



Best Practices to Secure Your Computers and Network

When it comes to computers and the Internet there is no single

product or process that can provide all the necessary elements to ensure complete protection. A secure computer and network needs a **(1)** good password policy, **(2)** hardware firewall, **(3)** current antivirus, **(4)** current operating system and network operating system patches, **(5)** current antispyware, **(6)** current antispam email filter, and **(7)** a current popup blocker. Notice the frequent use of the word "current?" This single item is the most important aspect of any security strategy. New risks arise every day and without the "current" protection your systems are at risk.

Top Seven (7) Recommendations—Checklist

(1) Password Policy

The first and easiest step is the use of a good password. Never leave a password blank or the manufacturer's default. A good password is one that mixes numbers, characters, and letters such as 100%off!, \$300house?, or ^CarrotIsOn1. Use something easy to remember and significant to you.

Update frequency: Monthly

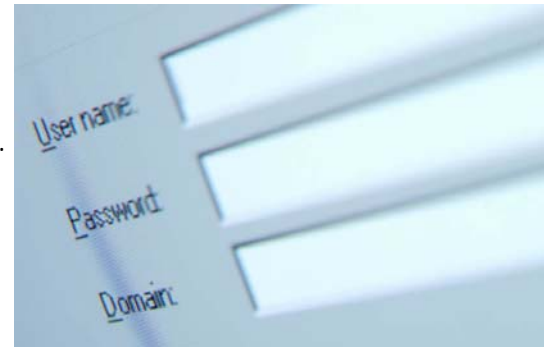
(2) Hardware Firewall

The single best way of securing your computer(s) and network from outside intrusion. A hardware firewall's primary purpose is to prevent unauthorized access. Software and inexpensive firewalls cannot block even the least experienced hacker. Tools are readily available on the Internet to bypass inadequate firewalls in seconds. Contact us for the latest prices on affordable hardware firewall solutions. *Update frequency: Monthly*

(3) Antivirus

Running on personal computers and network servers, antivirus solutions guard against the accidental infection from virus, trojans, and worms. Infections come from casual Internet browsing, email, and infected software installations. Two popular antivirus providers are McAfee (www.mcafee.com) and Symantec (www.symantec.com). *Update frequency: Daily*

(Continued on page 2)





Best Practices to Secure Your Computers and Network

(Continued from page 1)

(4) Operating System Patch

Microsoft provides Internet websites that can automatically update your computer(s). "Critical" updates are necessary to protect against known security vulnerabilities. (Microsoft Operating Systems: windowsupdate.microsoft.com) (Microsoft Office Products: office.microsoft.com/OfficeUpdate) *Update frequency: Weekly*

(5) Antispyware

Also known as *adware*, spyware is software that covertly gathers information from a computer including browsing habits, email addresses, and even passwords and credit card numbers. The information is then transmitted in the background to someone else. Typically used for targeted advertising, there are instances where identity theft has been linked to spyware. A free downloadable antispyware program called Ad-Aware is available at www.adaware.com. *Update frequency: Weekly*

(6) Antispam

Filling up our email boxes with volumes of unwanted messages, ads, virus, trojans, and worms, SPAM has the honor of being the highest productivity killer associated with the Internet. Get rid of it! One way is to run Postal Inspector available at www.giantcompany.com. *Update frequency: Weekly*

(7) Popup Blocker

As annoying as they are, popups add the additional risk of infecting your computer with unwanted software. If prompted to install, click Ok, or click "Yes" on a popup dialog box, make sure you know what you are getting. Try running a free software called AdBolish available at www.adbolish.com. *Update frequency: Weekly*

It is important to protect your valuable data and information. Do not risk any downtime or legal liability. Get started right away! Please contact us if you would like additional information. (586) 630-1979 or online at www.ISSentry.com.

Copyright 2004, I.S. Sentry, Inc.

