

Windows Guidelines

These are self-help guides offered by the SOS office related to assisting you in reformatting your hard drive and reinstalling your operating system. Note: Anyone from outside The Pennsylvania State University network may not be able to view some of these files.

The information on this web page contain only suggested guidelines for rebuilding and securing your machines. Because the process is different for every computer manufacturer, these guides are written at a high level. Any questions you have about this process should be directed to the [Help Desk](#), area [RESCOM](#), a faculty/staff IT contact or [Information Systems Consulting Services](#) for a specialized affordable alternative. Carefully consider which guidelines to implement, as every environment will have very differing needs and requirements. It is recommended that you implement one modification at a time to determine the impact of the change. Always be sure to document all modifications that are made and implement them in a test environment prior to deployment in a production environment.

[Detailed Instructions for Reformatting and Reinstalling Any Version of Windows](#)

Use the above detailed instructional guide in conjunction with the rebuild guidelines below for your specific operating system.

Windows XP Reinstallation Guidelines
--

Windows XP Checklist

If you have Windows installed on your computer but do not know which version you have, right-click on "My Computer" and select "Properties" from the menu that appears; it will display your operating system details.

1. Disconnect from the network

Unplug the PC's network cable and remove any wireless network adapters if you are near a wireless access point that allows automatic connections without any configuration by the user. If the wireless adapter is built-in, you are most likely using a laptop. Take the PC somewhere out of range of the wireless network.

2. Back up your files

Consider the files that you need to keep (word documents you have written, school projects, e-mail). Make copies of the files that are unique to you or irreplaceable. You can use an actual back up program, or you can manually copy the files. Either way, you will need to get the files to a location other than the drive where you plan to install Windows. Some examples, are; another hard drive installed in the PC or connected to it via USB or FireWire, one or more CDs or DVDs, another computer, via the network, zip disks, Jaz disks, or SuperDrive.

3. Preparation Steps

Once you have reformatted the machine, you will need to install several files before placing it on the network for the first time to prevent it from becoming infected again. Service Packs, patches, and hotfixes are software update programs which eliminate specific vulnerabilities that have been discovered in a larger piece of software. You can find some of the updates via the links below. You will need to use either a writeable optical drive (CD/DVD-R), a mobile/external drive, a logical drive, or your [PASS](#) space (although PASS is limited in size) to download the updates and burn them to a CD **before** you do the reformat from another computer. Patches should be downloaded from a trusted machine rather than a compromised host. **NOTE:** The service pack files are very large (over 100 megabytes each) and may take a while to download/burn to a disk, depending on your Internet connection.

The most highly recommended service packs and patches can be found below, however, this is not a comprehensive list of all the patches that exist. ALWAYS check the applicable operating system website (i.e., [Microsoft](#)) to get the latest patches for your computer. Many applications that are running on your system also have patches and hotfixes, and these updates will also need to be downloaded and applied prior to placing your computer on the Internet for the first time.

For Windows XP:

[Windows XP Service Pack 2 *](#)

[Security Update for Windows XP \(KB835732\)](#)

[Update for Windows XP Service Pack 2 \(KB884020\)](#)

- ***At the University Park campus XP SP2 CDs are available at the [ITS Help Desks](#) in 2 Willard Building and in 215 Computer Building.**
- At non-UP locations, the XP SP2 CDs are available at the same distribution points as the PAC-ITS CD.

4. Reformat & Reinstall

If a machine has been compromised in any way, the *ONLY* way to ensure that the machine is secure is to reformat the hard drive and reinstall the operating system. This process will involve backing up any data on the machine and reinstalling the operating system or running a system restore/recovery CD provided by the manufacturer. At this point, you will need to create an administrator system password, after which you will reinstall all programs, secure the machine, and restore data files.

Reformatting your machine removes all data from your computer. This is an irreversible process.

5. Create Passwords

Intruders do attempt to gain access to shared computer systems through the accounts of others. Their motives vary from curiosity to criminal malice. It is part of your responsibility as a computer user to create a strong password for both your Penn State access account and all operating system accounts on your computer. It is your privacy, your reputation, your files, and your computing resources that are all at risk. Often times passwords/password files are commonly collected for future use when a system is compromised. All passwords should be changed and strengthened in the event of compromise. For detailed instructions on how to create a good password go to the [SOS passwords page](#).

6. Install Firewalls

Windows XP has a built-in firewalls. For other operating systems, you should buy or download and install a personal firewall. It is important to ensure your firewall is enabled for complete protection. Instructions for configuring your firewall can be found at the Penn State ITS Helpdesk links below. Also included is a *link to personal firewall (that can be downloaded free of charge for non-University computers).

Windows XP	http://helpdesk.psu.edu/windows/xp/sp2/firewall.html
ZoneAlarm*	http://www.zonelabs.com

[Adaware](#) and [Spybot S&D](#), are both popular spyware tools, designed to detect and remove a variety of spyware types from a user's computer. Though equally effective, Spybot S&D is a bit more advanced than Ad-Aware; novices are encouraged to first try Ad-Aware. **Note:** Spybot Search and Destroy is free for use on both University and personally-owned machines. However, Ad-Aware is free only for personally-owned machines. Users who wish to run it on University-owned machines will need to purchase this product.

7. Automate Live Antivirus Updates

New viruses are written and released on a daily basis. Many of the more common viruses "morph" or change frequently to make them more difficult to detect. Viruses spread rapidly and by many different ways (for example, via e-mail attachments; infected document files; Web sites that contain hostile code that can infect your computer through vulnerable browsers; and unprotected file shares). Using Symantec AntiVirus ([FREE for Penn State students, faculty, and staff](#)) and configuring it to update virus definitions automatically with the directions below will help keep your computer protected.

Live Update Windows	http://helpdesk.psu.edu/virus/ liveupdpc.html
---------------------	--

8. Review Windows Security Guides and Documents

Windows XP Rebuild Guidelines	Windows XP Checklist
Investigating a suspected Windows compromise	Installing IPSecurity Filters in Windows 2000 or Windows XP