

# Dicas de segurança para pais de adolescentes

Independentemente de seus filhos serem novatos na Internet ou já terem bons conhecimentos da Web, você pode ajudar a orientá-los quanto ao uso da Internet à medida que eles crescem e passam por diferentes idades e estágios em suas vidas.

- **De 2 a 4 anos: começando**

Durante este estágio, a atividade online muito provavelmente envolverá os pais. Os pais podem segurar as crianças no colo enquanto vêem fotos de família, usam uma câmera da Web para entrar em contato com familiares ou visitam sites especiais para crianças.

- **De 5 a 6 anos: fazendo sozinhas**

Quando chegam aos 5 anos de idade, as crianças provavelmente desejarão explorar a Web sozinhas. É importante que os pais orientem-nas quanto a como surfar pela Internet com segurança, assim que elas começarem a usar a Internet sozinhas.

- **De 7 a 8 anos: o interesse aumenta**

Parte do comportamento normal das crianças nesta faixa etária é ver de quanto eles conseguem escapar impunes. Enquanto estiver online, uma criança desta idade poderá entrar em sites ou conversar em salas de bate-papo não autorizadas por seus pais.

- **De 9 a 12 anos: boas habilidades online**

Pré-adolescentes querem saber tudo e já ouviram falar do que está disponível na Web. É normal que eles tentem ver o que há online e busquem assuntos que os pais consideram censuráveis (por exemplo, conteúdo adulto sexualmente explícito ou instruções sobre como construir uma bomba).

## **De 13 a 17 anos: tecnicamente sofisticados**

Ajudar os adolescentes com a segurança online é uma tarefa delicada, visto que eles geralmente sabem mais que seus pais sobre software da Internet. Mesmo com crianças mais velhas, é importante que os pais assumam um papel ativo na orientação do uso da Internet. Um cumprimento rigoroso de regras de segurança online com que os pais e as crianças concordaram e a freqüente revisão dos relatórios de atividade online das crianças é especialmente importante. Os pais devem se lembrar de manter suas próprias senhas seguras para que os adolescentes não possam se registrar em nome dos pais.

# O que os adolescentes fazem online

Os adolescentes baixam música, usam mensagens instantâneas, email e jogos on line. Eles também usam mecanismos de pesquisa para encontrar informações na Internet. A maioria dos adolescentes já visitou salas de bate-papo e muitos já participaram de bate-papos adultos ou privados. Os **meninos** nesta idade gostam de ultrapassar os limites e procuram por sites de humor grosseiro, imagens violentas e chocantes, jogos de azar ou de conteúdo adulto explícito. As **garotas** tendem mais a bater papo online e, portanto, são mais suscetíveis ao aliciamento sexual online.

- Crie uma lista com regras da casa para o uso da Internet com seus filhos adolescentes. Você deve incluir os tipos de sites que estão fora dos limites, o número de horas que podem passar na Internet e orientações sobre comunicação online, incluindo comunicação em salas de bate-papo.
- Mantenha os computadores conectados à Internet em áreas comuns da casa, não nos quartos dos adolescentes.
- Converse com seus filhos sobre seus amigos virtuais e suas atividades online, da mesma forma que conversa sobre suas outras atividades.
- Converse com seus filhos sobre a sua lista de contatos em programas de mensagens instantâneas e instrua-os a não falar com estranhos.
- Pesquise sobre ferramentas de filtragem da Internet (como o Controle de Menores do MSN Premium, em inglês), que devem ser usadas como um complemento à supervisão paterna, não uma substituição.

- Saiba quais são as salas de bate-papo ou grupos de discussão que seus filhos estão visitando e com quem estão conversando online. Incentive-os a usar salas de bate-papo monitoradas e insista para que permaneçam em áreas de bate-papo públicas.
- Insista para que nunca concordem em encontrar pessoalmente um amigo virtual.
- Ensine-os a nunca fornecer informações pessoais sem a sua permissão ao usar email, salas de bate-papo ou mensagens instantâneas, preencher formulários de registro e perfis pessoais ou participar de competições online.
- Ensine-os a não baixar programas, músicas ou arquivos sem a sua permissão. Explique que se compartilharem arquivos ou copiarem textos, imagens e trabalhos artísticos da Web, eles podem estar violando leis de direitos autorais e que isso pode ser ilegal.

- Incentive-os a contar se algo ou alguém online fizer que se sintam desconfortáveis ou ameaçados. Mantenha a calma e lembre-os de que não estão fazendo nada de errado se quiserem lhe mostrar algo. (É importante deixar claro que eles não irão perder o direito de usar o computador.) Leia mais sobre como lidar com predadores online e intimidadores virtuais.
- Converse com seus filhos sobre conteúdo adulto e pornografia online e oriente-os a sites positivos sobre saúde e sexualidade.
- Ajude a protegê-los contra spam. Instrua-os a não fornecer seu endereço de email online, não responder a mensagens de lixo eletrônico e a usar filtros de email.
- Esteja atento aos sites da Web que seus filhos freqüentam. Verifique se não estão visitando sites com conteúdo ofensivo ou publicando informações pessoais ou fotos de si mesmos online.

- Ensine-os a ter um comportamento responsável e ético online. Eles não devem usar a Internet para espalhar fofocas, intimidações ou ameaças aos outros.
- Deixe claro que devem sempre consultar você antes de realizar qualquer transação financeira online, inclusive encomendar, comprar ou vender itens online.
- Converse com eles sobre os jogos de azar online e seus riscos potenciais. Lembre-os de que os jogos de azar online são ilegais para eles.

## • Quando em computadores públicos (lan-houses)

- **Não salve suas informações de logon.**

Sempre faça logout dos sites clicando em "log out" no site. Não basta apenas fechar a janela do navegador ou digitar outro endereço. Muitos programas (especialmente os de mensagens instantâneas) incluem um recurso de logon automático que salvam seu nome de usuário e senha. Desative essa opção para que ninguém possa fazer logon em seu nome.

- **Não deixe o computador desacompanhado com informações confidenciais na tela.**
- Se precisar deixar o computador público, faça o logout de todos os programas e feche todas as janelas que possam exibir informações confidenciais.

- **Apague seus rastros.**
- Os navegadores da Web, como o Internet Explorer, mantêm um registro de sua senha e de cada página que visita, mesmo que feche os programas e faça logout. Aprenda a usar essas opções de preenchimento automático de senhas e Exclusão de Arquivos e Históricos do navegador que você utiliza.

- **Tome cuidado com os bisbilhoteiros.**
- Quando usar um computador público, tome cuidado com ladrões que tentam espiar por cima do seu ombro enquanto você digita informações confidenciais, como uma senha.

- **Não digite informações confidenciais em um computador público.**
- Essas medidas oferecem certa proteção contra hackers casuais que usam um computador público depois de você. Mas saiba que um ladrão habilidoso pode instalar um software sofisticado no computador público que registre cada tecla digitada e envie as informações por email ao ladrão. Nesse caso, não importa se você não salvou as informações ou apagou os rastros. Essas informações não estarão seguras. Se você deseja realmente estar em segurança, evite digitar o número do seu cartão de crédito ou qualquer outra informação financeira ou confidencial em qualquer computador público.

# Vírus, worms e cavalos de Tróia

são programas mal-intencionados que podem causar danos ao seu computador e às informações armazenadas nele. Também podem deixar a Internet mais lenta e usar o seu computador para espalhar-se entre os seus amigos, familiares, colegas de trabalho e o restante da Web. A boa notícia é que, com prevenção e algum bom senso, você terá menos probabilidade de ser vítima dessas ameaças.

# Que é um vírus?

Um vírus é um código de computador que se anexa a um programa ou arquivo para poder se espalhar entre os computadores, infectando-os à medida que se desloca. Ele infecta enquanto se desloca. Os vírus podem danificar seu software, hardware e arquivos.

# Que é um worm?

Um worm, assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente. Primeiro, ele controla recursos no computador que permitem o transporte de arquivos ou informações. Depois que o worm contamina o sistema, ele se desloca sozinho. O grande perigo dos worms é a sua capacidade de se replicar em grande volume. Um worm pode enviar cópias de si mesmo a todas as pessoas que constam no seu catálogo de endereços de email, e os computadores dessas pessoas passam a fazer o mesmo, causando um efeito dominó de alto tráfego de rede que pode tornar mais lentas as redes corporativas e a Internet como um todo.

# Que é um cavalo de Tróia?

Assim como o mitológico cavalo de Tróia parecia ser um presente, mas na verdade escondia soldados gregos em seu interior que tomaram a cidade de Tróia, os cavalo de Tróia da atualidade são programas de computador que parecem ser úteis, mas na verdade comprometem a sua segurança e causam muitos danos. Um cavalo de Tróia recente apresentava-se como um email com anexos de supostas atualizações de segurança da Microsoft, mas na verdade era um vírus que tentava desativar programas antivírus e firewalls.

# Termos e Ferramentas de segurança

# O que é um firewall?

Um firewall (ou firewall da Internet) ajuda a tornar seu computador invisível para invasores online e alguns programas mal-intencionados, como vírus, worms e cavalos de Tróia. Um firewall também pode ajudar a impedir que software de seu computador acesse a Internet e aceite atualizações e modificações sem sua permissão. Firewalls são fornecidos em forma de software e hardware, mas firewalls de hardware destinam-se a uso com um firewall de software.

# O que é um Proxy?

- Um **Proxy** é um software que armazena dados em forma de cachê (arquivos que ficam armazenados localmente e não precisam ser acessados de novo remotamente). São instalados em máquinas servidoras com ligações tipicamente superiores às dos clientes e com poder de armazenamento elevado. Sua função inicial é fornecer um método de otimizar o uso do link de internet.

Por exemplo, no caso de um site na internet, o cliente requisita acesso a uma página, imagem ou um documento na Web e o proxy procura pelo documento em seu cachê. Se encontrado, o documento é retornado imediatamente. Senão, o proxy busca o documento no servidor remoto, entrega-o ao cliente e salva uma cópia no seu cachê.

- É de salientar que, utilizando um proxy, o endereço que fica registrado nos servidores é o do próprio proxy e não o do usuário cliente, por isso atualmente também servem para prover acesso anônimo a sites e serviços internet.
- A tradução da palavra inglesa *proxy*, segundo o dicionário *Michaelis*, significa *procurador, substituto ou representante*.

# Que é um Spam?

- É o termo pelo qual é comumente conhecido o envio, a uma grande quantidade de pessoas de uma vez, de mensagens eletrônicas, geralmente com cunho publicitário, mas não exclusivamente.
- O spam também é conhecido pela sigla inglesa UCE (Unsolicited Commercial Email, ou **Mensagem Comercial Não-Solicitada**).
- O termo derivou para designativo de qualquer comunicação eletrônica indesejada.

# Que é um software antivírus?

Software antivírus ajuda a proteger seu computador contra vírus específicos e software mal-intencionado, como worms e cavalos de Tróia. O software antivírus deve ser atualizado. Essas atualizações em geral estão disponíveis por meio de uma assinatura junto a um fornecedor de software antivírus.

# Preciso ter um firewall e um software antivírus?

Sim. Um firewall ajuda a impedir que hackers e vírus atinjam seu computador, e o software antivírus ajuda a se livrar de vírus conhecidos se eles conseguirem ultrapassar o firewall ou se já tiverem infectado o computador. Uma forma comum de vírus ultrapassarem um firewall é você ignorar mensagens de aviso ao baixar software da Internet ou por email.

# Que é um software anti-spyware?

O software anti-spyware ajuda a detectar e remover spyware de seu computador. "Spyware" (também chamado de "adware") normalmente refere-se a software destinado a monitorar as atividades de seu computador. Spyware pode exibir pop-ups de propaganda indesejados, coletar informações pessoais sobre você ou alterar a configuração de seu computador com as especificações do criador do spyware. No pior cenário, o spyware pode permitir que criminosos desativem seu computador e roubem sua identidade.

# Que são controles de restrição para menores?

Controles de restrição para menores ajudam a proteger seus filhos de conteúdo inadequado, tanto na Internet como em videogames de computador. Você pode escolher níveis separados de segurança para cada criança da família, dependendo de sua idade e maturidade. Alguns sistemas de videogame incluem controles de restrição para menores também os quais ajudam a restringir a capacidade de seus filhos de acessarem jogos ou filmes de DVD inadequados.

Fonte: <http://www.microsoft.com/brasil/athome/security/default.aspx>