This SPICE EduGuide covers malware prevention practices and safeguards for end users of the HSC computing environment. Malware means malicious software, a general term for software designed to cause damage or disrupt functions of your computer, or to collect private information about you and your computer use without your knowledge. Computer worms, viruses, spyware and adware are common examples of malware. Risks associated with malware are loss of productivity and privacy.

Loss of Privacy - Spyware or adware programs gather personally identifiable information and relay it to advertisers and other third parties. The information most typically collected includes browsing and on-line buying habits, and the computer's IP address. Some spyware programs obtain your name, password and other personal information that you have entered on your computer.

Productivity Loss - Computer viruses and worms cause a variety of disruptive events such as conflicts with legitimate software, or compromising the security of your operating system, or frequent workstation reboots or loss of data. Viruses and worms can spread over our network to the computers of your co-workers. The result could be a major diversion of support staff resources tasked with the clean-up effort, and users are often unaware of the effort.

SAFEGUARD REQUIREMENTS AND GUIDANCE

Malware often enters our computing environment through user practices and 'social engineering'. Social engineering is the practice of manipulating you for someone else's gain – similar to the behavior of a 'con artist'. User involvement is essential to help prevent malicious software in our environment:

- Spyware and adware are bundled with software that users like to download or install like AOL Instant Messenger, KaZaA, Gnutella and LimeWire. Illegally obtained and seemingly free software are often accompanied by viruses. You must notify your Unit ISM before you install software on an HSC computer to help you ensure the security of the software you wish to install. If it is a product in which the security and cannot be ensured, you may not install it.
- Email attachments, especially those that have arrived unexpected or those that you have accessed from a personal commercially available or free email system, carry viruses. Don't open an email attachment unless you are expecting it, are sure of the source, and are sure it passed through an antivirus scan.
- Files sent and received via instant messaging circumvent antivirus software protections provided by your HSC IT staff. Avoid this practice altogether. Contact your IT support staff for more secure methods of transferring files.
- Visiting unknown and untrusted web sites on the internet can easily result in malware being placed on your computer. Be wary of sites you have not visited before. Be skeptical of anything offered for free. Read all dialog boxes presented during your web site visit carefully. Ask for help or exit the site if you do not understand what you are being prompted to do.
- Your HSC computer must have malware software control. Commonly called antivirus software due to its legacy, today's products work to scan for and disable many types of malware. Your responsibilities regarding the malware software control on your HSC computer are:
    - Defer to your Unit ISM or IT Support staff for the right product and appropriate configuration. It can and should be configured to automatically 'scan' files and automatically update 'signature' or 'definition' files. New malware is released by malicious code writers almost daily and the 'signature' or 'definition' files of your antivirus software hold information that helps identify it.

- Know how to check your HSC computer to make sure the antivirus software is active and that its 'signature' or 'definition' files are up to date. The steps to check are specific to the antivirus software product installed by your IT Support staff. Contact your Unit ISM for assistance.
- Do not disable or circumvent malware software controls running on your HSC computer.
- Know that antivirus software is not a panacea for malware prevention. All the safeguards in this EduGuide are important to apply.

- If you suspect malware on your HSC computer, report it to your Unit ISM or IT Support staff.

SAFEGUARDS FOR PERSONALLY OWNED AND MANAGED COMPUTERS

If you connect a personally owned computer to our network, you must ensure malware software controls are installed and operating properly on your computer.

- Your personally owned computer may come pre-loaded with anti-virus, anti-spyware and anti-adware software. However, there is typically a subscription fee that you need to pay on an annual basis to keep it up to date. If you choose to keep the anti-virus, anti-spyware or anti-adware software that came with your computer:
  - Ensure that you register with the anti-virus, anti-spyware, and anti-adware companies for *automatic* updates to signature files and their scan engine. You'll want to configure your software to check for updates *and* install them automatically. Your software is only as good as the last time its signature files were updated.
  - Maintain your annual subscription fee ($$) or you will not be able to receive your updates.
- There are some lower cost alternatives for maintaining malware software controls on your personally owned computer:
  - UF has purchased McAfee Anti-Virus software for all faculty, staff and enrolled students to use on their personally owned computer. Dowload a copy of McAfee Anti-Virus software from http://www.software.ufl.edu. Follow the download and installation instructions carefully, even downloading VPN software which is necessary and safe. Enable the AutoUpdate feature and schedule it for daily updates. Enable Scan All Fixed Disks and schedule a scan at least weekly when you know your computer will be turned on.
  - There is a free and safe software utility called Spybot Search&Destroy (S&D) that helps control spyware. You can download Spybot S&D on your personally owned computer from http://www.safer-networking.org/en/download/. Use the advanced features of Spybot to enable Automatic Updates and Schedule Scans at least weekly to keep your 'include' files and Spybot version up to date.
  - There is a free and safe software utility called Ad-Aware SE Personal that helps control adware. You can download Ad-Aware SE Personal on your computer from http://www.lavasoft.de/software/adaware/. Unfortunately updates cannot be automated with the free version of Ad-Aware. So be sure that you manually check the web site on a weekly basis and download definition file and Ad-Aware program file updates.

Policy & Standards References:
TS0007 Malicious Software Controls
TS0004 Security Education Awareness
BA0001 Software Security Compliance