i.t.solutions
uahuntsville

SECURITY RECOMMENDATIONS FOR WORKSTATIONS

AUDIENCE

This document is for UAHuntsville students, staff and faculty, particularly for Windows users.

GENERAL RECOMMENDATIONS

A secure workstation can save time and trouble. A few simple steps can secure your workstation or laptop.

- Apply all the latest Microsoft Windows updates, including service packs.
- Configure Automatic Updates to install Microsoft Windows updates automatically.
- Apply the latest security updates for all applications.
- Apply all the latest Microsoft Office updates.
- Update your Adobe Reader/Writer products.

Note: Adobe is no longer providing security for versions 6.x and 7.x

- Update your Adobe Flash Player. Visit http://kb2.adobe.com/cps/155/tn_15507.html to check if you are using the latest version.
- Update to the latest Sun Java. Visit http://www.java.com/en/download/manual.jsp to download the latest version.

Note: Check to see if you have software that supports the new version of Java before upgrading.

- Avoid installing Instant Messengers like ICQ and other third-party products. If you must use a chat program, try Google Talk, which is integrated with UAHuntsville's Google Apps for Education.
- Avoid accessing social networking sites like FaceBook. If used, configure the appropriate privacy settings.
- Enable the Firewall and never disable it; it can take only seconds to get infected.
- Always install an Anti-Virus software package and make sure that it is updating.
- Perform a weekly Anti-Virus scan of your hard drive.
- Do not download and install shareware/freeware software unless it is from a trusted, reputable source.
- Avoid installing extra toolbars; some might contain spyware or slow your computer down.
- Use Mozilla Firefox with the extensions called Ad-Block and No-Script, or use Google Chrome which has a sandbox feature to protect the browser from attacks, for general off campus Internet browsing. Only use Microsoft Internet Explorer for campus authenticated applications. Upgrade Internet Explorer to 8.0 for phishing protection. For extra protections, use the Web Of Trust (WOT) safe browsing tool.
- Do not allow the web browser to store passwords when accessing password-protected sites.
- Clear your browser cache and temporary files using cache cleaners like CCleaner.
- Avoid questionable websites as some host malicious software that can infect your computer.
- Never open an email attachment unless you are positive about the source.

- Turn off USB autorun as this will help protect against autorun spreading viruses from USB devices.
- Enable a screen saver that will password protect your system when you are not in your office.
- Have a strong password for all user accounts and administrator accounts.
- Do not perform day-to-day work as local administrator. Most spyware can only infect within the user's profile.
- Turn off file and print sharing unless necessary. If required, then use the firewall to allow subnets only or select IP addresses.
- Use SSH instead of Telnet/FTP when connecting to remote services.
- If you use Remote Desktop to connect to your machine, then lock down port 3389 to allow just your remote IP address. Set Remote Desktop to use high encryption.
- Backup your documents and files regularly.

SPECIAL PRECAUTIONS TO PREVENT FAKE ANTIVIRUS INFECTIONS

If you get pop-ups claiming to advertise an antivirus or antispyware product, be careful. These could be Fake Anti-Virus Trojan attempts that mimic a real product. If you get pop-ups saying your system is out-of-date or infected, these may also be Fake Anti-Virus Trojans.

Use these steps to identify and eradicate a fake antivirus infection.

1. If the message is not from McAfee or your own ***known*** antivirus software, do not click on the window, or you will install the rogue software.
2. Do not select any buttons that allow the user to say no to the offer or the X button that would typically close the program down.
3. Press CTL/ALT/DEL which will bring up the task manager.
4. Look for the process or program and close it using Task Manager.

To view a list of rogue software, go to: http://www.spywarewarrior.com/rogue_anti-spyware.htm