Virus

What is a virus?

It is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.

It can also be defined as a set of codes written to cause mischief or damage to a computer system. Most viruses do damage, whether to your files, your registry, or even your hardware. Viruses are hard to detect, easy to propagate, and difficult to remove. Your computer can pick up a virus when you copy a seemingly normal file from a diskette or download it from the Internet.

What can you do to prevent your computer from getting infected from virus?
(List of to do)

- Make sure that you have a reliable **anti-virus software** installed in your computer that can be used to scan your removable and non-removable drives for infected files.
- **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program (normally a **firewall**) checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with your own anti-virus software.
- **Update your anti-virus software regularly.** Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the products virus signature files. You may also need to update the product's scanning engine as well.
- **Back up your files on a regular basis.** If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.

- When in doubt, **always err on the side of caution** and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats.

What should be avoided to prevent your computer from getting infected?
(List of Don't Do)

- **Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
- **Do not open** any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
- **Do not open** any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there always save the file to your hard drive before doing so.
- **Delete chain emails and junk email.** Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
- **Do not download** any files from strangers.

Spam

What is spam?

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services.

Mail spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses.

What can you do to prevent spam from spreading?
(List of to do)

- **Use a spam filter:** One to try is SpamBayes for Windows , (. Another is Mailshell, which is available on TechSoup Stock. (Visit the Mailshell page for details).

- **Use complicated e-mail addresses:** Spammers' software will look for the easy and obvious addresses first.

- **Before you join a list:** Make sure the list owner or Web master will not sell your address.

- **Preview your messages:** Before you open them. Outlook (and many other e-mail clients) let you use a preview mode to peek at the contents of a message before you actually open it. To do this in Outlook, go the View menu and select Preview Pane. Instead of double clicking a message, click it once to select it and you'll see the message displayed in the Preview Pane.

- **View a message's headers to see if a sender's e-mail address is valid:** In Outlook, you can do this by right-clicking the message and selecting Options. (Note that full message headers are usually hidden by default in most e-mail clients.) In the header information you can see if the return address is indeed the address it claims to be.

- **Read all your messages as text:** That means turning off the ability to view pictures, HTML, movies, and formatted text, which most spam contains.

What should be avoided to prevent spam from spreading?
(List of Don't Do)

- **Never, ever reply to a spam message:** This includes buying a product that is for sale or clicking the often-misunderstood "unsubscribe" link, which actually informs your spammer that you exist. If you can tell from the subject line that a message is spam, don't open it, and delete it. Spam subject lines usually promise you a better sex life, a more youthful appearance, prescription drugs without a doctor's approval, love, thicker hair, or a better mortgage rate. They also use attention-demanding punctuation, such as exclamation marks or all caps.

- **Don't click *any* links in a spam e-mail:** Spammers often have multiple, unique pages on their sites. Often times, when you click a URL in a spam message, this tells the spammer that you -- and only you -- received the message they sent.

- **Don’t forward an e-mail from someone you don’t know to a list of people:** You remember those “forward this e-mail to 20 of your friends” messages? They are perfect for spammers to harvest e-mail addresses, even if the sender of the original e-mail did not have this intent. These types of sign-and-forward e-mails often appear in the form of a petition -- and they don’t work.

- **Don’t use your home or business e-mail address:** when you register on a Web site or in a group. If you must sign up for services, want to receive more info, register for newspapers or domains; use a free e-mail address from a site like Yahoo to create an address especially for that purpose. This also goes for posting to the Web, in a listserv, newsgroup, on a contact page for a Web site, or on a resume that is posted on the Web.

- **Don't use Hotmail/AOL/MSN as your primary mail provider:** That's because spammers often flood common usernames on widely-used mail systems (e.g. dave23, dave24, etc.). If your main e-mail address is currently on Hotmail, MSN, AOL, Yahoo or any other major national mail provider, you may want to think about getting a less visible e-mail address to minimize your exposure to spam. (for example, Excite, Rediff)

- **Never use your e-mail address as your screen name:** in chat rooms. It will give spiders or human e-mail harvesters an absolute yes to a questionable e-mail address.

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.

Spyware can 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.

What should be done to combat Spyware?

Do’s

- Use a firewall all the time

  Most computers that run Windows already have a firewall in them and needs to be set to on. Other firewalls like **Zone Alarm** are also very popular. This can keep hackers from getting into your computer and downloading Spyware to get your information. A firewall can help block viruses and worms for getting into your computer. It will cause the system to ask for permission to block or not block connection requests. A firewall can also create a security log that will record successful and not successful connection attempts on your computer.

- Update your software regularly

  You always want to make sure all your Windows security systems are up to date. All you need to do is go into your setting and make sure you have checked the box for automatic updates. This will ensure that your computer is equipped with the latest of Defense Systems.

- Adjust Internet Explorer security settings accordingly.

  This will allow you to decide how much or in the case of Spyware, how little information you are willing to take from a web site. You want to keep your Internet zone setting to at least medium for it to be effective.

- Surf and download more safely

  Be sure you always know and trust the sites you are downloading from. Even the most seemingly harmless downloads can contain Spyware.

What should be avoided to prevent your Computer from getting infected by Spyware?

Don’ts

- Don’t download anything you aren’t sure of. The best defense from Spyware is not installing it in the first place.
- Never give out your private information like PC IP address, PC Name, OS to strangers. Else you may become an easy target for the Spyware.
- Never ever disable your real time protection provided by anti Spyware and firewall if asked to do so while downloading from an unsafe site. Sometimes, hackers fool people by displaying messages like “Please disable your firewall settings to proceed with your free download”. The moment you agree, it’s just too late because the Spyware is already in your system. Spyware may take just a few seconds to infect a PC.