

# Dicas de Segurança

## SPAM – Como diminuir o impacto dos spams, spywares e vírus na sua vida.

Siga as dicas abaixo e diminua o impacto dos spams, spywares e vírus em sua rotina:

Dicas Anti-Spam	Explicação
<b>Use endereços de e-mail pouco usuais</b>	Alguns <i>spammers</i> usam programas de computador para “adivinhar” endereços de e-mail. Utilizar e-mails pouco usuais, contendo números e letras, pode driblar essa tática.
<b>Não dê o seu endereço de e-mail através de Instant Messaging</b>	Não divulgue o seu endereço de e-mail em chats, serviços de mensagens instantâneas ou grupos de e-mail. <i>Spammers</i> usam programas específicos para bisbilhotar a net a procura de endereços de emails.
<b>Ao invés de criar um e-mail para contato, crie um formulário</b>	Se você deseja criar um canal para que os usuários do seu site contactem você, crie um formulário do tipo “Fale Conosco”. Assegure-se de que o código “send to” não está na página HTML, mas somente no script do formulário.
<b>Nunca responda a um spam</b>	Nunca responda a mensagens de spam mesmo quando elas oferecem a possibilidade de remoção de seu mailing list. Geralmente, as instruções para remoção são falsas ou então uma maneira de coletar mais e-mails. O ato de responder confirma para o Spammer que o seu e-mail está ativo, abrindo caminho para o recebimento de mais e mais spams.
<b>Use endereços de e-mail falsos</b>	A maioria dos formulários que encontramos na web exige o seu e-mail para realizar login. Se você não quiser receber novidades sobre os sites em questão (e não necessitar de e-mail de confirmação de cadastro ou suporte técnico), não dê o seu endereço de e-mail verdadeiro. Se a confirmação é mandada para um email válido, crie um outro só para estes casos.
<b>Opt out</b>	Ao se cadastrar em sites para realizar compras online ou coisas do gênero, lembre-se de desmarcar a opção “quero receber novidades” caso esse seja realmente o seu desejo.
<b>Nunca envie informações pessoais para sites não seguros</b>	Nunca envie detalhes sobre o seu cartão de crédito ou outras informações de cunho pessoal para Web sites não seguros. Web sites seguros sempre apresentarão o ícone de um “cadeado trancado” em cor amarela no topo do seu browser. Outra maneira de verificar se o site é seguro é observar se antes do nome do site, em vez do tradicional endereço: <a href="http://www.nomedosite.com.br">http://www.nomedosite.com.br</a> , aparecer <a href="https://www.nomedosite.com.br">https://www.nomedosite.com.br</a> uma vez que o https significa que voce está conectado a um site seguro e todas as informações trocadas estão devidamente criptografadas.
<b>Use o Barracuda Spam Firewall</b>	Mesmo seguindo todas as orientações acima, você ainda receberá spam. Fale com a <a href="#">CLM</a> para conhecer a revenda mais próxima e instale um <a href="#">Barracuda Spam Firewall DEMO</a> por duas semanas totalmente grátis; o nível de spams em sua empresa será reduzido brutalmente. Experimente ainda hoje e proteja os e-mails da sua organização.

Dicas Anti-Vírus	Explicação
<b>Mantenha o seu sistema atualizado</b>	Mantenha o seu sistema atualizado – incluindo pacotes de antivírus e anti-spywares. Novos spywares vêm a tona diariamente. Sistemas desprotegidos e desatualizados estão praticamente pedindo para serem infectados. Existem muitos Anti-Spywares grátis na Internet, inclusive no site da Microsoft ( <a href="http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&amp;displaylang=pt-br">www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&amp;displaylang=pt-br</a> ). Copie e coloque o link inteiro no seu browser.
<b>Não clique em links em janelas de pop up</b>	Janelas de pop up geralmente são ativadores de spywares. Clicar em algum link localizado em uma pop up pode instalar um software spyware em seu computador. Feche a janela no botão “X” do browse em cima à direita e nunca em links como “fechar” ou “close”, caso existam.
<b>Não faça download de arquivos de origem desconhecida</b>	Não faça downloads de arquivos vindos de origem desconhecida mesmo se o assunto ou nome soar familiar. Basta um único download para que um vírus ou spyware se propaguem na sua máquina e em outras que entraram em contato.
<b>Fique atento ao realizar downloads de arquivos na Internet</b>	Assegure-se de que a origem é legítima e possui boa reputação. Se você não estiver tão certo da procedência, não faça o download ou então o faça em um disquete e teste com o seu software anti-vírus e anti-spyware.
<b>Configure o seu Barracuda Web Filter para fazer atualizações automáticas</b>	Mais de 90% dos computadores conectados a Internet estão infectados com spywares. A <a href="#">Barracuda Networks</a> atualiza o <a href="#">Barracuda Web Filter</a> automaticamente com as regras e definições de spyware mais atuais hora a hora, garantindo uma proteção robusta.
<b>Seja cético em relação a downloads gratuitos</b>	Muitos sites que oferecem toolbars customizadas ou outros benefícios são chamarizes. Não faça download de programas a partir de sites em que você não confia ou não conhece. Você pode expor o seu computador a ataques de spyware desta maneira.
<b>Não acredite em links oferecendo softwares anti-spyware</b>	Tome cuidado! Na verdade, estes links podem instalar um spyware.
<b>Não faça downloads de códigos do browser</b>	Muitos programas contendo spywares lançam uma caixa de diálogo com aparência oficial perguntando se você deseja fazer o download de um plugin para o seu browser. Esses pop ups podem parecer oficiais, mas na verdade são spywares aguardando para instalar um turbilhão de pop ups, toolbars indesejadas ou qualquer outro tipo de conteúdo não desejado. Certificados não irão proteger sua máquina contra adwares e outros aborrecimentos trazidos por estes ActiveX controls.

Dicas Anti-Vírus	Explicação
<b>Não abrir anexos de remetentes desconhecidos</b>	Não abra nenhum arquivo anexado a um e-mail de remetente desconhecido e/ou assunto suspeito.
<b>Não abrir arquivos ou anexos desconhecidos</b>	Alguns vírus podem se auto-replicar e espalhar-se através do e-mail. Mesmo que conheça o remetente, é melhor prevenir do que remediar e confirmar de que a pessoa realmente o enviou.
<b>Não fazer o download de arquivos desconhecidos</b>	Não faça o download de arquivos de desconhecidos mesmo que a linha de assunto sugira que te conhecem. Basta o download de apenas um arquivo para propagar o vírus.
<b>Fazer sempre a verificação de vírus em disquetes e CDs.</b>	Faça sempre a verificação de vírus em disquetes ou CDs que tenham sido obtidos de fontes não confiáveis. Caso empreste um disquete, verifique-o quando for devolvido.
<b>Cuidado ao realizar downloads de arquivos da Internet</b>	Assegure-se de que a fonte seja verdadeira e respeitável. Certifique-se de que um programa antivírus faça a verificação dos arquivos do site de download. Caso não tenha certeza, não faça o download do arquivo ou faça-o para um disquete e teste-o com o seu próprio software antivírus.
<b>Configurar seu Barracuda Spam Firewall para atualizações automáticas</b>	Mais de 500 vírus são descobertos a cada mês. Portanto, é melhor estar protegido. A Barracuda Networks atualiza automaticamente a cada hora o seu Spam Firewall com as últimas definições de vírus.
<b>Fazer backup dos seus arquivos regularmente</b>	Certifique-se de fazer regularmente um backup dos seus dados importantes e de que os procedimentos para recuperá-los funcionem corretamente. Deste modo, se for infectado por um vírus, será possível recuperar os seus dados mais importantes. Guarde sua cópia de backup num local separado dos seus arquivos de trabalho, de preferência, fora do seu computador.
<b>Anti Virus Grátis</b>	Se a sua empresa está protegida por qualquer um dos produtos <a href="#">Barracuda</a> as estações estarão protegidas automaticamente. Em casa, baixe qualquer antivírus que tenha uma edição gratis. Consulte a página de Antivirus Free em <a href="http://www.download.com/Antivirus/3150-2239-0.html">http://www.download.com/Antivirus/3150-2239-0.html</a>