Modern antivirus programs work by comparing files to a known set of virus definitions and the behavior of programs. The virus definitions are updated frequently to include the latest known viruses and malware programs. If a file or program is not in the set of definitions then the antivirus software will not act against the contaminated file. It is important to make sure antivirus definitions are always current.

Most updates and scans take place overnight. With laptops, it is important to manually check for antivirus updates at least weekly. Also, ensure that a system scan is taken place weekly at a minimum. The only time that viruses are found using the dictionary method is during active scans with a matching record in the dictionary.

The other technique used in blocking malware is to recognize behavior of programs. Programs that try and alter registry settings, changes to operating system updates, change antivirus protocols, change firewall settings, etc. When these behaviors are recognized by the antivirus software a message is presented to the user to allow or deny the program to have access. Always be certain of the software that is raising these exceptions. Freeware and shareware from the internet are frequent targets for carrying a malware payload.

If the user authorizes a download or program to access system files then the antivirus software 'stands to the sidelines' and allows the access. Many viruses enter systems in this manner. Even if the new virus is in the set of definitions, once downloaded and installed it may be too late for the antivirus software to do anything about the infection.

UMD no longer supports updates for McAfee products. The university switched to Microsoft's security essentials for Windows machines and combination of antivirus and ClamXav for Macs.

Please check in your programs list for the proper antivirus configuration. Zone Alarm and McAfee virus scan are no longer supported and should be changed to the new anti-virus configuration. If you have questions or need help contact the IT-helpdesk: mmaddox@essic.umd.edu Ext 4-2627

Anti-Virus Software Update

How Antivirus Software Works
**Importance of Updates**

**Updates prevent malware infections**

Computer hackers spend endless resources trying to exploit vulnerabilities in operating systems and software. These vulnerabilities, once identified, are fixed by the use of software updates. Installing operating system updates frequently is very important to maintaining a secure computer system.

Most of the ESSIC systems are set to run updates every night. To run the update routines, systems must be powered on and have an internet connection. With laptops, it is important to manually ensure that updates are taken place.

Updates are not always about the operating system. Java, Flash, Acrobat, etc. also will have periodic updates. A large percentage of these updates fix a security vulnerability in the software. Without the updates, there may exists tunnels for malware to infect a computer without the notice of antivirus software.

**UPDATE FREQUENTLY!!!!!!!!!!!!!!**

---

**SPYWARE**

Images of someone in a café seeing every keystroke and webpage visited can instill a great feeling of fear.

Spyware is a type of malicious software that tries to go unnoticed on a system. Most spyware will not be recognized by typical antivirus software. It is only recognized when the spyware behavior triggers a response by the antimalware software in a system.

Spyware often piggybacks itself onto a system in downloads, toolbars, and web browser add-ons. Always be cautious when installing browser add-ons, like the ask toolbar.

Windows 7 has integrated anti-spyware protection into the O/S. This tool only recognizes behavior and asks for permissions or denials. If you allow the program into your system then ‘all bets are off’.

When in doubt contact the help desk at x42627 or mmaddox@essic.umd.edu

---

**Infected Computer-What to do?**

I think my computer is infected, Now what?

1) Disconnect from the internet. On a laptop, turn off the wifi receiver or unplug the lan cable. On a desktop, disable the network card or

2) Contact the help desk using x42627 or room 4061 in m-square if your phone is disconnected.

3) Removing viruses/malware/spyware can be a lengthy process that may involve formatting a hard disk
Rogue Security Software

Rogue security software (scareware) poses as a valid security software install or upgrade. The messages and alerts can appear to be from legitimate companies, like Microsoft, McAfee, or other producers of security software. The message is designed to trick the user into downloading rogue software that may contain a virus or spyware. Some of these packages will ask the user to purchase an upgrade or add-on to the system. These are attempts to steal money or identities. The security software installed by the ESSIC IT staff will never ask you to install an add-on, component, upgrade or any other object to your system.

Gone Phishing in E-Mail

Phishing e-mails are designed to steal money, identities or both. These scams are becoming more sophisticated every day. Identifying phishing e-mails:

- Bad grammar or spelling—a multinational company will review mass mailings for proper grammar for the country of delivery. An e-mail from Citibank written with ‘British’ grammar or spelling is phishing.
- Links in emails are a sign of phishing. Hover your mouse over the link and see if the website matches the embedded link.
- Threats of account closure and loss of assets. E-mail telling you to respond or you will lose services is a sign of phishing.
- Spoofing websites—linking to a phony website to simulate a recognized organization. Check the web address in the browser against the website. Bank of America, Citibank, etc.

Microsoft® Windows® Malicious Software Removal Tool


When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malware was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from Microsoft Update. Windows
HELPDESK CONTACT INFORMATION

For all your IT questions, problems, etc.

Walk-In #4061

Phone 301.314.2627

E-mail mmaddox@essic.umd.edu

Online Resources:

http://www.essic.umd.edu/~mmaddox/

http://helpdesk.umd.edu/

Information Technology Administration and Planning Group

Manager
Mark Baith x44269

Web Services
Travis Swaim x50145

IT Helpdesk
Mike Maddox x42627

Dell Latitude ST Windows 7 Tablet

The Latitude™ ST features Windows®-enabled power in the body of a touch screen slate, combining the mobility of a tablet with the manageability, security and compatibility you expect from Dell Latitude. Hit the ground running with an OS interface you already know. Produce and edit business documents on the go with the Latitude ST running Windows 7. Weighs less than 2 pounds with a screen size of 10.1”.

The ITAP group will be receiving a demo model of the Dell ST in February. There will be a hands on demonstration period for interested parties by March.

The Basics
- Intel® Atom® Processor Z670 (1.50GHz) 512KB
- 2.0GB, DDR2-800MHz SDRAM, Integrated
- 4-cell (30WH) Primary Lithium Ion Battery
- Dell Wireless™ 1535C 802.11a/b/g/n And BlueTooth 4.0
- Dual Webcams with Digital Microphone - 1.3MP Front / 5.0MP Rear
- 10.1” WXGA (1280x800) Wide Viewing Angle LED with Corning® Gorilla® Glass, Pen & Touch Input
- Intel® Graphics Media Accelerator 600
- 30W A/C Adapter (3-pin)
- Covered under the Universities’ 3 year next business day Dell service plan

Upgrades available 128 gb internal ss drive, wireless mouse and keyboard, docking station, etc.