Sugestões relacionadas à segurança da informação

Mantenha os programas instalados com as versões mais recentes

Segurança em computadores e dispositivos móveis.
Fabricantes costumam lançar novas versões quando há recursos a serem adicionados e vulnerabilidades a serem corrigidas. Sempre que uma nova versão for lançada, ela deve ser prontamente instalada, pois isto pode ajudar a proteger seu computador da ação de atacantes e códigos maliciosos. Além disto, alguns fabricantes deixam de dar suporte e de desenvolver atualizações para versões antigas, o que significa que vulnerabilidades que possam vir a ser descobertas não serão corrigidas:

- remova programas que você não utiliza mais. Programas não usados tendem a ser esquecidos e a ficar com versões antigas (e potencialmente vulneráveis);
- remova as versões antigas. Existem programas que permitem que duas ou mais versões estejam instaladas ao mesmo tempo. Nestes casos, você deve manter apenas a versão mais recente e remover as mais antigas;
- tenha o hábito de verificar a existência de novas versões, por meio de opções disponibilizadas pelos próprios programas ou acessando diretamente os sites dos fabricantes.

Mantenha os programas instalados com todas as atualizações aplicadas

Quando vulnerabilidades são descobertas, certos fabricantes costumam lançar atualizações específicas, chamadas de patches, hot fixes ou service packs. Portanto, para manter os programas instalados livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis:

- configure, quando possível, para que os programas sejam atualizados automaticamente;
- programe as atualizações automáticas para serem baixadas e aplicadas em horários em que seu computador esteja ligado e conectado à Internet. Alguns programas, por padrão, são configurados para que as atualizações sejam feitas de madrugada, período no qual grande parte dos computadores está desligada (as atualizações que não foram feitas no horário programado podem não ser feitas quando ele for novamente ligado);
- no caso de programas que não possuam o recurso de atualização automática, ou caso você opte por não utilizar este recurso, é importante visitar constantemente os sites dos fabricantes para verificar a existência de novas atualizações;
- utilize programas para verificação de vulnerabilidades, para verificar se os programas instalados em seu computador estão atualizados.

Use apenas programas originais

O uso de programas não originais pode colocar em risco a segurança do seu computador já que muitos fabricantes não permitem a realização de atualizações quando detectam versões não licenciadas. Além disto, a instalação de programas deste tipo, obtidos de mídias e sites não confiáveis ou via programas de compartilhamento de arquivos, pode incluir a instalação de códigos maliciosos:

- ao adquirir computadores com programas pré-instalados, procure certificar-se de que eles são originais solicitando ao revendedor as licenças de uso;
- ao enviar seu computador para manutenção, não permita a instalação de programas que não sejam originais;
- caso deseje usar um programa proprietário, mas não tenha recursos para adquirir a licença, procure por alternativas gratuitas ou mais baratas e que apresentem funcionalidades semelhantes as desejadas.

Use mecanismos de proteção e prevenção

O uso de mecanismos de proteção e prevenção, como programas antimalware e firewall pessoal, pode contribuir para que seu computador não seja infectado/invadido e para que não participe de atividades maliciosas:

- utilize mecanismos de segurança;
- mantenha seu antimalware e antivírus atualizado, incluindo o arquivo de assinaturas;
- assegure-se de ter um firewall pessoal instalado e ativo em seu computador;
- crie um disco de emergência e o utilize quando desconfiar que o antimalware instalado está desabilitado/comprometido ou que o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc.);
- verifique periodicamente os logs gerados pelo seu firewall pessoal, sistema operacional e antimalware (observe se há registros que possam indicar algum problema de segurança).

Use as configurações de segurança já disponíveis

Muitos programas disponibilizam opções de segurança, mas que, por padrão, vêm desabilitadas ou em níveis considerados baixos. A correta configuração destas opções pode contribuir para melhorar a segurança geral do seu computador:

- observe as configurações de segurança e privacidade oferecidas pelos programas instalados em seu computador (como programas leitores de e-mails e navegadores Web) e altere-as caso não estejam de acordo com as suas necessidades.

Seja cuidadoso ao manipular arquivos

Alguns mecanismos, como os programas antimalware, são importantes para proteger seu computador contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança e, por isto, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas:

- seja cuidadoso ao clicar em links, independente de como foram recebidos e de quem os enviou;
- seja cuidadoso ao clicar em links curtos, procure usar complementos que possibilitem que o link de destino seja visualizado;
- não considere que mensagens vindas de conhecidos são sempre confiáveis, pois o campo de remetente pode ter sido falsificado ou elas podem ter sido enviadas de contas falsas ou invadidas;
- desabilite, em seu programa leitor de e-mails, a auto-execução de arquivos anexados;
- desabilite a auto-execução de mídias removíveis (se estiverem infectadas, elas podem comprometer o seu computador ao serem executadas);
- não abra ou execute arquivos sem antes verificá-los com seu antimalware;
- configure seu antimalware para verificar todos os formatos de arquivo pois, apesar de inicialmente algumas extensões terem sido mais usadas para a disseminação de códigos maliciosos, atualmente isso já não é mais válido;
- tenha cuidado com extensões ocultas. Alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos conhecidos. Exemplo: se um atacante renomear o arquivo “exemplo.scr” para “exemplo.txt.scr”, ao ser visualizado o nome do arquivo será mostrado como “exemplo.txt”, já que a extensão “.scr” não será mostrada.

Cuidados ao usar computadores de terceiros

Ao usar outros computadores, seja de seus amigos, na sua escola, em lanhouse e cyber café, é necessário que os cuidados com segurança sejam redobrados. Ao passo que no seu computador é possível tomar medidas preventivas para evitar os riscos de uso da Internet, ao usar um outro computador não há como saber, com certeza, se estes mesmos cuidados estão sendo devidamente tomados e quais as atitudes dos demais usuários. Alguns cuidados que você deve ter são:

- utilize opções de navegar anonimamente, caso queria garantir sua privacidade (você pode usar opções do próprio navegador Web ou anonymizers);
- utilize um antimalware online para verificar se o computador está infectado;
- não efetue transações bancárias ou comerciais;
- não utilize opções como "Lembre-se de mim" e "Continuar conectado";
- não permita que suas senhas sejam memorizadas pelo navegador Web;
- limpe os dados pessoais salvos pelo navegador, como histórico de navegação e cookies (os navegadores disponibilizam opções que permitem que isto seja facilmente realizado);
- assegure-se de sair (logout) de sua conta de usuário, nos sites que você tenha acessado;
- seja cuidadoso ao conectar mídias removíveis, como pen-drives. Caso você use seu pen-drive no computador de outra pessoa, assegure-se de verificá-lo com seu antimalware quando for utilizá-lo em seu computador;
- ao retornar ao seu computador, procure alterar as senhas que, por ventura, você tenha utilizado.

Seja cuidadoso ao enviar seu computador para serviços de manutenção

- procure selecionar uma empresa com boas referências;
- pesquise na Internet sobre a empresa, à procura de opinião de clientes sobre ela;
- não permita a instalação de programas não originais;
- se possível, faça backups dos seus dados antes de enviar seu computador, para não correr o risco de perdê-los acidentalmente ou como parte do processo de manutenção do seu computador;
- se possível, peça que a manutenção seja feita em sua residência, assim fica mais fácil de acompanhar a realização do serviço.

Seja cuidadoso ao utilizar o computador em locais públicos

Quando usar seu computador em público, é importante tomar cuidados para evitar que ele seja furtado ou indevidamente utilizado por outras pessoas:

- 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 você 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.

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.

É importante que você esteja informado dos riscos aos quais está exposto para que possa tomar as medidas preventivas necessárias. Alguns destes riscos são:

- Acesso a conteúdos impróprios ou ofensivos: ao navegar você pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo;
- Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro;
- Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação;
- Furto e perda de dados: os dados presentes em seus equipamentos conectados à Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos;
- Invasão de privacidade: a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não serão repassadas. Além disto, os sites costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado;
- Divulgação de boatos: as informações na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo. Enquanto isto pode ser desejável em certos casos, também pode ser usado para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas;
- Dificuldade de exclusão: aquilo que é divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você e acessada por diferentes pessoas, desde seus familiares até seus chefes;
- Dificuldade de detectar e expressar sentimentos: quando você se comunica via Internet não há como observar as expressões faciais ou o tom da voz das outras pessoas, assim como elas não podem observar você (a não ser que vocês estejam utilizando webcams e microfones). Isto pode dificultar a percepção do risco, gerar mal-entendido e interpretação dúbia;
- Dificuldade de manter sigilo: no seu dia a dia é possível ter uma conversa confidencial com alguém e tomar cuidados para que ninguém mais tenha acesso ao que está sendo dito. Na Internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo;
- Uso excessivo: o uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional;
- Plágio e violação de direitos autorais: a cópia, alteração ou distribuição não autorizada de conteúdos e materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras;
- Outro grande risco relacionado ao uso da Internet é o de você achar que não corre riscos, pois supõe que ninguém tem interesse em utilizar o seu computador ou que, entre os diversos computadores conectados à Internet, o seu dificilmente será localizado. É justamente este tipo de pensamento que é explorado pelos atacantes, pois, ao se sentir seguro, você pode achar que não precisa se prevenir. Esta ilusão, infelizmente, costuma terminar quando os primeiros problemas começam a acontecer. Muitas vezes os atacantes estão interessados em conseguir acesso a grandes quantidades de computadores, independente de quais são, e para isto, podem efetuar varreduras na rede e localizar grande parte dos computadores conectados à Internet, inclusive o seu.

Um problema de segurança em seu computador pode torná-lo indisponível e colocar em risco a confidencialidade e a integridade dos dados nele armazenados. Além disto, ao ser comprometido, seu computador pode ser usado para a prática de atividades maliciosas como, por exemplo, servir de repositório para dados fraudulentos, lançar ataques contra outros computadores (e assim esconder a real identidade e localização do atacante), propagar códigos maliciosos e disseminar spam.

O primeiro passo para se prevenir dos riscos relacionados ao uso da Internet é estar ciente de que ela não tem nada de "virtual". Tudo o que ocorre ou é realizado por meio da Internet é real: os dados são reais e as empresas e pessoas com quem você interage são as mesmas que estão fora dela. Desta forma, os riscos aos quais você está exposto ao usá-la são os mesmos presentes no seu dia a dia e os golpes que são aplicados por meio dela são similares àqueles que ocorrem na rua ou por telefone.

É preciso, portanto, que você leve para a Internet os mesmos cuidados e as mesmas preocupações que você tem no seu dia a dia, como por exemplo: visitar apenas lojas confiáveis, não deixar públicos dados sensíveis, ficar atento quando "for ao banco" ou "fizer compras", não passar informações a estranhos, não deixar a porta da sua casa aberta, etc.

Para tentar reduzir os riscos e se proteger é importante que você adote uma postura preventiva e que a atenção com a segurança seja um hábito incorporado à sua rotina, independente de questões como local, tecnologia ou meio utilizado.

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 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.

Não é indicado bloquear totalmente o recebimento de cookies, pois isto pode impedir o uso adequado ou até mesmo o acesso a determinados sites e serviços. Para se prevenir dos riscos, mas sem comprometer a sua navegação, há algumas dicas que você deve seguir, como:

- ao usar um navegador Web baseado em níveis de permissão, como o Internet Explorer, procure não selecionar níveis de permissão inferiores a "médio";
- em outros navegadores ou programas leitores de e-mail, configure para que, por padrão, os sites não possam definir cookies e crie listas de exceções, cadastrando sites considerados confiáveis e onde o uso de cookies é realmente necessário, como Webmails e de Internet Banking e comércio eletrônico;
- caso você, mesmo ciente dos riscos, decida permitir que por padrão os sites possam definir cookies, procure criar uma lista de exceções e nela cadastre os sites que deseja bloquear;
- configure para que os cookies sejam apagados assim que o navegador for fechado;
- configure para não aceitar cookies de terceiros (ao fazer isto, a sua navegação não deverá ser prejudicada, pois apenas conteúdos relacionados a publicidade serão bloqueados);
- utilize opções de navegar anonimamente, quando usar computadores de terceiros (ao fazer isto, informações sobre a sua navegação, incluindo cookies, não serão gravadas).

Veja que, quando você altera uma configuração de privacidade ela é aplicada aos novos cookies, mas não aos que já estão gravados em seu computador. Assim, ao fazer isto, é importante que você remova os cookies já gravados para garantir que a nova configuração seja aplicada a todos.

Janelas de pop-up

Janelas de pop-up são aquelas que aparecem automaticamente e sem permissão, sobrepondo a janela do navegador Web, após você acessar um site. Alguns riscos que podem representar são:

- apresentar mensagens indesejadas, contendo propagandas ou conteúdo impróprio;
- apresentar links, que podem redirecionar a navegação para uma página falsa ou induzi-lo a instalar códigos maliciosos.

Prevenção

- configure seu navegador Web para, por padrão, bloquear janelas de pop-up;
- crie uma lista de exceções, contendo apenas sites conhecidos e confiáveis e onde forem realmente necessárias.

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;
- 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 deixá-lo 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:

- infome 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.

Senhas

A sua conta de usuário é de conhecimento geral e é o que permite a sua identificação. Ela é, muitas vezes, derivada do seu próprio nome, mas pode ser qualquer sequência de caracteres ou números que permita que você seja identificado unicamente.

Uma senha, ou password, serve para autenticar uma conta, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a simplicidade que possui.

Elaboração de senhas

Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também não convém que você crie uma senha fácil de ser lembrada se ela puder ser facilmente descoberta por um atacante.

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? O CbcaRddus (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 à 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 aneis 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".

Você deve alterar a sua senha imediatamente sempre que desconfiar que ela pode ter sido descoberta ou que o computador no qual você a utilizou pode ter sido invadido ou infectado.

Algumas situações onde você deve alterar rapidamente a sua senha são:

- se um computador onde a senha esteja armazenada tenha sido furtado ou perdido;
- se usar um padrão para a formação de senhas e desconfiar que uma delas tenha sido descoberta. Neste caso, tanto o padrão como todas as senhas elaboradas com ele devem ser trocadas pois, com base na senha descoberta, um atacante pode conseguir inferir as demais;
- se utilizar uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles. Neste caso, esta senha deve ser alterada em todos os lugares nos quais é usada;
- ao adquirir equipamentos acessíveis via rede, como roteadores Wi-Fi, dispositivos bluetooth e modems ADSL (Asymmetric Digital Subscriber Line). Muitos destes equipamentos são configurados de fábrica com senha padrão, facilmente obtida em listas na Internet, e por isto, sempre que possível, deve ser alterada.

Nos demais casos é importante que a sua senha seja alterada regularmente, como forma de assegurar a confidencialidade. Não há como definir, entretanto, um período ideal para que a troca seja feita, pois depende diretamente de quão boa ela é e de quanto você a expõe.

Não convém que você troque a senha em períodos muito curtos (menos de um mês, por exemplo) se, para conseguir se recordar, precisará elaborar uma senha fraca ou anotá-la em um papel e colá-lo no monitor do seu computador. Períodos muito longos (mais de um ano, por exemplo) também não são desejáveis pois, caso ela tenha sido descoberta, os danos causados podem ser muito grandes.

Guarda de senhas

Salvar as senhas no navegador Web. Esta prática é bastante arriscada, pois caso as senhas não estejam criptografadas com uma chave mestra, elas podem ser acessadas por códigos maliciosos, atacantes ou outras pessoas que venham a ter acesso ao computador:

- assegure-se de configurar uma chave mestra;
- seja bastante cuidadoso ao elaborar sua chave mestra, pois a segurança das demais senhas depende diretamente da segurança dela;
- não esqueça sua chave mestra.

Para não ter que recorrer a estas técnicas ou correr o risco de esquecer suas contas/senhas ou, pior ainda, ter que apelar para o uso de senhas fracas, você pode buscar o auxílio de algumas das formas de gerenciamento disponíveis.

Uma forma bastante simples de gerenciamento é listar suas contas/senhas em um papel e guardá-lo em um local seguro (como uma gaveta trancada). Neste caso, a segurança depende diretamente da dificuldade de acesso ao local escolhido para guardar este papel (de nada adianta colá-lo no monitor, deixá-lo embaixo do teclado ou sobre a mesa). Veja que é preferível usar este método a optar pelo uso de senhas fracas pois, geralmente, é mais fácil garantir que ninguém terá acesso físico ao local onde o papel está guardado do que evitar que uma senha fraca seja descoberta na Internet.