Safe Computing Practices

1.) Keep your Windows updated!

- Go to Start > **Windows Update** or navigate to **http://windowsupdate.microsoft.com**, and install **ALL** Critical security updates listed (you will need to use Internet Explorer to do this). If you're running Windows XP, that includes Service Pack 3 (SP3)
  If you are running Vista, be sure to install **SP1**
- If you suspect your computer is infected with Malware of any type, please do **NOT** install any updates yet. Read the **Pre- HJT Post Instructions** and post a HijackThis log in our forums to get help cleaning your machine. Once you are sure you have a clean system, it is highly recommended to install SP2 (or SP1 for Vista) to help prevent against future infections.
- It's important always to keep current with the latest security fixes from Microsoft. This can patch many of the security holes through which attackers can infect your computer.
  Please either enable **Automatic Updates** under Start > Control Panel > Automatic Updates, or get into the habit of checking for Windows updates regularly.

2.) Watch what you download!

- Many "freeware" programs come with an enormous amount of bundled spyware that will slow down your system, spawn pop-up advertisements, or just plain crash your browser or even Windows itself.
- Peer-to-peer (P2P) note also that even if the P2P software you are using is "clean", a large percentage of the files served on the P2P network

are likely to be infected. Do not open any files without being certain of what they are!

3.) Avoid questionable web sites!

- Many disreputable sites will attempt to install malware on your system through "drive-by" exploits just by visiting the site in your browser. Lyrics sites, free software sites (especially ones that target young children), cracked software sites, and pornography sites are some of the worst offenders.
- Most of these drive-by attempts will be thwarted if you keep your Windows updated and your internet browser secured (see below). Nevertheless, it is **very** important only to visit web sites that are trustworthy and reputable.
- In addition, never give out personal information of any sort online. And never click "OK" to a pop-up unless it is signed by a reputable company and you know what it is!
- For more general information see the first section, **"Educate yourself and be smart about where you visit and what you click on"**, in **this tutorial** by Grinler of BleepingComputer.

Must-Have Software

NOTE: Please only run one anti-virus and one anti-spyware program (in resident mode) and one firewall on your system. Running more than one of these at a time can cause system crashes and/or conflicts with each other. Of the following programs, passive protection like SpywareBlaster, IE-SPYAD and MVPS Hosts file can be used with active resident protection programs effectively. The free version of Malwarebytes' Anti-Malware is an on-demand scan and clean program that will also not conflict with resident protection, Spybot is also on-demand but has resident protection if the Teatimer function is used. Only one scan at a time should be run.

4.) Antivirus

- An Anti-Virus product is a necessity. There are many excellent programs that you can purchase. However, we choose to advocate the use of free programs whenever possible. Some very good and easy-to-use free antivirus programs are **Avast**, and **AntiVir**. Please run only one antivirus resident at a time!
- It's a good idea to set your antivirus to receive automatic updates so you are always as fully protected as possible from the newest threats.

5.) Internet Browser

- Many malware infections install themselves by exploiting security holes in Microsoft Internet Explorer. It is strongly suggested that you consider using an alternate browser.
- Both Mozilla Firefox and Opera are next-generation browsers that are more secure and faster than Internet Explorer, immune to most known browser hijackers, and outfitted with built-in pop-up blockers and other useful accessories.

6.) Firewall

- It is critical that you use a firewall to protect your computer from hackers. We don't recommend the firewall that comes built into Windows XP. It doesn't block everything that may try to get in, it doesn't block anything at all outbound, and the entire firewall is written to the registry. (The built-in Vista firewall blocks both incoming and outbound, but is still written to the registry). Since most malware accesses the registry and can disable the Windows firewall, it's preferable to install one of these excellent third party solutions.

- Two good free ones are **Online Armor** and **Outpost**. The trial version of **Sunbelt Kerio Personal Firewall** will also work in "free mode" after the trial period expires. Please only use one firewall at a time!

7.) Install Javacool's SpywareBlaster

- This excellent program blocks installation of many known malicious ActiveX objects. Run the program, download the latest updates, "Enable All Protection" and you're done. Although it won't protect you from every form of spyware known to man, it is a very potent extra layer of protection.
- Don't forget to check for updates every week or so. Also see **this tutorial** by Grinler. (Note: This tutorial is for an earlier version, so there may be some minor differences)

8.) HOSTS file

- Another good program is **MVPS HOSTS**. This little program packs a powerful punch as it blocks ads, banners, 3rd party Cookies, 3rd party page counters, web bugs, and many hijackers.
- For information on how to download and install, please read **this tutorial** by WinHelp2002.

Other Cleaning / Protection Software

9.) Spybot

- **Spybot Search & Destroy** is a good free scanner. Spybot has an **"Immunize"** feature which works roughly the same way as SpywareBlaster above.

- Another feature within Spybot is the TeaTimer option. TeaTimer detects when known malicious processes try to start and terminates them. It also detects when something wants to change critical registry keys and prompts you to allow this or not.
- See **this tutorial** by Grinler for more information on running spybot. (Note: Tutorial is for an earlier version, so there may be some minor differences)

10.) Malwarebytes' Anti-Malware

- An outstanding all-purpose anti-malware scanner and cleaner is **Malwarebytes' Anti-Malware**. Although there is also a paid version with added features, the free version is fully functional.

11.) Windows Defender

Microsoft now offers their own free malicious software blocking and removal tool, **"Windows Defender"** (Not compatible with Windows 98 and ME.) It also features real-time protection.

12.) Lock down ActiveX in Internet Explorer

- Even if you plan to use an alternate browser, you will have to use Internet Explorer for tasks like updating Windows or visiting any other site that requires ActiveX. Also, since Internet Explorer is integrated into the Windows core, keeping it locked down is very important.
- For IE7, open IE and go to **Tools > Internet Options > Security > Internet**, then press **"Default Level"**, then **OK**.
  For IE6, now press **"Custom Level."**
- In the ActiveX section, set the first two options ("Download signed and unsigned ActiveX controls)

to **"Prompt"**, and ("Initialize and Script ActiveX controls not marked as safe") to **"Disable"**.

- Now you will be asked whether you want ActiveX objects to be executed and whether you want software to be installed. Sites that you know for sure are above suspicion can be moved to the Trusted Zone in Internet Option > Security.
- So why is ActiveX so dangerous that you have to increase the security for it? When your browser runs an ActiveX control, it is running an executable program, no different from double-clicking an exe file on your hard drive. Would you run just any file downloaded off a web site without knowing what it is and what it does?

13.) Finally, after following up on all these recommendations, why not run **Jason Levine's Browser Security Tests**

They will provide you with an insight on how vulnerable you might still be to a number of common exploits.

Happy **safe** computing!