

1. Cuidados a serem tomados ao usar suas contas e senhas:

- Certifique-se de não estar sendo observado ao digitar as suas senhas;
- Não forneça as suas senhas para outra pessoa, em hipótese alguma;
- Certifique-se de fechar a sua sessão ao acessar *sites* que requeiram o uso de senhas. Use a opção de sair (*logout*), pois isto evita que suas informações sejam mantidas no navegador;
- Elabore boas senhas;
- Altere as suas senhas sempre que julgar necessário;
- Não use a mesma senha para todos os serviços que acessa;
- Ao usar perguntas de segurança para facilitar a recuperação de senhas, evite escolher questões cujas respostas possam ser facilmente adivinhadas;
- Certifique-se de utilizar serviços criptografados quando o acesso a um *site* envolver o fornecimento de senha;
- Procure manter sua privacidade, reduzindo a quantidade de informações que possam ser coletadas sobre você, pois elas podem ser usadas para adivinhar a sua senha, caso você não tenha sido cuidadoso ao elaborá-la;
- Seja cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos.

2. Elaboração de senhas

Alguns elementos que você **não deve** usar na elaboração de suas senhas são:

- **Qualquer tipo de dado pessoal:** evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas (estes dados podem ser facilmente obtidos e usados por pessoas que queiram tentar se autenticar como você).
- **Sequências de teclado:** evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG", pois são bastante conhecidas e podem ser facilmente observadas ao serem digitadas.
- **Palavras que façam parte de listas:** evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas

Alguns elementos que você **deve** usar na elaboração de suas senhas são:

- **Números aleatórios:** quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem **exclusivamente** caracteres numéricos.
- **Grande quantidade de caracteres:** quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente.
- **Diferentes tipos de caracteres:** quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

Algumas dicas práticas que você pode usar na elaboração de boas senhas são:

- **Selecione caracteres de uma frase:** baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "O Cravo brigou com a Rosa debaixo

- de uma sacada" você pode gerar a senha "?OCbcaRddus" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).
- **Utilize uma frase longa:** escolha uma frase longa, que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas a você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha "1 dia ainda verei os anéis de Saturno!!!".
 - **Faça substituições de caracteres:** invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei do Sistema Solar" você pode gerar a senha "SS0L, asstrr0-rrei d0 SSisstema SS0Larr".

3. Segurança de computadores

- Mantenha os programas instalados com as versões mais recentes;
- Mantenha os programas instalados com todas as atualizações aplicadas;
- Use apenas programas originais;
- Mantenha seu computador com a data e a hora corretas;
- Crie um disco de recuperação de sistema;
- Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros;
- Procure manter a segurança física do seu computador, utilizando travas que dificultem que ele seja aberto, que tenha peças retiradas ou que seja furtado, como cadeados e cabos de aço;
- Procure manter seu computador bloqueado, para evitar que seja usado quando não estiver por perto (isso pode ser feito utilizando protetores de tela com senha ou com programas que impedem o uso do computador caso um dispositivo específico não esteja conectado);
- Configure seu computador para solicitar senha na tela inicial (isso impede que alguém reinicie seu computador e o acesse diretamente);
- Utilize criptografia de disco para que, em caso de perda ou furto, seus dados não sejam indevidamente acessados.

4. Uso seguro da Internet

A Internet traz inúmeras possibilidades de uso, porém para aproveitar cada uma delas de forma segura é importante que alguns cuidados sejam tomados. Além disto, como grande parte das ações realizadas na Internet ocorrem por intermédio de navegadores *Web* é igualmente importante que você saiba reconhecer os tipos de conexões existentes e verificar a confiabilidade dos certificados digitais antes de aceitá-los.

Alguns dos principais usos e cuidados que você deve ter ao utilizar a Internet são:

Ao usar navegadores *Web*:

- Mantenha-o atualizado, com a versão mais recente e com todas as atualizações aplicadas;
- Configure-o para verificar automaticamente atualizações, tanto dele próprio como de complementos que estejam instalados;

- Permita a execução de programas *Java* e *JavaScript*, porém assegure-se de utilizar complementos, como o NoScript (disponível para alguns navegadores), para liberar gradualmente a execução, conforme necessário, e apenas em *sites* confiáveis;
- Permita que programas *ActiveX* sejam executados apenas quando vierem de *sites* conhecidos e confiáveis;
- Seja cuidadoso ao usar *cookies* caso deseje ter mais privacidade;
- Caso opte por permitir que o navegador grave as suas senhas, tenha certeza de cadastrar uma chave mestra e de jamais esquecê-la
- Mantenha seu computador seguro).

Ao usar programas leitores de *e-mails*:

- Mantenha-o atualizado, com a versão mais recente e com as todas atualizações aplicadas;
- Configure-o para verificar automaticamente atualizações, tanto dele próprio como de complementos que estejam instalados;
- Não utilize-o como navegador *Web* (desligue o modo de visualização no formato HTML);
- Seja cuidadoso ao usar *cookies* caso deseje ter mais privacidade;
- Seja cuidadoso ao clicar em *links* presentes em *e-mails* (se você realmente quiser acessar a página do *link*, digite o endereço diretamente no seu navegador *Web*);
- Desconfie de arquivos anexados à mensagem mesmo que tenham sido enviados por pessoas ou instituições conhecidas (o endereço do remetente pode ter sido falsificado e o arquivo anexo pode estar infectado);
- Antes de abrir um arquivo anexado à mensagem tenha certeza de que ele não apresenta riscos, verificando-o com ferramentas *antimalware*;
- Verifique se seu sistema operacional está configurado para mostrar a extensão dos arquivos anexados;
- Desligue as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
- Desligue as opções de execução de *JavaScript* e de programas *Java*;
- Habilite, se possível, opções para marcar mensagens suspeitas de serem fraude;
- Use sempre criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
- Mantenha seu computador seguro.

Ao acessar *Webmails*:

- Seja cuidadoso ao acessar a página de seu *Webmail* para não ser vítima de *phishing*. Digite a URL diretamente no navegador e tenha cuidado ao clicar em *links* recebidos por meio de mensagens eletrônicas;
- Não utilize um *site* de busca para acessar seu *Webmail* (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas);
- Seja cuidadoso ao elaborar sua senha de acesso ao *Webmail* para evitar que ela seja descoberta por meio de ataques de força bruta
- Configure opções de recuperação de senha, como um endereço de *e-mail* alternativo, uma questão de segurança e um número de telefone celular;
- Evite acessar seu *Webmail* em computadores de terceiros e, caso seja realmente necessário, ative o modo de navegação anônima
- Certifique-se de utilizar conexões seguras sempre que acessar seu *Webmail*, especialmente ao usar redes Wi-Fi públicas. Se possível configure para que, por padrão, sempre seja utilizada conexão via "https";
- Mantenha seu computador seguro.

Ao efetuar transações bancárias e acessar *sites* de *Internet Banking*:

- Certifique-se da procedência do *site* e da utilização de conexões seguras ao realizar transações bancárias via *Web*;
- Somente acesse *sites* de instituições bancárias digitando o endereço diretamente no navegador *Web*, nunca clicando em um *link* existente em uma página ou em uma mensagem;
- Não utilize um *site* de busca para acessar o *site* do seu banco (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas);
- Ao acessar seu banco, forneça apenas uma posição do seu cartão de segurança (desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição);
- Não forneça senhas ou dados pessoais a terceiros, especialmente por telefone;
- Desconsidere mensagens de instituições bancárias com as quais você não tenha relação, principalmente aquelas que solicitem dados pessoais ou a instalação de módulos de segurança;
- Sempre que ficar em dúvida, entre em contato com a central de relacionamento do seu banco ou diretamente com o seu gerente;
- Não realize transações bancárias por meio de computadores de terceiros ou redes Wi-Fi públicas;
- Verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito e, caso detecte algum lançamento suspeito, entre em contato imediatamente com o seu banco ou com a operadora do seu cartão;
- Antes de instalar um módulo de segurança, de qualquer *Internet Banking*, certifique-se de que o autor módulo é realmente a instituição em questão;
- Mantenha seu computador seguro.

Ao efetuar transações comerciais e acessar *sites* de comércio eletrônico:

- Certifique-se da procedência do *site* e da utilização de conexões seguras ao realizar compras e pagamentos via *Web*;
- Somente acesse *sites* de comércio eletrônico digitando o endereço diretamente no navegador *Web*, nunca clicando em um *link* existente em uma página ou em uma mensagem;
- Não utilize um *site* de busca para acessar o *site* de comércio eletrônico que você costuma acessar (não há necessidade disto, já que URLs deste tipo são, geralmente, bastante conhecidas);
- Pesquise na Internet referências sobre o *site* antes de efetuar uma compra;
- Desconfie de preços muito abaixo dos praticados no mercado;
- Não realize compras ou pagamentos por meio de computadores de terceiros ou redes Wi-Fi públicas;
- Sempre que ficar em dúvida, entre em contato com a central de relacionamento da empresa onde está fazendo a compra;
- Verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito e, caso detecte algum lançamento suspeito, entre em contato imediatamente com o seu banco ou com a operadora do seu cartão de crédito;
- Ao efetuar o pagamento de uma compra, nunca forneça dados de cartão de crédito em *sites* sem conexão segura ou em *e-mails* não criptografados;
- Mantenha seu computador seguro.

5. Segurança em dispositivos móveis

Dispositivos móveis, como *tablets*, *smartphones*, celulares e PDAs, têm se tornado cada vez mais populares e capazes de executar grande parte das ações realizadas em computadores pessoais, como navegação *Web*, *Internet Banking* e acesso a *e-mails* e redes sociais. Infelizmente, as semelhanças não se restringem apenas às funcionalidades apresentadas, elas também incluem os riscos de uso que podem representar.

Assim como seu computador, o seu dispositivo móvel também pode ser usado para a prática de atividades maliciosas, como furto de dados, envio de *spam* e a propagação de códigos maliciosos, além de poder fazer parte de *botnets* e ser usado para disparar ataques na Internet.

Somadas a estes riscos, há características próprias que os dispositivos móveis possuem que, quando abusadas, os tornam ainda mais atraentes para atacantes e pessoas mal-intencionadas, como:

Grande quantidade de informações pessoais armazenadas: informações como conteúdo de mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, números de cartão de crédito e senhas costumam ficar armazenadas nos dispositivos móveis.

Maior possibilidade de perda e furto: em virtude do tamanho reduzido, do alto valor que podem possuir, pelo status que podem representar e por estarem em uso constante, os dispositivos móveis podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes.

Grande quantidade de aplicações desenvolvidas por terceiros: há uma infinidade de aplicações sendo desenvolvidas, para diferentes finalidades, por diversos autores e que podem facilmente ser obtidas e instaladas. Entre elas podem existir aplicações com erros de implementação, não confiáveis ou especificamente desenvolvidas para execução de atividades maliciosas.

Rapidez de substituição dos modelos: em virtude da grande quantidade de novos lançamentos, do desejo dos usuários de ter o modelo mais recente e de pacotes promocionais oferecidos pelas operadoras de telefonia, os dispositivos móveis costumam ser rapidamente substituídos e descartados, sem que nenhum tipo de cuidado seja tomado com os dados nele gravados.

De forma geral, os cuidados que você deve tomar para proteger seus dispositivos móveis são os mesmos a serem tomados com seu computador pessoal, como mantê-lo sempre atualizado e utilizar mecanismos de segurança. Outros cuidados complementares a serem tomados são:

Antes de adquirir seu dispositivo móvel:

- Considere os mecanismos de segurança que são disponibilizadas pelos diferentes modelos e fabricantes e escolha aquele que considerar mais seguro;
- Caso opte por adquirir um modelo já usado, procure restaurar as configurações originais, ou "de fábrica", antes de começar a usá-lo;
- Evite adquirir um dispositivo móvel que tenha sido ilegalmente desbloqueado (*jailbreak*) ou cujas permissões de acesso tenham sido alteradas. Esta prática, além de ser ilegal, pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho.

Ao usar seu dispositivo móvel:

- Se disponível, instale um programa *antimalware* antes de instalar qualquer tipo de aplicação, principalmente aquelas desenvolvidas por terceiros;
- Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas;
- Fique atento às notícias veiculadas no *site* do fabricante, principalmente as relacionadas à segurança;
- Seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e *plug-ins*. procure usar aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários. Verifique comentários de outros usuários e se as permissões necessárias para a execução são coerentes com a destinação da aplicação;
- Seja cuidadoso ao usar aplicativos de redes sociais, principalmente os baseados em geolocalização, pois isto pode comprometer a sua privacidade.

Ao acessar redes:

- Seja cuidadoso ao usar redes Wi-Fi públicas;

- Mantenha interfaces de comunicação, como *bluetooth*, infravermelho e Wi-Fi, desabilitadas e somente as habilite quando for necessário;
- Configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou "descoberto") por outros dispositivos (em muitos aparelhos esta opção aparece como "Oculto" ou "Invisível").

Proteja seu dispositivo móvel e os dados nele armazenados:

- Mantenha as informações sensíveis sempre em formato criptografado;
- Faça *backups* periódicos dos dados nele gravados;
- Mantenha controle físico sobre ele, principalmente em locais de risco (procure não o deixar sobre a mesa e cuidado com bolsos e bolsas quando estiver em ambientes públicos);
- Use conexão segura sempre que a comunicação envolver dados confidenciais;
- Não siga *links* recebidos por meio de mensagens eletrônicas;
- Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas);
- Configure-o para que seja localizado e bloqueado remotamente, por meio de serviços de geolocalização (isso pode ser bastante útil em casos de perda ou furto);
- Configure-o, quando possível, para que os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso (use esta opção com bastante cautela, principalmente se você tiver filhos e eles gostarem de "brincar" com o seu dispositivo).

Ao se desfazer do seu dispositivo móvel:

- Apague todas as informações nele contidas;
- Restaure a opções de fábrica.

O que fazer em caso de perda ou furto:

- Informe sua operadora e solicite o bloqueio do seu número (*chip*);
- Altere as senhas que possam estar nele armazenadas (por exemplo, as de acesso ao seu *e-mail* ou rede social);
- Bloqueie cartões de crédito cujo número esteja armazenado em seu dispositivo móvel;
- Se tiver configurado a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados nele armazenados.

6. Controle de Acesso

O controle de acesso lógico às telas de negociação é gerido pelos respectivos fornecedores, onde cada um deles possui seus mecanismos próprios para redefinição de senhas e desbloqueio de contas de usuários, sempre mediante a validação de dados. Caso seja necessário, nosso departamento de DMA pode intermediar esse contato para auxiliar os clientes.