PROTECTING YOURSELF FROM VIRUSES AND SPYWARE

Why do people write viruses or spyware?

Viruses are typically written for one of the two reasons below.

Monetary Gain

Many viruses come in the form of programs that get installed without your permission and then claim to offer some function such as Virus Protection, some utility that claims to make your computer faster, or will get you coupons that will save you money. These are all typically scams that intend to use your computer as a zombie to perform attacks on other computers, send large amounts of spam email, and other devious things all without your knowledge. No legitimate software company will solicit you through a program that installed itself without your permission!

Vandalism

Some viruses literally do nothing more than wreak havoc on your computer. The answer to why someone would want to do such a thing is a combination of Vandalism, Egotism and Malice. Viruses are almost impossible to trace back to the author so these people want only to harm your computer for their own sadistic reasons.

General Policies

If you use a cable or DSL internet service, install a router. A router acts as a hardware firewall and provides additional protection by sitting between your computer and the internet. Use a router in conjunction with your software firewall for additional protection.

Don't let kids on the internet on your work system! For home systems, monitor and educate your children. Talk to your kids about their internet habits. Keep the computer in a public room so you can keep an eye on what they're doing and setup a limited user account for kids or guest access.

Messaging (E-Mail, Instant Messages, Social Networking Messages)

Don't automatically trust that instant messages, email messages, or messages on social networking websites are from the person they appear to be from. Even if they are from someone you know, contact the person before you click the link to ensure that they intended to send it.

Don't participate in Email forwarding of non-work related material. Email attachments and forwards are a very common way to get infected, even if you receive an email with a link or attachment from someone you know it can still harm your computer.

Never open unsolicited email attachments. Email is one of the main methods of spreading viruses. If you don’t know who the email is from, delete the entire message right along with the attachment.

Viruses come with some very nasty messages to trick you into opening the attachments. Examples: "Your email account has been cancelled, see attachment for details", “Your UPS package has been delayed, please open the attachment for more details” or “Urgent Reply Needed”. Be careful with all anonymous and impersonal emails that encourage you to open an attachment, for instance, a funny picture, video or link to click. When in doubt, delete the email!

Avoid clicking “phishing” emails, which are messages that purport to be from a bank, UPS, a credit card company, etc. and attempt to scare the recipient into clicking a link or opening an attachment.

PROTECTING YOURSELF FROM VIRUSES AND SPYWARE

Whenever you get a scary email from a bank or other institution, visit the company's official website, rather than clicking the link

Browsing/Surfing/Web Site Policies

Never click "Agree" or "OK" to close a browser window. Instead, click the red "x" in the corner of the window or press ALT + F4 on your keyboard to close a window.

Be careful with social networking. Social networking sites like Facebook, MySpace, and Twitter are generally safe but people can post links and advertisements that will direct your browser to a potentially bad site where you can then become infected.

Search safely. When using online search engines such as Google be sure to scrutinize your search results and read the information displayed, don't just click on the first link that you see.

Visiting Adult, Free game or gambling sites pose a high risk of infection.

Do not download software or Add-ons from web sites that you are unfamiliar with. This includes sites such as "Facebook" and "Myspace".

Do not click on sudden pop-up windows while browsing the internet.

Stay away from file-sharing sites. Sites that distribute illegal software, music, or movies are known to be riddled with viruses. This includes torrents or other forms of P2P activities. File Sharing Programs such as: Limewire, Kazaa, Frostwire, Morpheus, uTorrent, Ares for example. Staying away from these sites and programs is in your computer's health's best interest, as well as a good way to avoid being sued for copyright violation.

Unless the window originates from your own antivirus program, avoid clicking on pop-up windows that alert you to "infections" on your computer. Rather, use the X in the upper right of the window to close it out, or hit CTRL+ALT+DEL and use Task Manager to terminate your browser.

Avoid sites that excessively promote free giveaways. Anytime you see offers for special contests, free music downloads, or free software add-ons, be aware that spyware, viruses, or other malicious software may be weaseling into your computer on the backs of these downloads.

Software/Downloading Policies

The best defense against spyware and other unwanted software is not to download any software in the first place. If you need software installed, enter a ticket into our system so that we can review it before it is installed.

Don't download anything for free. Free pictures, music, ring tones, and screen savers are usually just vehicles for viruses and spyware.

Do not install unknown codecs: A codec enables your computer to properly play video or audio. A common virus infection ploy is to put a popular video out which might play back without the sound accompanied with a note to download a 'special' codec to get the sound. Needless to say, the codec is genuine 'special' since it contains a virus.

Never purchase software offered through emails. Those special bargains may come with an additional unwelcome bonus in the form of a virus.