

Technology for Librarians 101

Computer Security - Tips for avoiding viruses and other security attacks

Almost all of our computers or mobile devices are connected directly to the Internet. Unbeknownst to you, it is very likely that several times a day other computers are trying to find out information about you or if your computer can be taken over and used for criminal mischief without your knowledge.

Follow these preventive steps to avoid viruses, spyware, trojan horses, and other security attacks.

- 1. Windows or Mac OS: make sure the Update feature automatically downloads critical updates.**
 - Windows computer: See "[Service Pack and Update Center](http://windows.microsoft.com/en-us/windows/service-packs-download#sptabs=win7)" (<http://windows.microsoft.com/en-us/windows/service-packs-download#sptabs=win7>).
 - Mac computer: See "[OS X: Updating OS X and Mac App Store apps](http://support.apple.com/kb/HT1338)" (<http://support.apple.com/kb/HT1338>)
- 2. Make sure you have anti-virus software installed and that it updates automatically.**
- 3. Make sure all software is automatically updated.** This is usually the default setting when software is installed.
 - Web Browser (Google Chrome, Mozilla Firefox, Internet Explorer, Safari, or others)
 - Adobe Reader (used for reading and printing PDF files)
 - Adobe Flash (used for playing animations or videos)
 - Microsoft Office
 - Java (recommend that this software is NOT installed; if installed on your computer)
 - Other installed software
- 4. Scan ALL files on your computer at least once a month for viruses and other security threats.**
 - See your anti-virus software Help documentation for instructions.
- 5. Use a firewall to block unwanted access.** A firewall helps protect your computer from hackers who might try to delete information, crash your computer, or even steal your passwords or credit card numbers.
 - Windows Firewall: See "[Firewalls in versions of Windows](http://www.microsoft.com/security/pc-security/firewalls-using.aspx)" (<http://www.microsoft.com/security/pc-security/firewalls-using.aspx>)
 - Mac Firewall: See "[OS X Mavericks: Firewall pane of Security & Privacy preferences](http://support.apple.com/kb/PH14124)" (<http://support.apple.com/kb/PH14124>)
- 6. Only download software, programs, or apps from websites you trust.** Be cautious of "free" offers of music, games, videos, and the like. They are notorious for including malware in the download.
- 7. Do NOT share Drive C:** because viruses and network attacks can spread through the network by finding shared hard drives. To check your Windows settings, click the Start button > Computer (or My Computer) and right-click on the Drive C: icon.



Technology for Librarians 101 is offered as part of the Nebraska Broadband Mapping and Planning Initiative, funded through a grant by the U.S. Department of Commerce's National Telecommunications and Information. The Initiative aims to increase broadband adoption and use.

For more information, check <http://broadband.nebraska.gov>

