

Tek
TIME



Computer/Internet Need to Know



Downloading

When downloading programs from the Internet, be sure that you trust the site from which you are downloading.

Software Categories

- **Commercial:** Mainstream software offered for download by big companies. Some are even free or free for home use. Most of it is priced in the "boxed software" range. The same software is usually available in stores as well as online.
- **Freeware:** Some freeware rivals the capability of *commercial* software, but usually it's smaller programs developed by individuals or *shareware* developers. Warning: freeware can be addictive -- it's free -- easy to download -- often excellent -- and there are thousands of programs to try. Many freeware programs are superb, but a few are written poorly. Freeware can also conceal "spyware," viruses or trojans and other parasites. Avoid problems by using your common sense and by following the rules for safe downloading listed below.
- **Shareware:** Usually modestly priced, intermediate in size and closer to commercial software in features. Some shareware is the best software written. The usual price range is \$10 to \$30. Often there's both a freeware and shareware version of the same software. The *freeware version* may run ads and/or limit functions. Shareware can often be used for 30 days or so on a free trial basis. After that time it will shut down unless you buy a registration code to keep it working.
- **Updates & Extensions:** "Filters," "codecs," "modules," updates, etc., augment or revise the capabilities of Windows and other programs, mostly browsers. They're usually free, and they are often offered when you click a link that won't work without the new software. They're often needed by Multimedia programs like Windows Media Player and RealPlayer. Be sure the site is trustworthy before you proceed though.

Downloading Rules

1. Use your common sense: Be very, very suspicious of any unsolicited invitation to download something wonderful or urgently important. These offers often appear as a flashy ad or popup window. Some will arrive as spam, some of it very clever, and often with an attachment.
2. Never download a file -- including pictures and music -- unless you know the source is trustworthy. Download software only from well-known companies (Microsoft, Symantec, Intuit, etc.) or from other trustworthy sources.
3. Never download a file via BitTorrent or other file-sharing networks.
4. "Google" it: Let's say the program is called Spyban. Go to Google and enter "Spyban spyware" (without the quotes) and see what you get.
5. Read the description and recommendations at the download site, or at the program's website. You don't want to install something that won't be compatible with your needs or your computer.

6. Before you install any software you download, make sure that you have a current backup of your documents and system.
7. Take precautions against viruses, trojans and adware. It's no longer a sure thing, but it's still a good practice to scan files for viruses, worms and other malware before you open them -- no matter what the source.

Viruses

A computer virus is a program that invades your computer system, hides there and makes copies of (replicates) itself. Viruses spread when you launch an infected application or start up your computer from a disk that has infected system files.

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected application is running. Turning off your computer or exiting the application removes the virus from memory, but does not remove the virus from the infected file or disk.

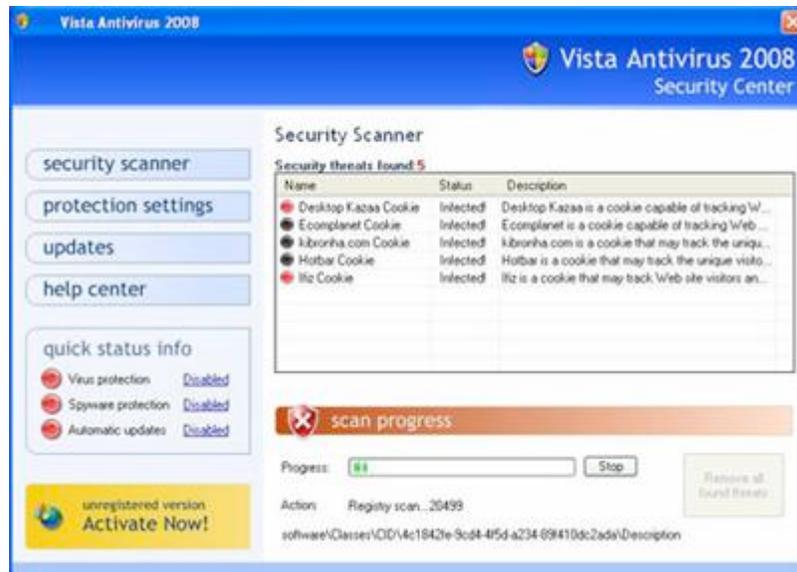
Some viruses are programmed specifically to damage the data on your computer by corrupting programs, deleting files or erasing your entire hard disk.

Many computer viruses turn out to be hoaxes or myths. Hoaxes are false alerts about viruses that don't exist. For a list of hoaxes check out Computer Virus Myths (vmyths.com/hmul/) and snopes (www.snopes.com/).

It is very important that you have an antivirus program on your computer. A few of the popular ones are:

- AVG – free (you can also upgrade to one that is charged for)
- Avast – free
- Norton
- McAfee
- SecureIT

You see a screen that asks if you want to remove a detected virus. You probably don't have a virus (yet). **DO NOT CLICK ON VIRUS POPUPS, NOT EVEN ON THE "X" CLOSE BUTTON.** This is commonly used by computer hackers to put a virus on your system! Use Ctrl+Alt+Delete and end the task.



The popup offers to scan your system or may start scanning on its own. It reports numerous fake viruses on your system. It may be a ploy to scare you into paying for phony antivirus software.

If you do not recognize the Antivirus software that is scanning, you will want to use the Ctrl+Alt+Delete and end the task.

Always scan your computer with your antivirus software after receiving anything like those mentioned above.

Spyware:

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information or changing the configuration of your computer, generally without appropriately obtaining your consent.

At best, these programs are an annoyance. At worst, they are a severe security risk. Aside from their intended purpose they can also have other effects. Since they run every time you boot your computer, they can cause slowdowns and software conflicts which can make your computer less stable.

You might have spyware or other unwanted software on your computer if:

- You see pop-up advertisements even when you're not on the Web.
- The page your Web browser first opens to (your home page) or your browser search settings have changed without your knowledge.
- You notice a new toolbar in your browser that you didn't want and find it difficult to get rid of.
- Your computer takes longer than usual to complete certain tasks.
- You experience a sudden rise in computer crashes.

Spyware is often associated with software that displays advertisements (called adware) or software that tracks personal or sensitive information. That does not mean all software which provides ads or tracks your online activities is bad.

Other kinds of unwanted software will make changes to your computer that can be annoying and can cause your computer to slow down or crash. These programs have the ability to change your Web browser's home page or search page, or add additional components to your browser you don't need or want. These programs also make it very difficult for you to change your settings back to the way you originally had them. These types of unwanted programs are also often called spyware.

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer. There are a number of ways spyware or other unwanted software can get on your system. A common trick is to covertly install the software during the installation of other software you want. Whenever you are installing something on your computer, make sure you carefully read all of the disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it may appear at the end of a license agreement or privacy statement.

Many kinds of unwanted software, including spyware, are designed to be difficult to remove. If you try to uninstall this software like any other program, you might find that the program reappears as soon as you restart your computer. If you're having trouble uninstalling unwanted software, you may need to download a tool to do the job for you. Several companies offer free and low-cost software that will check your computer for spyware and other unwanted software and help you remove it.

To deal with spyware, you can scan your computer regularly with free software programs like:

1. Adaware www.lavasoftusa.com
2. SpyBot Search and Destroy www.spybotsearchanddestroy.com
3. Malwarebytes www.malwarebytes.org

Be cautious when you receive a popup on your computer claiming that your computer is infected and to click on a button to scan your computer. These are most likely viruses and spyware programs trying to attack your computer.

Following these tips can go a long way toward helping you steer clear of the nuisances and dangers of adware and spyware.

- Stay away from dangerous neighborhoods – You can avoid some of the most dangerous spyware by not downloading software from certain sites.
- People who distribute pirated software also often distribute spyware and trojans.
- Just Say No – If a box pops up on your screen and asks you to click yes, or OK, only do so if you are actually trying to install software. Some Web sites try to trick you into installing adware or spyware.
- Ask for some ID – You can use a small program called Spychecker to find out if the software you are about to download contains spyware.

- Use protection – Run anti-virus software and keep it updated.
- Lock the door – A good personal firewall not only protects you from hackers, it will keep programs from contacting the Internet without your permission. Adware and spyware cannot function without sending information from your computer to the Internet.
- Get a checkup – There are several programs which can scan your computer for adware and spyware and remove it for you. No matter how careful you are, chances are very good that some spyware and adware will slip through your defenses.

Warning: When removing spy-files from your computer, there is a chance that those files may affect a program on your computer. Run spyware removal programs at your own risk!

How to prevent Viruses and Spyware:

1. Internet Safety – be a smart Internet browser. Don't download anything from websites you are unfamiliar with. Do not click on any popups. Those popups that say you are a winner – you didn't win a prize, but you may "win" a virus!
 - a. Use the Ctrl+Alt+Delete, then End Task. Under process, right click on iexplorer.exe, choose End Process Tree. This will close all your browser windows, including the potentially harmful one.
2. Suspicious Emails – an email may look questionable, either because
 - a. It is from someone you don't know
 - b. It is from someone you do know but the subject line or body appears suspicious. Sometimes there are links on the email.

If the email looks questionable, DON'T open it. Delete the email from your inbox and from the deleted items folder.

Tips N' Tricks

Web Address Shortcuts

When entering website addresses: instead of putting www.google.com in the address bar – type google and hold the CTRL+Enter. It will automatically convert to www.google.com. (Only works on the .com addresses.)

Domains:

.com = a commercial business
.edu = an educational institution
.gov = a governmental institution
.org = a non-profit organization
.mil = a military site
.net = a network site

Internet Explorer Shortcuts:

History – CTRL+H

CTRL+W – gets rid of current tab that is open

CTRL+tab – switches between tabs

Ctrl+T – New tab

Ctrl+N – New Window

F11 – Full Screen

Finding text on a Web page: Click Edit on the Menu Bar and select Find. Enter the text you are searching for and click Find.

Following a link while staying at the current page: Right Click on the link, Click Open in New Window or just hold down the Shift Key and click the link! This will open a separate browser window with the original page directly beneath it.

Shortcuts using your keyboard

Home takes you to the top of page (or beginning of line in some programs),

End takes you to the bottom of the page (or end of line in some programs).

F1 - Help

Ctrl+A – Select All

Ctrl+B – Bold

Ctrl+C – Copy

Ctrl+D – Delete

Ctrl+F – Find

Ctrl+G – Go To (Excel)

Ctrl+I – Italic

Ctrl+M – New Slide (Power Point)

Ctrl+N – New file

Ctrl+O – Open

Ctrl+P – Print

Ctrl+S – Save

Ctrl+U – Underline

Ctrl+V – Paste

Ctrl+X – Cut

Ctrl+Y – Redo

Ctrl+Z – Undo

Ctrl+Home – beginning of document

Ctrl+End – end of document

Win key – opens start menu

Win key+D – Brings the desktop to the top of all other windows.

Win key+M – Minimizes all windows

Win key+Shift+M – Undo the minimize done by Winkey+M and Winkey +D



(Windows Key or Win key)

To Highlight: Shift arrow – highlights, Shift+end - highlights to end of row, Shift+page up or page down – highlights page up or page down.

Hold Shift and Select first and last item for a Sequential Group

Hold Control and Select each item for a Non-Sequential Group

F7 Spell Check

Shift+F7 Thesaurus

Printing what you want: Select whatever you want to print (by holding your mouse button down and dragging over what you want to print). Once you have selected what you want to print, click File on the Menu Bar and then Print. In the Print Range, put the dot to the left of “Selection” and then click the print button.

Avoiding Spam:

Junk Email: spam is a slang name for unsolicited or junk email. One of the most popular methods for a spammer to obtain and use your email address is actually a direct result of how you, your friends and your relatives forward email to one another. When email is forwarded utilizing the “To” field or the “Cc” field, everyone can see the other recipients – and after being forwarded multiple times email can contain hundreds of email addresses. One of those recipients could be a spammer who collects email addresses and not only sends you spam but sells your email address to other spammer! Below is a tip on how to avoid this situation and encourage the people you correspond with to do the same!



If you do not see “Bcc” Click on Create Mail on the New Message, click on View and Select All Headers. Now the “Bcc” area will show up all the time. In Windows Live Mail – Click on view and click Cc and Bcc.

What is “Cc” and “Bcc”? “Cc” is for Carbon Copy and “Bcc” is for Blind Carbon Copy. You should only place multiple email addresses in the “To” field when each of the recipients knows each other. Utilize the “Cc” field when sending an email meant for one person but carbon copying others using “Cc.” The “To” person is able to see who else got a copy of the message. The “Bcc” is used to send messages to a group of recipients in a manner that prevents the recipients from seeing who else got the message. This is especially useful when forwarding messages to a group of people without spreading their email addresses across the world.

When forwarding emails, remember to delete the unnecessary information – such as email addresses and etc.

I can't open some attachments:

What is the file extension – do a search for a free viewer

Some examples are:

.doc or .docx – Microsoft Word

.xls or .xlsx – Microsoft Excel

.mdb – Microsoft Access Database

.pdf – Adobe Acrobat Portable Document Format

.pps or .ppt - .pps Microsoft Powerpoint Slide Show, .ppt Microsoft PowerPoint Presentation

.pub – Microsoft Publisher

What is the difference between http and https:

http – Hyper-Text Transfer Protocol

https – Hyper-Text Transfer Protocol Secure

Programs running in the background

1. Click Start
2. Run (if using earlier version of Windows)
3. Type “msconfig” (without the quotes) in the dialog box
4. Press enter
5. Click the start up tab
6. Uncheck what you don't want started – if you do not know what the program does – you should search the internet before disabling it.
7. Click OK – you will get a popup asking you to restart your computer or exit without restarting. If you choose not to restart the changes will occur the next time you reboot. I recommend you choose reboot.
8. When you do reboot you will see a popup on your screen saying you are in “Selective Startup” mode. If you don't select the highlighted box this will appear on every reboot and add an MSConfig entry to the list of start-up programs. This can be seen under the "General" tab and is perfectly normal if you've disabled an entry. **Warning:** If you subsequently decide to choose "Normal startup," all disabled items will be re-enabled
9. Some disabled items may disappear from MSConfig when you re-start Windows.

Why your computer is running slow

Your computer requires a certain amount of “resources” in order to perform well.

- **System Resources** – at a very basic level, computers need a Central Processing Unit (CPU), a motherboard, memory, storage and an operating system to function. The capacity and available size and speed of these pieces of the puzzle are largely responsible for how well the computer will be able to perform. These are referred to as a computer's “System Resources.”
- **Disk Space** – The disk space of the hard drive is where the operating system, programs and stored files reside. If disk space runs dangerously low, the system may reach a point where it is no longer able to function. In Microsoft Windows systems, you can find out how much space remains and is in use in “My Computer” or “Computer” from within the

Start menu. Right click on the hard drive (the main drive is normally labeled “C”), and choose “Properties.” This will show the “Used Space,” “Free Space” and “Capacity” of the drive in both text and pie-chart form. If you’re running short of space, it may be time to remove some files or uninstall some programs.

- **Memory** – Random Access Memory (RAM) is often referred to as “volatile” memory, because it is wiped clean when the system is shut down or restarted. This invisible temporary storage space is where instructions sent to the system are stored, and where programs and much of the operating system operate from. If you use the “Copy” function to copy and paste something (e.g. a word, sentence, paragraphs, photos), it is stored in this temporary memory space. If you are actively using several programs at once, more of the memory space is used up.

