Safe Computing Basics

The following are thoughts and strategies on how to keep your computer free from viruses, Trojan Horses, Spyware, etc.

Quick start. If you'd rather not read a bunch of techno-mumbo jumbo, just make sure you have the following bases covered:

- Anti Virus Software – Download and install AVG Free Edition (http://www.grisoft.com/doc/1)
- Personal Firewall Software – Download and install ZoneAlarm (the free version) (http://www.zonelabs.com/store/content/home.jsp)
- Spyware Software – Download and install Ad-aware (the free version) (http://www.lavasoftusa.com/software/adaware/)

The bottom line is that you want to be running Anti Virus (AV), Personal Firewall and Spyware software. The AV and Firewall software run continuously and should automatically check for updates. You should run the Spyware software somewhere between weekly and monthly, checking for updates each time you do.

Getting a bit more advanced, we need to think about what we'd do if we did get a serious problem.

- **Anti Virus Rescue Disks.** If you are already running virus protection, make sure you update the virus definitions and then find the routine to make the Anti-Virus Emergency Recovery disks. Most AV (Anti Virus) software has this feature and most of us probably skipped that step too. Test to make sure that your PC is able to boot from your rescue disk.
- **Backing up your computer.** OK, we are getting more advanced now, but please bear with me. You can back up just your critical files, or your entire hard drive. It just depends on the amount of risk you want to take.
    - Critical Files Only – make a copy of you Outlook data files (outlook.pst and outlook.ost) and your Word Documents and spreadsheets. If you save everything in just a few directories, then you'll just need to copy those entire directories. If you've been less organized, you might consider how you can reorganize where you store your stuff to facilitate copying things quickly and easily. This is important because after I'm through scarring you, you'll be doing this at least every two weeks. The Outlook files are best found by doing a search on outlook.pst from Windows Explorer or My Computer. These files get HUGE. If you don't go in periodically

and clean out your send and deleted folders, you should get in this habit.

I can hear you about now wondering where to copy the files to. If you have 2 computers on a home network, you can copy the files from the laptop to the desktop. You could do the same thing with a USB Memory stick, but you'll need a big one, 512 Mb to 4 Gb because your Outlook file alone is probably 300 – 400 Mb. Of course you can always burn a CD. Whatever method you choose, you need to verify that the files transferred correctly. Some times good old Windows will copy a shortcut for you instead of the file. When you need to use the backup is a bad time to find out that it didn't work.

- Complete System Backup. – This is what the Pros do. It involves some software (Norton's Ghost program, about $70.00, is the most popular) and either a DVD-R drive or a networked computer with a secondary hard drive that is at-least as big as the one in the machine that you are backing up. The theory is very simple; the Ghost program let you make an exact copy or "image" of your entire hard drive, even while Windows is running. If your hard drive goes out or Window gets totally corrupted, it is a simple process to copy that image back to your hard drive.

- Selective Backup. The program Ezback-it-up is a free program you can download and use to backup selected file and folders to another drive or computer. A great solution if you don't want to hassle with the time it takes to do a complete back up. http://www.rdcomp.net/download.php

Why spend so much time on backups? Just try to imagine what you would do it your computer smoked – literally. Or got stolen. All the information that you need on a daily basis is either totally gone or, at best, temporarily unavailable. I don't know about you, but this is a crisis I'd prefer to avoid.

It is no accident that I covered system back-ups early on in this discussion. **It is important that you recognize that any time you add software or update Windows; you could loose your operating system.** Granted, this doesn't happen often, but it can. The last thing I want to have happen is for you to do something I've told you to do and have Windows crash so bad that you have to wipe your hard drive clean and reinstall from scratch. So be forewarned to read on only after you've done some backing up!

Windows Update. Now that you are backed up, if you haven't been running windows update, now would be a good time to start. I recommend installing all critical updates EXCEPT SP2. If you install SP2 you are on your own!

Firewalls. I'm assuming that you are all on some type of High Speed Internet, usually either Cable Modem or DSL. The one best thing that you can do to protect your system from the outside world is to install a Router. A Router is a little box that goes between the cable or DSL modem and your computer. Most Routers are also "Switches" that allow you to take the 1 internet connection that comes out of the modem and gives you 4, 8 or 16 ports that you can hook additional computers to. Because most all routers also act as firewalls, it will say this on the box, once your PC is behind a router, you are invisible to the world. If you have a laptop, you'll want to consider a wireless router. We'll talk more later about special considerations for wireless systems.

Anti Virus Software. If your are not using, and keeping current, AV software, you had better start. The programs that are the most popular are Norton, McAfee, and AVG. I'm sure there are others, but those are the one that come up over and over again. I'm a big fan of AVG (http://www.grisoft.com) Their free version is so full of features, I don't know why you'd pay for their "Pro" version. What I like about it is that it automatically goes and looks for updates every day. Hopefully you have picked up how important that it is that you keep the software up-to-date. Just running the AV software is not enough protection.

After you install your AV software, you really need to find the page where you set the options. This may be painful, but YOU have to decide what file types get scanned and which do not. It is better than it used to be, but you can't assume that the default settings are what you want. Fear not, usually the help screens help you make the right decisions.

I should also forewarn you that ZoneAlarm will also initially annoy the heck out of you with Alert Windows. If you click on the "remember this" click box, you won't see that one any more. Believe me, the safety is worth the minor annoyance.

Wireless Networking

There are a couple of reasonably simple things that you can do to dramatically improve the security of your wireless network. If you are a wireless network at home, I strongly encourage these things.

- On your wireless router, change the Network Name and the administrator password from the default vales to something of your own choosing. Failure to do this could allow someone to log into your router, change the settings, and prevent you from using your own network. The paperwork that came with your router will explain how to do this.
- Enable encryption. Somewhere in your router settings, you will have the option to enable encryption. Usually you choices are WEP or WPA. You may have to look at the settings for your wireless card and choose the one that is common to both. Any encryption is better than none. Your router will likely offer default "KEYS" A key is kind of like a password; the key on

your wireless PC must match the key in your router. It is a good idea to change the key from the default key to one you make up.

For your reference, I've attached a bunch of links that may or may not ever come in handy.

Resources

Virus Resources
F-PROT: http://www.f-prot.com/virusinfo/
McAfee : http://vil.nai.com/vil/default.asp
Symantec Norton: http://www.symantec.com/avcenter/
Trend Micro: http://www.trendmicro.com/vinfo/
NIST GOV: http://csrc.nist.gov/virus/

Free software
AVG Anti-Virus - http://free.grisoft.com Free
F-Prot - http://www.f-prot.com Free for home users

Free online Virus scan
BitDefender - http://www.bitdefender.com/scan
HouseCall - http://housecall.trendmicro.com
McAffe - http://us.mcafee.com/root/mfs
Panda ActiveScan - http://www.pandasoftware.es/activescan/activescan-com.asp
RAV Antivirus - http://www.ravantivirus.com/scan

Free online Trojan scan
TrojanScan - http://www.windowsecurity.com/trojanscan/

Free online Security scan
Symantec Security Check - http://security.symantec.com/sscv6
Test my Firewall - http://www.testmyfirewall.com/

More Security Resources
Forum of Incident Response and Security Teams: http://www.first.org/
Microsoft: http://www.microsoft.com/technet/security/current.aspx
SANS Institute: http://www.sans.org/resources/
Webopedia: http://www.pcwebopedia.com/