University Information Security Office
University of South Carolina

Securing Your PC

How to get the most security from your Windows machine.

Kyle S. Brown

Kyle is an alumnus of the University of South Carolina and is currently the university's information security awareness specialist. He is part of the University Information Security Office where he works to help people understand the dangers of modern computing.

Basic Steps

At a minimum, these "Basic" recommendations should be implemented. These steps should be completed before moving on to the "Intermediate" or "Advanced" sections.

Make sure your version of Windows is supported.

Finding your Windows version:
http://windows.microsoft.com/en-us/windows/which-operating-system

Microsoft currently supports Windows XP SP3, Vista SP2, 7 SP1, and 8 for client devices such as laptops and desktops. Windows XP is no longer supported as of April, 2014. Unsupported versions of Windows do not receive important security fixes that could leave your computer vulnerable to attack.

Keep Windows up to date.

Turning on automatic updates for Windows:
http://windows.microsoft.com/en-us/windows/turn-automatic-updating-on-off#turn-automatic-updating-on-off=windows-7

Remember to install the updates soon after they become available if you are interested in better protecting your computer from Internet criminals.

Install anti-virus software.

Microsoft Security Essentials:
http://windows.microsoft.com/en-us/windows/security-essentials-download

Anti-Virus provides basic protection against malicious software. In many cases, free anti-virus products provide just as much protection as paid products.

Use a secure Internet browser.

Google Chrome:
http://www.google.com/chrome

Google is committed to continually improving the security of Chrome. It is often the first company to implement new security features within its browser.

Intermediate Steps

Once the basic recommendations have been implemented, the following steps should be completed for increased security.

Protect your PC from known malicious websites.

OpenDNS (Free for personal use):
http://www.opendns.com

UNIVERSITY OF SOUTH CAROLINA

OpenDNS provides a service which will monitor the location of sites that are being visited, and protect you when needed. The service maintains a list of bad locations that it will block, if needed. The services can also be configured to provide parental controls for blocking inappropriate content.

***OpenDNS should not be setup on University-owned systems. It is known to cause problems when attempting to connect to resources like printers or shared drives.**

Keep your applications up to date.

Secunia PSI:
http://secunia.com/vulnerability_scanning/personal/

Outdated applications have weaknesses that may allow an attacker to access or take control of your computer. Keep the security of your machine strong by updating your applications. Secunia PSI will notify you when updates for your applications become available, and will help you install them.

Keep a regular backup schedule.

Backup and Restore:
http://www.howtogeek.com/howto/1838/using-backup-and-restore-in-windows-7/
Box (10GB Free):
http://www.box.com
OneDrive (1 TB Free):
http://windows.microsoft.com/en-us/skydrive/download

Your photos and documents are hard to replace in the event of a catastrophic crash. By backing up your files, you can keep an already difficult experience from becoming worse. Do not wait until its too late.

With the exception of Windows' built-in backup and restore, the rest of the tools above will store your data in the cloud. Backing up to the cloud does not require any additional hardware such as a flash drive, external hard drive, or CD/DVD-ROM.

When using a cloud storage provider, the following are recommended.

- Make sure you understand the provider's privacy policy.
- Use multi-factor authentication.
- Occasionally (every 6 months) backup to a physical media.

Most of the cloud-based backup tools provide a certain amount of storage for free. A larger plan will need to be purchased to upload larger amounts of data.

Turn on the built-in firewall.

Prevent unwanted connections with a firewall:
http://windows.microsoft.com/en-us/windows7/understanding-windows-firewall-settings

Attackers can use listening applications to harm your computer. Use the built-in firewall to limit the number of accessible applications.

Subscribe to a Malware Domain Feed.

Ad Block Plus for Google Chrome:
https://adblockplus.org/en/chrome

After installing AD Block Plus,
click "subscribe" in the Malware
Dmain section of the following link.

https://adblockplus.org/en/subscriptions

By using AD Block Plus and subscribing to the Malware Domain list, your browser will refuse access to known bad websites.

Disable risky browner plugins.

Disable Google Chrome plugins:
https://support.google.com/chrome/answer/142064?hl=en
Disable Mozilla Firefox plugins:
https://support.mozilla.org/en-US/kb/disable-or-remove-add-ons#_how-to-disable-plugins
Disable Internet Explorer 10 plugins.
http://windows.microsoft.com/is-is/internet-explorer/manage-add-ons

Internet browser plug-ins (such as Adobe Flash and Java) are vulnerable to attacks and may allow an attacker to harm your PC. If you are not regularly using plug-ins, try disabling them.

Use a password management tool.

Keepass Classic Edition (Free for personal use).
http://keepass.info/
LastPass (Free for personal use).
http://www.lastpass.com

Choosing strong and unique passwords is critical to keeping your data safe. Each online account should have a different password. Easier said than done, right? Well, password management tools will help you keep up with all your passwords. Tools like Keepass or LastPass will even enter your username and password upon accessing a familiar website. Do not let an attacker get access to all of your important accounts by stealing one password. Remember, we do not want to make it easy for the attackers.