

Personal Tech Aid

The father-son business you can trust with your computer

help@personaltechaid.com ◆ www.personaltechaid.com ◆ (206) 463-0079

Preventing Virus / Malware Infections in Windows

portions courtesy of Stephen Boots, MVP (Microsoft® Most Valuable Professional)

May 2011

- Make sure that the Windows Firewall [or similar firewall] is enabled.
- Make sure that all important/critical updates, including service packs for the operating system and programs are installed from Microsoft Update (Windows Update).
- Make sure that Microsoft Update is set to at least notify of new updates; the preferred setting is to download and install automatically. If you update manually, be sure to update as soon as possible after being notified of available updates.
- Make sure Internet Explorer is at version 8 or 9 and updated with all patches.
- In Internet Explorer, use the SmartScreen Filter.
- Make sure that IE Internet Security settings are at least set to medium-high (default).
- Enable the pop-up blocker in IE.
- On Vista and Windows 7 make sure that User Account Control (UAC) ON and not running with elevated privileges.
- Install an anti-malware program like Microsoft Security Essentials (MSE) or McAfee AntiVirus and ensure that databases are updated automatically.
- Programs like MSE or McAfee AntiVirus can't catch all malware. They are especially not good at catching "rogue" malware: the kind that pretends to be an anti-malware program, but whose constant pop-ups are just a ruse to get your credit card info. Remedy: perform all the other items in this list, and install a program like Malwarebytes Anti-Malware (MBAM). Either get the free version of MBAM and do a quick scan at least weekly, or get the paid version with which you can schedule automatic updates and scans. **WARNING:** If you get the paid version, do not run the "Realtime Proactive Protection" function; doing so could conflict with your main anti-malware program.
- Make sure that installed applications, especially Adobe Reader, Adobe Flash Player, and Java are at their latest versions. Many vendors regularly update and patch for security holes.
- Never click through links from unknown sources, and use caution even if they are from a "trusted" source.
- Never open unsolicited email attachments.
- Practice safe web browsing. Avoid file sharing (especially torrent) websites like the plague.