Tips for Keeping Your Computer Safe

Learn About Window XP's Built-In Security Features:

If you are using Windows XP, use the built in firewall to protect all dial-up, wired, or wireless network you may have. Also regularly check for System Updates from Microsoft or enable Automatic Updates.

Free Anti-Virus & Firewall Software:

Always keep an up-to-date virus checker installed on your machine. Although there are several such programs for sale, there are good ones that are absolutely free for individual home use. One is the AVG Anti-Virus program. To get a copy, go to free.grisoft.com. Another possibility is avast! Home Edition from www.avast.com.

Although Windows XP comes with a built-in firewall, it is fairly minimal and experts recommend you install another for added security. ZoneLabs provides an easy-to-use firewall that is free for individual home users. Go to www.zonelabs.com to get it (the free edition is well hidden, you may have to hunt around to find it!)

For the more advanced user, Sygate provides a free firewall that provides more advanced control over the security rules. Go to www.sygate.com to download your copy.

Getting Rid Of Spyware and Adware:

Spyware and adware are the leading cause of computer slowdowns and the major reason people seek service for their PCs. To get rid of these pests yourself, get SpyBot Search & Destroy from www.safer-networking.org (not .com). It will scan your PC for spybots and adware and will allow you to remove these villains from your PC for free. Another popular ad-ware remover is AdAware from LavaSoft. Download it from www.lavasoftusa.com.

Learn About Hoax Chain E-Mails and Avoid Passing Them Along:

If you are forwarded an e-mail that asks you to pass it on to all your friends, it most likely is a hoax. Unless it is funny or inspirational, chances are that if you pass it on you will just wasting everyone's time with untrue or false information. Before passing on such types of e-mails, look for it on www.snopes.com. Use the oddly named "Inboxer Rebellion" section to learn about the truth or falsity of many e-mails that may come your way.

Snopes is also a fun site for browsing in your free time. In addition to learning about scams and hoaxes that are on the loose, you will find the stories and truth behind many strange and fascinating urban legends!

Beware of E-Mail Bearing Gifts:

In the old days, people infected their computers with viruses by moving floppy disks from computer to computer. Now a days most viruses are transmitted through e-mail attachments. Avoiding contamination is usually a matter of being skeptical of all attachments you receive. A good rule of

"...and for $200 more you can get our Internet model, which is configured for viewing smileys!"

thumb is not to open any attachment unless you are expecting it, even if it is from someone you know. Many viruses will send you e-mails that appear to come from people you know and will include a friendly note urging you to take a look at the attachment. Be careful!

Avoid Common E-Mail Scams:

Your Internet service provider, financial institution, or online merchant will never send you an e-mail message asking you to verify your social security number, account numbers, or passwords. Many e-mails like these are sent out by identity thieves trying to steal information from people. Never assume e-mail messages asking for such things are legitimate, no matter how official they look. When in doubt, call the institution by phone (never use a phone number or contact information provided in the e-mail) and ask to speak with customer service representative.

Get More Ham and Less Spam In Your E-Mail Box:

It is impossible to hide from spam completely, but a few easy tips can help to keep the problem under control:

✔ Use a private e-mail address for friends and family, while using another e-mail address for filling out online registrations, posting to public forums, or subscribing to mailing lists and newsletters. Free web-based e-mail services like hotmail or yahoo are great for creating disposable e-mail addresses for these purposes.

✔ Many mail programs (and most web-mail services) offer you the option to block pictures and graphics in an e-mail message until you specifically ask for those to be shown. Enable this feature and only unblock pictures on e-mail messages from people you trust. Never view pictures or graphics in a piece of spam since doing so may allow the spammer to track whether you have read the message or not!

✔ If you receive spam, never click the "opt-out" link in those e-mails. By doing so you confirm that you read the e-mail making your address more valuable to an unscrupulous spammer.

Be Safe By Being Unique:

Just as with human viruses, a computer virus is more effective if it can infect the most computers in the least amount of time. This means that most viruses target computers and software that are used by the greatest number of people in the world. This is why Microsoft products are so often vulnerable to new viruses and other cybernetic maladies.

You can use this knowledge to your advantage by using alternatives to the software that most people use. The following table shows you some good alternative to popular software.

Software	Possible Alternatives
Internet Explorer	Firefox: www.mozilla.org Opera: www.opera.com
Outlook Express	Thunderbird: www.mozilla.org Pegasus: www.pmail.com Eudora: www.eudora.com
Microsoft Office	OpenOffice: www.openoffice.org

About The Author:

Marcio obtained his degree at CSU and is a certified PC technician. He enjoys helping people with their computers and teaching technology classes. For information on training at your organization, call 970-215-7140 or e-mail marciot@yahoo.com.