Smeal College of Business - Guidelines for Anti-Virus & Anti-Spyware Protection: SCB-AVSP-01

Recommended processes for ensuring significant virus protection:

- Always run either the current University site licensed anti-virus software, which is available from the University download site (https://downloads.its.psu.edu), through the RIIT Group, or other reputable anti-virus software (in the case of personally owned machines).
- Download and install anti-virus software updates as soon as they become available.
- Set your anti-virus software to run complete scans on a daily basis
- DO NOT disable real-time file protection or automatic floppy drive or memory key scanning.
- NEVER open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately. Empty the mail application's trash bin to be certain the deleted attachments are completely removed from the computer.
- Always delete spam, chain, and other junk email. Do NOT forward such emails to others. This is covered in the College of Business *Acceptable Computer Use Policy*.
- Never download files (applications, multimedia) from unknown or suspicious sources.
- Avoid directly sharing your disk drive or a folder with read/write access unless there is a significant business requirement to do so. Alert the RIIT Group department of the need to do so.
- Always scan any media from an unknown source for viruses before using it. De-activate the auto-run feature on your PC.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place. DO NOT take these back-ups home. Make arrangements with the RIIT Group for safekeeping of your back-ups.
- If lab research conflicts with anti-virus software, perform a complete scan with the anti-virus utility to ensure a clean machine, disable the software, then run the lab experiment or research. After the experiment is complete, enable the anti-virus software. When the anti-virus software is disabled, do not run or download any applications or un-trusted files that could transfer a virus, e.g., email or file sharing, on-line documents.

Recommended processes for ensuring significant spyware/adware/malware protection:

- University computers often contain private/privileged data. Software such as spyware that monitors web browsing, keyboard use or related activities must not be installed.
- Download and run trustworthy anti-spyware/adware detection and removal tools on a regular basis. These include applications such as Spybot S&D and Ad-Aware available from the University download site (https://downloads.its.psu.edu) *note: the free version of Ad-Aware can be installed on personally owned machines only*

- You should check for updates at least once a week for the application/s to be effective in finding and removing spyware/adware/malware
- You should never install any anti-spyware software except those mentioned above. Some supposed free and pop-up styled "anti-spyware" programs are actually spyware or contain viruses that can actually infect your computer rather than clean it.
- Be wary of using peer-to-peer programs (P2P) file sharing programs such as Kazaa, BearShare, Limewire, etc. Music and filesharing applications are known to leave your computer vulnerable to spyware, adware and hackers.
- Be wary of installing freeware/shareware. Spyware applications may be bundled as a hidden component of these types of programs. Also, the "free" or "share" aspect of the software is often supported through the use of advertising which may include spyware.

The most direct route by which spyware can infect a computer involves the user installing it. Know your download source. Only download software from trusted sources.

Revision History

06/04/2007 - Initial modification from COE policies, used with permission in conjunction with the Penn State IPAS project. http://www.ipas.psu.edu

06/05/2007 – Addition of Anti-Spyware guidelines.