# Keeping Your Home PC Safe

**

*In recognition of National Cyber Security Awareness Month, the Office of Safe and Secure Computing is bringing you tips to stay safe online. Our second weekly topic is keeping your home PC safe.*

*Keeping your PC free of malware can be a challenge. By following these tips, you can help keep your PC safe.*

**Only install software from trusted sources**. Even [seemingly-trustworthy popular download sites](https://askleo.com/is-it-safe-to-download-from-download-sites/) can bundle “Potentially Unwanted Programs” along with the software you desire. Files from peer-to-peer and file-sharing apps should be avoided as these are much more likely to contain malware.

**Keep all your software up to date**, especially web browsers and plugins. Configure automatic updates where possible.

* Visit <https://browsercheck.qualys.com/> to check if your web browser and plugins are up-to-date
* Uninstall software you no longer need, especially browser plugins, such as Java, Silverlight, Shockwave, Adobe Air, etc. If you don’t have it installed, it cannot be exploited.
* Use software like [Secunia PSI](http://secunia.com/vulnerability_scanning/personal/) (Personal Software inspector) to check for out-of-date software.

**Keep offline backups of your important files**. You can do this using external hard drives, but Cloud services like [Carbonite](http://www.carbonite.com/), [Mozy](https://mozy.com/), and others work best by automatically backing files up and storing them offline. It is important that the backup location you rely upon is not connected to your computer, since ransomware will encrypt and hold hostage all files on directly-attached or mapped network storage.

**Ensure you are using antivirus software.** Antivirus is not perfect, but it is part of a layered defense. You need not purchase an expensive solution - there are free antivirus programs, such as “[Microsoft Security Essentials](http://www.microsoft.com/en-us/download/details.aspx?id=5201)” and others.

**Use anti-exploit software.** Anti-Exploit software provides protection against memory-based attacks. Since it does not rely on signatures, it can even protect against unknown attacks and those for which no patch is available. Consider using the free "[Microsoft Enhanced Mitigation Experience Toolkit](http://www.microsoft.com/en-us/download/details.aspx?id=43714)" (Microsoft EMET) for exploit protection. See this [installation guide](https://www.trustedsec.com/november-2014/emet-5-1-installation-guide/) for assistance.