Reducing Your Risk When Internet Browsing At UNH

IT Security 8/06/2012

1. Log onto your computer as a non-administrator. Create and use an account on the computer which does not have administrative privileges to browse the Internet.
2. If possible, browse the Internet using a Macintosh rather than Windows computer.
3. Set the security level on your browser to as high a level as possible.
4. Read the warning signs in URLs before you click on them. Learn how to distinguish between www.unh.edu vs. www.unh.edu.bad.
5. Run your searches in trusted websites. For example, we provide a link for Windows Defender Offline below. If you were looking for that link, you should go to www.microsoft.com and search for it there, NOT in Google, Yahoo, or any other site. Make sure the search setting is for "Microsoft.com" and not "search the Internet".
6. Check your Microsoft Forefront virus scanning settings frequently. Make sure on-demand scan is turned on and that full scans are programmed (in addition to doing off-line scans) for a time of day or night when the machine is actually turned on.
7. Scan the machine periodically with another anti-virus product, such as Malware Bytes.
8. Use an off-line scan tool, at least weekly. We recommend using Microsoft Defender Offline using a bootable flash drive which can be setup at http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline. *Note: encrypted computers must be decrypted to enable use of a bootable flash drive.*
9. For assistance with any of these recommendations, contact your departmental IT support or UNH IT Security.