



Security is everyone's responsibility. If you have a computer, you are responsible for making sure it is secure. You must follow these expectations to help the University of Evansville protect its resources.

Secure Computing Expectations

1. Apply security software patches and updates regularly. Windows users can use Microsoft's Windows Update service. Refer to [http://ots.evansville.edu/techfaqs/Using Microsoft Windows Update.htm](http://ots.evansville.edu/techfaqs/Using_Microsoft_Windows_Update.htm) for more information. Apple OSX users should install security updates when prompted by "software update," or by visiting <http://www.apple.com/support/downloads>
2. Install and use anti-virus software. The Office of Technology Services has licensed Sophos Anti-Virus and security software for all University owned PC's. There are several very good commercial software packages available as well as some free ones. A decent free package is AVG Anti-Virus, which is available for download at www.grisoft.com. You should set your computer to automatically update anti-virus applications at least once per week. However, once per day is preferable. For more information, please visit <http://ots.evansville.edu/techfaqs/viruspywareremoval.asp> for more information.
3. Always use strong passwords, and keep them secret.
4. Install firewall security software. Microsoft's Windows XP Internet Connection Firewall (ICF) software ships with Windows XP and should be activated. Free firewalls are available on the Web.
5. Apply patches to application software such as word processors, IM clients, and other programs. For example, Microsoft Office updates are available at <http://office.microsoft.com>.
6. Never comply with requests for personal information from an email or phone call unless you initiated the contact. These are often phishing scams trying to steal your personal information. For more information see the OUCH report on the Security site, <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm> , or http://www.antiphishing.org/phishing_archive.html
7. Never store sensitive personal information such as your bank account information or Social Security numbers on your computer.
8. It is your responsibility to abide by any University of Evansville policies, including the University of Evansville Acceptable Use Policy, any other relevant University of Evansville policies, and any and all federal and state laws including copyright law. You can view the Office of Technology Services Acceptable Use Policy at <http://ots.evansville.edu/policies/AUP.asp>

As member of the University of Evansville community, there are several computer security resources available to you. These include documentation, software, and tools to maintain a secure computer. Below is a list of best practices you should follow to help keep your information and your computer secure.

Be Sure to.....

- * use adware and spyware removal programs. Refer to <http://ots.evansville.edu/techfags/virusspywareremoval.asp> for more information.
- * back up files and data to storage media such as CDs, Zip disks, DVDs, flash drives, or other media.
- * set the security settings to the highest level on Internet browsers. This may disrupt some of your favorite Web sites. If so, lower the settings until you find one that allows Web sites to work. Disable cookies, or set cookies to be discarded when the Web site is closed. Again, this may disrupt some Web sites and adjustments may be needed. Remember to update your Web browser as you would any other application.
- * verify your system security by using online tools such as Symantec's Security Check, <http://security.symantec.com/sscv6>, and GRC's "Shield's UP!", <https://www.grc.com/x/ne.dll?bh0bkyd2>

DO NOT....

- * click "Yes" to install software downloaded from Web sites before you read the fine print. Other programs, such as spyware applications, may be included with a program you download, so check the fine print before installing programs.
- * open email attachments that you aren't expecting. Especially avoid attachments ending in .exe, .vbs, .pif, .scr, .com, or .bat, and don't unzip files you are not expecting. Don't open the attachment even if it looks like it is sent from someone you know—many viruses can forge, or spoof, the sender's name from names found in address books.
- * open files sent to you in Instant Messaging (IM) or peer-to-peer (P2P) programs. Viruses can be spread through IM and P2P programs and many anti-virus programs cannot detect viruses spread in this way.
- * download software such as screensavers, games, or other programs from unfamiliar or unverified sources. These can harbor computer viruses or open a "back door," giving others access to your computer.
- * set the computer for automatic login.
- * leave any guest accounts enabled.
- * share directories and files. If you must have a shared drive on a network, make sure you have a strong password.

For more information about current security threats, please read the monthly SANS OUCH report. This report gives information and, in many cases, the exact wording of Internet threats. Visit the OTS Security News site at <http://ots.evansville.edu/Security/> for more information.

Questions? Contact the OTS Help Desk at Help@Evansville.edu or 488-2077