

# Dicas de Segurança

Grande parte dos problemas de segurança ocorrem por puro desconhecimento dos procedimentos básicos de segurança por parte dos usuários. Saber como agir em caso de problemas, também poderá ajudar, e muito, nas investigações policiais dos crimes virtuais.

Mas, como utilizar a internet de maneira segura? Vejamos alguns pontos a considerar.

## 1. Uso de Senhas

Uma senha ou password na Internet, ou em qualquer sistema computacional, serve para autenticar o usuário, ou seja, a senha garante que determinado indivíduo que se utiliza de um serviço é ele mesmo. Se você fornece sua senha para uma outra pessoa, esta poderá utilizar a senha para se passar por você na Internet e, dependendo do caso, o estrago poderá ser grande. Portanto, a senha merece consideração especial, afinal, ela é de sua inteira responsabilidade.

### 1.1 Como escolher uma senha?

Evite utilizar senhas que contenham o seu sobrenome, números de documentos, placas de carros, números de telefones e datas deverão estar fora de sua lista de senhas. Pois esses dados são muito fáceis de se obter e qualquer criminoso tentaria utilizar este tipo de informações para se autenticar como você.

## 2. Problemas usuais

### 2.1 Engenharia Social

O termo é utilizado para os métodos de obtenção de informações importantes do usuário, através de sua ingenuidade ou da confiança. Quem está mal intencionado geralmente utiliza telefone, e-mails ou salas de bate-papo para obter as informações que necessita.

Por exemplo: algum desconhecido liga para a sua casa e se diz do suporte técnico do seu provedor. Nesta ligação ele te convence de que sua conexão com a Internet está problemática e pede sua senha para corrigir o problema.

Como sempre, o bom senso nestes casos é tudo. Duvide desse tipo de abordagem e contate o provedor caso algum técnico ligue para sua casa pedindo dados confidenciais a seu respeito (senhas, números de cartões, etc.) avisando-o do ocorrido.

Outro caso típico são sites desconhecidos que prometem "horas grátis" em seu provedor caso você passe o seu username e a sua senha para eles. É claro que eles utilizarão estes dados para conseguir "horas grátis", não para você mas para eles.

### 2.2 Cavalos de Tróia

Conta a mitologia grega, que há muito tempo atrás, houve uma guerra entre as cidades de Atenas e de Tróia. Como Tróia era extremamente fortificada, os militares gregos a consideravam inexpugnável. Para dominá-la os gregos construíram uma enorme estátua de madeira na forma de um cavalo e deram de presente para os troianos que a aceitaram de bom grado. O problema é que o cavalo foi recheado com centenas de soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos soldados gregos e a dominação de Tróia. Daí surgiram os termos Presente de Grego e Cavalo de Tróia.

Em tempos modernos o cavalo virou um programa e a cidade o seu computador. Conhecidos como Cavalos de Tróia ou Trojan Horses estes programas são construídos de tal maneira que, uma vez instalados nos computadores, abrem portas em seus micros, tornando possível o roubo de informações (arquivos, senhas, etc.).

#### 2.2.1 Como meu computador pode ser infectado por um Cavalo de Tróia?

Normalmente você receberá o Cavalo de Tróia como presente (de grego). Ele pode ser dado a você de várias maneiras, mas na maioria das vezes ele vem anexado a algum e-mail. Estes e-mails vêm acompanhados de mensagens bonitas que prometem mil maravilhas se o arquivo anexado for aberto. Não se deixe enganar. A melhor política é nunca abrir um arquivo anexado, principalmente se o remetente for desconhecido.

Programas piratas, adquiridos pela rede, poderão conter Cavalos de Tróia, assim, evite a instalação de programas de procedência desconhecida ou duvidosa.

#### 2.2.2 O que um Cavalo de Tróia pode fazer em meu computador?

O Cavalo de Tróia, na maioria das vezes, vai possibilitar aos hackers o controle total da sua máquina. Ele poderá ver e copiar todos os seus arquivos, descobrir todas as senhas que você digitar, formatar seu disco rígido, ver a sua tela e até mesmo ouvir sua voz se o computador tiver um microfone instalado. Este processo é chamado de invasão.

#### 2.2.3 O hacker poderá me invadir se o computador não estiver conectado à Internet?

Não, o Cavalo de Tróia somente poderá ser utilizado se o computador estiver conectado à Internet. Os hackers somente invadem computadores quando eles estão conectados.

## 2.2.4 O computador pode ser infectado por um Cavalo de Tróia sem que se perceba?

Sim, com certeza. Essa é a idéia do Cavalo de Tróia, entrar em silêncio para que você não perceba e quando você descobrir ser tarde demais.

## 2.2.5 Como posso saber se o computador está infectado?

Os programas anti-vírus normalmente detectam os programas Cavalos de Tróia e tratam de eliminá-los como se fossem Vírus. As atualizações dos Anti-Vírus possibilitam a detecção dos Cavalos de Tróia mais recentes.

## 2.2.6 Como proteger o computador dos Cavalos de Tróia?

A maioria dos bons programas de anti-vírus são capazes de detectar e eliminar estes programas. Mesmo assim a proteção é parcial, uma vez que os Cavalos de Tróia mais novos poderão passar despercebidos. O ideal é nunca abrir documentos anexados aos e-mails.

Existem ainda programas de Firewall pessoal que podem ser utilizados para barrar as conexões dos hackers com os Cavalos de Tróia que possam estar instalados em seu computador. Tais programas não eliminam os Cavalos de Tróia, mas bloqueiam seu funcionamento.

## 2.3 Backdoors

Existe uma confusão entre o que é um Backdoor e um Cavalo de Tróia, principalmente porque o estrago provocado por ambos é semelhante. Para deixar claro, um Cavalo de Tróia é um programa que cria deliberadamente um Backdoor em seu computador.

Programas que usam a Internet e que são de uso corriqueiro, como Browsers, programas de e-mail, ICQ ou IRC podem possuir Backdoors.

Os Backdoors são abertos devido a defeitos de fabricação ou falhas no projeto dos programas, isto pode acontecer tanto acidentalmente ou ser introduzido ao programa propositalmente.

Como exemplo: versões antigas do ICQ possuem defeito que abre um Backdoor que permite ao hacker derrubar a conexão do programa com o servidor, fazendo que ele pare de funcionar.

### 2.3.1 Como se prevenir dos Backdoors?

A maneira mais correta é sempre atualizar as versões dos programas instalados em seu computador. É de responsabilidade do fabricante do software avisar aos usuários e prover uma nova versão corrigida do programa quando é descoberto um Backdoor no mesmo.

A dica é sempre visitar os sites dos fabricantes de software e verificar a existência de novas versões do software ou de pacotes que eliminem os Backdoors (esses pacotes de correção são conhecidos como patches ou service packs.).

Os programas Anti-Vírus não são capazes de descobrir Backdoors, somente a atualização dos programas é que podem eliminar em definitivo este problema. Programas de Firewall pessoal, no entanto, podem ser úteis para amenizar (mas não eliminar) este tipo de problema.

## 2.4 Vírus

Vírus de computador são programas capazes de se reproduzir. O ato de se reproduzir, no caso destes Vírus, é a capacidade do mesmo de se copiar de um computador a outro utilizando-se de diversos meios: através dos disquetes, embutindo-se em documentos de texto ou planilhas de cálculo e, atualmente, distribuindo-se por e-mail.

### 2.4.1 Como o computador é infectado por um Vírus?

Seu computador pode ser infectado de diversas maneiras:

- através de um disquete esquecido no drive A: quando o micro é ligado;
- executando um programa desconhecido que esteja em um disquete ou, até mesmo, em um CD-ROM;
- instalando programas de procedência duvidosa;
- abrindo arquivos do Word, Excel, etc.; e
- em grande parte dos casos, abrindo arquivos anexados aos e-mails.

É claro que novas maneiras do computador ser infectado por um Vírus podem ser criadas.

Neste caso é sempre bom manter-se informado através de jornais, revistas e dos sites dos fabricantes de Anti-Vírus.

### 2.4.2 O que os Vírus podem fazer no computador?

Infelizmente os Vírus podem fazer de tudo, desde mostrar uma mensagem de "feliz aniversário" até destruir irremediavelmente os programas e arquivos de seu computador. Praticamente o vírus passa a ter controle total sobre o computador.

### 2.4.3 O computador pode ser infectado por um Vírus sem que se perceba?

Sim, sempre. A idéia do Vírus é permanecer escondido (encubado) reproduzindo-se e infectando outros micros até um evento qualquer acordá-lo. Geralmente os Vírus entram em atividade em alguma data específica como na sexta-feira, dia 13.

#### **2.4.4 Como posso saber se o computador está infectado?**

Os sistemas operacionais dos computadores (como o Windows ou o MacOS) não detectam Vírus, assim sendo, a melhor maneira de descobrir se um computador está infectado é através dos programas Anti-Vírus.

#### **2.4.5 Existe alguma maneira de proteger o computador dos Vírus?**

Sim, instalando e mantendo atualizado um bom programa Anti-Vírus e evitando executar programas desconhecidos. Como medida de prevenção, veja a seção 3.4.1.

#### **Fui atacado! E agora?**

Toda vez que você se sentir lesado, seja por ataques, seja por e-mail não solicitado, entre em contato com seu provedor. Todos os bons provedores possuem uma equipe para cuidar da segurança de seus usuários e do próprio provedor.

Segundo normas da Internet (RFC2142), todos os provedores (domínios) devem possuir os seguintes endereços de e-mails:

- abuse@(seu provedor).com.br - usado para informar a respeito dos SPAMs ou e-mails de conteúdo abusivo ou ofensivo;
- noc@(seu provedor).com.br - utilizado para relatar problemas com a rede; e
- security@(seu provedor).com.br - utilizado para relatar problemas envolvendo segurança, como invasões, ataques, etc.

Todos os bons provedores costumam auxiliar o usuário quando este é atacado ou invadido por hackers.

