10 Steps to Protecting Your Computer

Step 1. Use a Firewall.

What's a Firewall?

A firewall helps protect your computer from hackers who might try to delete information, crash your computer, take control of your computer or steal your passwords or credit card numbers.

Step 2. Use updated anti-malware software

What is malware?

Viruses and spyware are two kinds of malicious software that you need to protect your computer against. WIU has an enterprise Symantec license for university computers (available for student personal computers as well) that provides additional protection such as anti-virus, anti-spyware and an IPS (Intrusion Prevention System) in addition to a firewall.

Step 3. Keep your Operating System (OS) updated.

As vendors discover flaws in their Operating Systems (OS) they make updates available in the form of patches, hotfixes and service packs. As an example, every second Tuesday of the month Microsoft comes out with security patches for its Windows operating systems. Patches can be configured for automatic installation or can be installed manually from the Windows Update web site.

Step 4. Run your computer with limited rights.

Most of the things we do day in and day out on a computer do not require the ability to install anything (installing software is one of the few things that requires administrative rights). Yet we tend to run our computers with full administrative rights, opening our computers to the covert installation of malicious applications via clicking on infected email attachments or by following links to web sites hosting malicious code. While disallowing all administrative rights may not be practical, running with dual accounts (one with local administrative rights for limited use and a second for everyday use with no administrative rights), is a concept worth exploring. WIU's University Technology (uTech) will be evaluating the feasibility of this dual account concept for university computers.

Step 5, Step 6 ... Step 9. Think before you click!!!!

Don't click on unsolicited attachments or follow unsolicited web links.

Clicking on attachments or following web links sent in email that you did not specifically request opens you up to infecting your computer. Be aware that social engineering goes on all the time and therefore your guard must remain up all the time. Even if something appears to be sent by someone you know and trust it may not be coming from whom you think and instead may be malware in disguise.

Step 10. Think before you click!!!!

Did I mention not to click on unsolicited attachments or follow unsolicited web links?

Regards,

Michael Rodriguez CTSO @ Western Illinois University
MA-Rodriguez@wiu.edu

"Let us not look back in anger or forward in fear, but around in awareness."
~ James Thurber