

### Basic Computer Security Practices

- Make backups of important files.
- Apply patches to the operating system.
- Use anti-virus software, update definitions very frequently, and run a full virus scan at least once a month.
- Use a firewall.
- Use anti-spyware software, and run a scan at least once a month.
- Run disk defragmenter and disk cleanup on an occasional basis.

### Back Up Personal Files

- *Before doing any kind of maintenance on your computer*, it is vital to back up your files. Backups protect you if anything truly disastrous happens to your system: in the worst possible case, you could buy a new computer, reinstall your programs (because you still have the CDs they came on – don't you?) and restore all your personal files from your backup disks.
- *At a minimum*, you need to back up any file you have created. These may include: Word documents, Excel spreadsheets, other Office documents, photos from your digital camera, data from Quicken or Microsoft Money or another "checkbook management" program, saved email, or any other file you care deeply about.
- Very Basic Back-up: use My Computer/Windows Explorer to locate the files you want and copy them to some kind of backup media (see below).
- Most versions of Windows come with a backup utility. Locate it by clicking *Start → Accessories → System Tools → Backup*, and follow the instructions to back up the desired files/folders. If you cannot find Backup in the list, you may need to install it from your original Windows CD-ROM. See the following website: [http://www.langa.com/backups/backups\(8\).htm](http://www.langa.com/backups/backups(8).htm) for instructions on installing the backup utility for each version of Windows.

### Backup Media (things onto which you can back up files)

Floppy Disk	Small and pathetic – holds 1.4 MB. You'll need lots of these to back up any significant amounts of data. Older computers came with a floppy disk drive; most new ones do not.
Zip Drive	Uses Zip disks that hold up to 750 MB of data. Must buy and hook up the drive.
Tape Drive	Uses tapes that hold up to hundreds of GB (thousands of MB). Must buy and hook up the drive.
CD burner	Recordable CDs (CD-Rs) can hold around 700 MB of data. All newer computers have CD-burners; some also have DVD burners (DVD-Rs hold 4.7 GB of data)
Flash Drive USB Drive Thumb Drive	Lots of names for the same thing: a removable drive that fits into your computer's USB port. Holds between 10 MB and 16 GB of data. Requires USB port.

### Why do I have to patch Windows?

Patching is necessary because hackers constantly search for security holes in Windows; when they find one, they write viruses and other exploits to take advantage of it. Also, other types of bugs are discovered as more people use each version of Windows over time. Microsoft produces patches that plug security holes and fix other bugs, and publishes them on their site.

### Apply patches to the operating system

- Updates are no longer available for Microsoft Windows NT Workstation, Windows 95, Windows 98, or Windows ME. They are still available for all versions of Windows XP and Vista.
- To update Windows, go to the Windows Update Web site at <http://windowsupdate.microsoft.com>.
  - Click Scan for Updates. Windows Update will scan your computer and give you a pre-selected list of critical updates.
  - Click Critical Updates and Service Packs in the “Pick updates to install” list at the left side of your screen. Windows Update will create a list of the updates appropriate for your computer.
  - Click Review and install updates. Select the updates to install, including any service packs and critical updates, and then click Install Now. You may need to restart your computer after installing the updates.
- It’s a good idea to turn on Automatic Updates in Windows XP and Vista. Click *Start* → *Control Panel* → *Security (Security Center in XP)*, then click Automatic Updates. On the tab, select your preferred update method.

### Phishing: Don’t Take the Bait

You receive official looking email or a pop-up message from someone you trust (a bank, your internet service provider, etc.) informing you that they need to verify some information (personal info, passwords, account info) and asking you to email the info to them or to click a link to correct the problem. The link takes you to a fake site that looks exactly like the real site, and asks you to verify your personal information (passwords, social security numbers, bank account numbers, etc.) You’ve just given your information to an identity thief!

- **No reputable company will ever ask you for personal information via email.**
- If you think a warning may be genuine, contact the company. (Look up the number in the phone book, don’t call one on the suspicious message! Similarly, type in the company’s web address yourself or use a search engine, don’t click any links in the message.)

### The Bad Stuff: Definitions

- **Virus:** A piece of computer code that attaches itself to a program or file so it can spread from computer to computer, infecting as it travels. Viruses can damage your software, your hardware, and your files.
- **Worm:** A type of virus that copies itself from one computer to another automatically by taking control of the computer’s communications features like email or instant messaging. For example, a worm could send out copies of itself to everyone listed in your e-mail address book, and their computers would then do the same. They can also tunnel into your system and allow somebody else to take control of your computer remotely.

## Computer Security

- **Trojan horse:** A computer program that appears to be useful software, but instead it compromises your security and causes a lot of damage. Examples: an e-mail with attachments claiming to be Microsoft security updates, but which really were viruses that attempted to disable antivirus and firewall software; a pop-up ad that warns you your computer is infected with spyware, which installs spyware when you click it.
- **Adware:** Software that comes bundled with something useful, which displays advertisements as you use the free software. *May be harmless*, but may also perform drive-by downloads; may be spyware.
- **Drive-by download:** Some sites stealthily download software to your computer by using misleading dialog boxes or other means.
- **Spyware:** Software that covertly gathers user information without the user's knowledge. May record keystrokes as you type them, harvest passwords, credit card numbers, sensitive information, where you surf, chat logs, and even random screenshots of your activity
- **Browser hijackers:** Malicious programs that change browser settings, especially homepages and default search pages. Some also produce pop-up ads for pornography, add dozens of bookmarks -- some for extremely hard-core pornography websites -- to Internet Explorer's Favorites folder, and can redirect users to porn websites when they mistype URLs.

### Vectors of infection

- **Discs or CDs:** Don't use a disk or CD from someone else's computer unless you are running antivirus software in the background. If you lend a writable disk to someone else, check it yourself when you get it back, *before* using it.
- **Email Attachments:** Everybody knows this one now. Don't open email attachments if you don't know what they contain, *even if* they come from someone you know. Don't *ever* open email attachments from someone you don't know.
- **Chat, IM:** Malicious code can now get on your computer via chat sessions, IM sessions, etc. If you do any of these things, you **MUST** use up-to-date virus scanners and firewalls, etc.

### Identifying dangerous websites

A lot of sites offering free goodies – screen savers, music downloads, games – are just fine. Another huge number are not. A free tool, McAfee Site Advisor, helps tell the difference.

- Search Google for "McAfee Site Advisor". Download and install the program. If you use Internet Explorer and another browser like Firefox, you need to download versions for each one.
- McAfee rates websites for safety. When you search in Yahoo, Google, and MSN, your results will be tagged in green, yellow or red. (Good, dubious, and bad, of course.)
- When you browse the web, an advisor button appears in your browser window. It will color code the web pages you are on the same way.

### Download a free antivirus tool

- AVG is one of many companies that provide free antivirus software to individual home users.
- To download this program, do a Google search for "Free AVG" and click on the link. Follow the directions on the web page to download and install AVG antivirus.
- Set your anti-virus software to automatically download anti-virus definition updates.
- Another good free antivirus is "avast!" ([www.avast.com](http://www.avast.com)).

### Scan your computer for viruses using AVG

- Set up your antivirus program to run in the background, and also run a full anti-virus scan of your hard-drive once a month.
- Before scanning, update your virus definitions.
- Click *Start* → *Programs* → *AVG [whatever version] Antivirus System* → *AVG [version #] for Windows* (or double click AVG icon on desktop) to begin a scan.

### Firewalls

Firewalls keep other people/other computers out of your computer while it is on the Internet. Good firewalls monitor both inbound and outbound Internet traffic. Firewalls are important even if you use a dial-up connection, but are *vital* if you use DSL, cable, or some other kind of always-on Internet connection. By monitoring outbound traffic, good firewalls can help foil programs whose purpose is to steal your personal information (SSN, credit card numbers) or which use your computer as a platform to attack others by keeping them from “phoning home”.

### Download a free firewall

- Do a Google search for “Zonealarm” and click the link.
- On the sidebar at the left of the web page, click “Home and Home Office” under the Products heading.
- A listing of various Zonealarm products will appear on the sidebar. Click the plain “Zonealarm” (as opposed to “Zonealarm Pro” and the like).
- Follow the on-screen instructions to download and install the free Zonealarm firewall
- Another good free firewall is Comodo (<http://www.personalfirewall.comodo.com>)

### Using Zonealarm

Once Zonealarm is installed, it will run in the background. When it detects a program trying to contact the Internet, it will display a balloon identifying the program and letting you “Allow” or “Deny” that program to access the Web. Clicking Allow lets the program access the Web once; clicking Deny blocks it once. To make your choice permanent for that program click the “Remember this setting” checkbox before clicking Allow or Deny.

### Download and use free anti-spyware tools

- Two good free anti-spyware tools are Spybot Search and Destroy and Adaware (NOT “Adware”; the second “a” is important!) These antispyware tools are active only when you run a scan, so they don’t prevent spyware from being installed. These two tools use different search methods and will detect and remove different spyware.
- To download these tools, Google search for them by name and follow the on-screen instructions.
- Scan your system for spyware at least once a month. Check for a program update before each scan to detect newly developed spyware.
- You may have to run Spybot more than once to eradicate spyware on your system.

## Why Defragment?

When you save a file or program to your hard drive disk, the computer system attempts to keep related files in the same physical location on the disk. As files are deleted or programs uninstalled the disk can become fragmented (blank areas or gaps are left). This can affect your computer's performance since programs have to access more areas of the hard drive to operate. The disk defragmentation tool will rearrange the computer's hard drive (close the gaps on the disk) to allow programs to run more efficiently.

## Defragment ("defrag") your hard drive

### Windows XP/2000

- Click *Start* → *Programs* → *Accessories* → *System Tools* → *Disk Defragmenter*
- Click "Analyze" and the program will indicate if your hard drive needs to be defragmented.

Example:

*Analysis is complete for: (C:)*

*You should defragment this volume.*

- Click "Defragment" to begin.

### Windows 95/98/ME

- Click *Start* → *Programs* → *Accessories* → *System Tools* → *Disk Defragmenter*
- Hard drive C: will be automatically selected in the drop box under "Please select which drive to defragment". Click OK to begin. If the drive is not very fragmented, the program will tell you not to bother defragmenting.

## Why run Disk Cleanup?

As you surf the internet, your web browser (Internet Explorer/Netscape etc.) stores copies of web pages to make the sites appear to load faster. These copies can take up space on your hard drive. The disk clean-up tool can help you eliminate these files along with any files you may have downloaded from the internet or files you may have sent to the recycle bin.

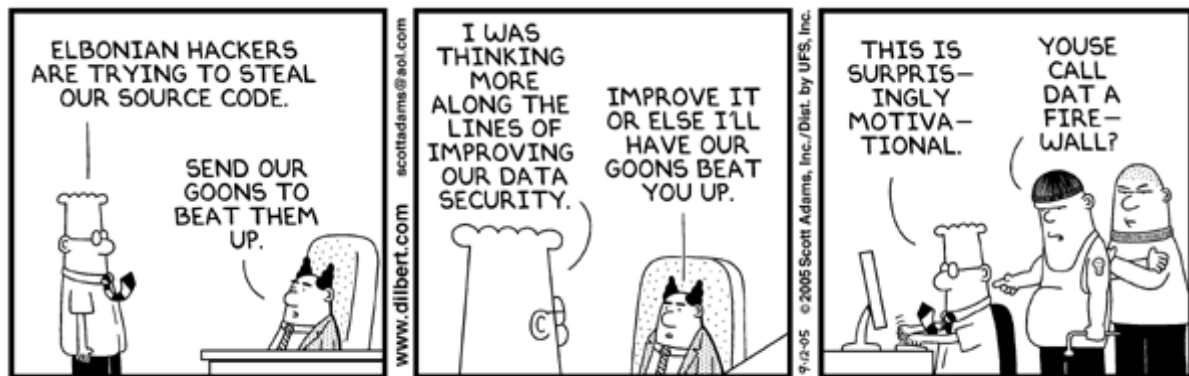
## Run Disk Cleanup

This process works in all versions of Windows.

- Click *Start* → *Programs* → *Accessories* → *System Tools* → *Disk Cleanup*
- Disk Cleanup will analyze your drive for unnecessary files. Once analysis is complete, you can select which categories of files to delete from your hard drive.
- The categories, Downloaded Program Files, Temporary Internet Files, and Temporary Offline Files are selected automatically. These categories are generally safe to delete without fear of losing a valuable file. Select "OK" to begin cleanup. Under "Are you sure you want to perform these actions" click "Yes".

Useful security links and info

- PC Magazine always has many articles on security issues
- Microsoft security for home users: <http://www.microsoft.com/security/home>
- Microsoft's Hotline for free virus and security patch related support in the United States and Canada: 1-866-PCSAFETY
- Symantec Security Response: [www.sarc.com](http://www.sarc.com) Symantec's Security site offers up-to-date information on the latest virus threats and their severity.
- The Security Tango: <http://www.securitytango.com/>
- Tutorial about viruses: <http://www.cknow.com/vtutor/>



© Scott Adams, Inc./Dist. by UFS, Inc.