira.
- Procure obter aplicativos de fontes confiáveis, como lojas oficiais ou o site do fabricante.
- Ao instalar aplicativos, verifique se as permissões solicitadas para a instalação e execução são coerentes com a finalidade do aplicativo.
- Seja cuidadoso ao permitir que os aplicativos acessem seus dados pessoais.
- Utilize mecanismos de segurança, como antivírus, antispam, antispyware e antimalware.
- Mantenha o dispositivo atualizado com as versões mais recentes de todos os aplicativos instalados.
- Cadastre uma senha para o aparelho e configure o bloqueio na tela inicial, para que seja ativado quando o aparelho não está em uso.
- Ao se desfazer de um dispositivo móvel, apague os dados e restaure as configurações de fábrica.

9. Glossário

Antimalware

Ferramenta que procura detectar e anular ou remover os códigos maliciosos de um computador. Os programas antivírus, *antispyware*, *antirootkit* e *antitroja*n são exemplos de ferramentas *antimalware*.

Ataque

Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede.

BACKDOOR

Tipo de código malicioso. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim. Normalmente esse programa é colocado de forma a não a ser notado.

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.

Conexão segura

Conexão que utiliza um protocolo de criptografia para a transmissão de dados, como por exemplo, HTTPS ou SSH.

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.

DNS

Do inglês *Domain Name System*. O sistema de nomes de domínios, responsável pela tradução, entre outros tipos, de nome de máquinas/domínios para o endereço IP correspondente e vice-versa.

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.

Endereço IP

Sequência de números associada a cada computador conectado à Internet. No caso de IPv4, o endereço IP é dividido em quatro grupos, separados por "." e compostos por números entre 0 e 255, por exemplo, "192.0.2.2".

ENGENHARIA SOCIAL

Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desta Cartilha, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social.

Filtro antispam

Programa que permite classificar os e-mails conforme regras pré-definidas, de forma a impedir que e-mails mal intencionados cheguem às caixas postais dos usuários.

Firewall

Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

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

Tipo específico de spyware. Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.

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.

Malvertising

Do inglês *Malicious advertsing*. Tipo de golpe que consiste em criar anúncios maliciosos e, por meio de serviços de publicidade, apresentá-los em diversas páginas Web. Geralmente, o serviço de publicidade é induzido a acreditar que se trata de um anúncio legítimo e, ao aceitá-lo, intermedia a apresentação e faz com que ele seja mostrado em diversas páginas.

Phishing, phishing scam, phishing/scam

Tipo de golpe por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

SPAM

Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

SPYWARE

Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware.

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

Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

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.


SICOOB