



### Safe Computing

Due to an increase in the amount of threats on the internet, it is important for users to follow safe computing practices to provide the best protection against viruses, spyware, and hackers. These are tips we believe, that if followed, can help you to protect you and your computer's security.

▶ WHAT TO DO!

*Install Anti-virus and keep virus definitions up-to-date*

- Ask Z64IT Tech for free Virus Scanning software.
- Run LiveUpdate weekly
- Run Full system scans weekly

*Keep your operating system (i.e. Windows) up-to-date with latest security patches and downloads*

- Run Windows Update weekly ([www.windowsupdate.com](http://www.windowsupdate.com)) or/
- Turn on Automatic Updates.
- Update your MS Office Software. Use

*Set an Administrator password on your computer*

- Set complex passwords for all user accounts
- Never leave Administrator account with a blank Password.

*Don't use file sharing programs*

- Ex. Kazaa, iMesh, Grokster, Xolox, Morphheus, Bearshare, Limewire, Torrents etc.

Viruses are malicious programs that run on your computer. They take control by being:

- Destructive: compromising files and allowing outsiders access to your files; viruses can also grab e-mail addresses from a contacts list and send itself to those addresses.
- Non-destructive: consume computer resources and annoying error messages

Hackers like to find and exploit bugs and loopholes in software products. By having an up-to-date operating system, the likelihood of being exploited is decreased.

- Updates are periodically released when vulnerabilities have been discovered

Administrative passwords protect your vulnerability to viruses and hackers. They can try to login as Administrator with a blank password. If you don't have an Administrator password, boom they are in.

File sharing allows for the easy transfer of viruses and spyware from computer to computer sharing the network because it gives computer access to others sharing the server with you . Spyware can be packaged into a song you download

▶ WHY ?

## Safe Computing Cont.

▶ WHAT TO DO!

### Turn on a Firewall

- The built in firewall in Win XP can be turned on in the Control Panel
- Firewall products can also be purchased or downloaded for free (i.e. Norton Firewall, ZoneAlarm, Sygate etc.)

### Run removal tools for Spyware

- Run Spyware scans/repairs weekly
- We recommend downloading SpyBot Search & Destroy, along with Lavasoft Ad-Aware
- Stay away from programs like Gator, WebShots, Bonzi, Hotbar, Comet Cursor, etc .

### Do NOT open email attachments or executables from unknown senders

- Delete unknown emails immediately from your inbox.
- Check this website for hoaxes:
- Even if you know the sender, be careful what you download.
- If you are going to open an attachment or executable, please take these safety measures:
  1. SAVE the file in a folder, such as "attachments"
  2. Scan the folder using an updated Anti-virus software
  3. If the scan comes checks clean, then you can open the attachment

Connecting to the Internet can expose critical or confidential data to malicious attackers from anywhere in the world. Firewalls are like building a moat around your castle. Intruders will have to first break through the firewall to try to exploit your vulnerabilities.

- Win XP has a built in firewall.

Spyware is harmful to you and your computer because it can:

- Make your computer slow/crash
- Slow down your Internet connection
- Monitor your computer activity: Can lead to identity fraud
- Obtain your personal information
- "Hijack" your computer to send out spam or viruses

Many viruses are transferred through email as attachments or web links. By opening, the door is open to infect your computer.

- Can be as good as: "Recently we have received an order... This order was made online at our official BestBuy website on 06/19/2006 Our Fraud Department has some suspicions regarding this order and we need you to visit a special Fraud Department page at our web store where you can confirm or decline this transaction by providing us with the correct information..."
- Or someone asking you to click on a link that claims to have a picture of you, but only to send you to a hack link.

▶ WHY ?