Keewatin Academy
OF INFORMATION TECHNOLOGY

www.kait.ca

Keewatin Career Development Corporation

CISCO Networking Academy

IT Computer Security

Why Security Is Important

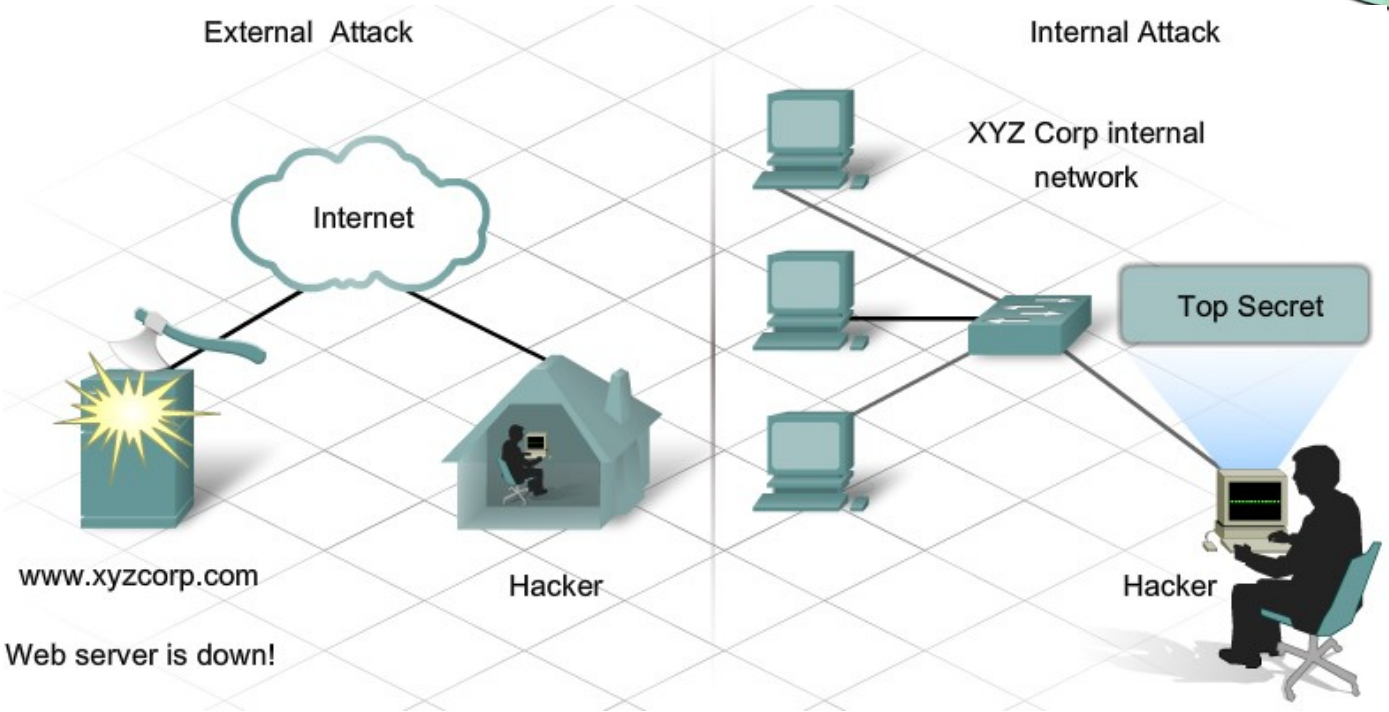
- Keeps data and equipment functioning
- Lack of security can expose confidential information and reduce network resources
- Can degrade performance of a network
- Keeping yourself current with today's computer security threats will give you a foothold into prevention techniques
- Will keep your school/organization's data safe and your personal information safe

Types of Security Threats

Keewatin Academy
OF INFORMATION TECHNOLOGY

- Two types of threats to computer security:
- **Physical** – stealing, damaging, or destroying equipment such as workstations, servers, switches, routers, wiring, etc.
- Ex. Theft of laptop from desk, cutting networking wires in server room/closet
- **Data** – removal, corruption, denying acces allow unauthorized access to, or stealing confidential or private data
- Ex. Virus/Worm/Trojan Attacks, Spam, Cracking network security, Spyware

Types of Security Threats



- Unauthorized users attempting to gain access to your computer or computer network
- Can happen as an Unstructured or Structured Attack

- An Individual Working From Within an Organization
- Some unintentional threats such as an employee opening an e-mail attachment and spreading a virus at work

Virus, Worms, & Trojans

Keewatin Academy
OF INFORMATION TECHNOLOGY

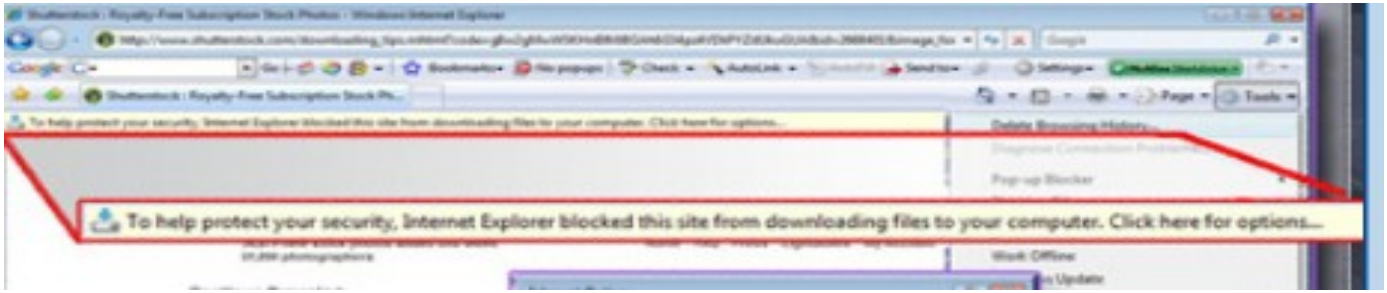
- A computer **virus** is software code that is deliberately created by an attacker. Viruses may collect sensitive information or may alter or destroy information.

- A **worm** is a self-replicating program that uses the network to duplicate its code to the hosts on the network. At a minimum, worms consume bandwidth in a network.
- A **Trojan horse** is technically a worm and is named for its method of getting past computer defenses by pretending t be something useful.

- Some viruses can record keystrokes and report them back to the virus author. This type of virus is called a **keylogger** and can be dangerous if it captures confidential information.
- Anti-virus software is designed to detect, disable, and remove viruses, worms, and Trojan horses before they infect a computer.

Web Security

- ActiveX
  - Microsoft Technology: Controls interactivity on web pages



Internet Explorer prompting for your permission to install an ActiveX applet or to Download a File

- Java
  - Allows applets to run within a browser
  - Ex: a calculator or a counter
- JavaScript
  - Interacts with HTML source code to allow interactive web sites
  - Ex: a rotating banner or a popup window

Social Engineering

- **Social Engineering** refers to the ability of something or someone to influence the behaviour of an individual or a group of people.
- **Pretexting** is a form of social engineering where an invented scenario (the pretext) is used on a victim in order to get the victim to release information or perform an action. The social engineer usually has a tidbit of information about the victim before they call to help gain their trust.
- **Phishing** is when an individual pretends to represent a legitimate outside organization by internet, e-mail, phone, in-person or by other means of communication.
- **Vishing** (Phone Phishing) is relatively new where an unsuspecting user is sent a voice mail instructing them to return a call to their banking service at a bogus toll-free number left on the voicemail. They are prompted to enter in information such as bank card information

Adware, Malware, Spyware

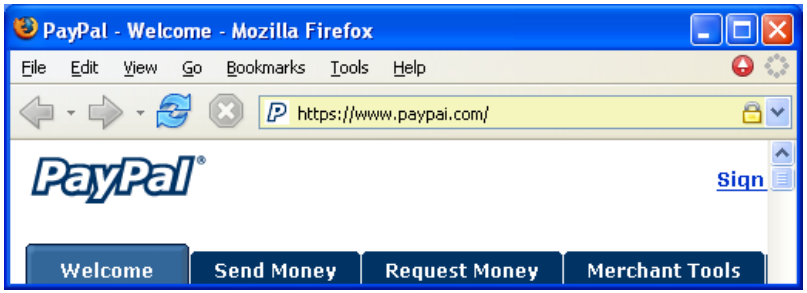
- **Adware** displays advertising, usually in a popup window.
- **Grayware or malware** is a file or program other than a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information.
- **Spyware**, a type of grayware, is distributed without any user intervention of knowledge. Spyware monitors computer activity then sends the information back to the organization responsible for launching the spyware.
- **Tracking Cookies** track a user's browsing behaviour and can allow an individual to customize their website experience or preferences. Some cookies can be harmful if they are spyware "super" cookies or data miners. They may collect more personal information. Spyware programs can remove these.

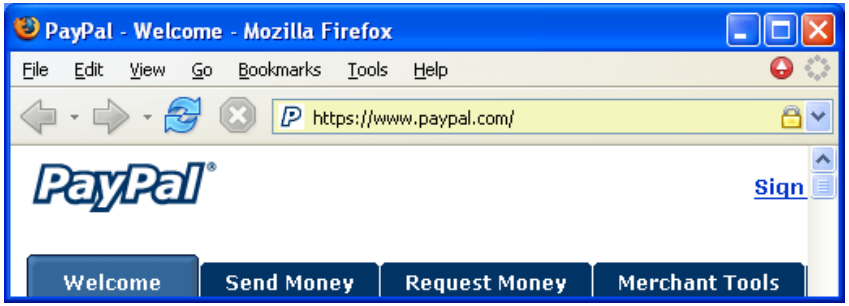
Spam and Popup/Popunders

- **Spam** is unsolicited email that can be used to send harmful links or deceptive content.
- **Popups** are windows that automatically open and are designed to capture your attention and lead you to advertising sites.
- **Pop-unders** are windows that appear but hide behind your currently opened windows. When you close the windows you are using, you will see the pop-under which is usually a lingering advertisement. These may be dangerous as well because they can contain a tracking cookie that will follow your browsing habits

Spoofing

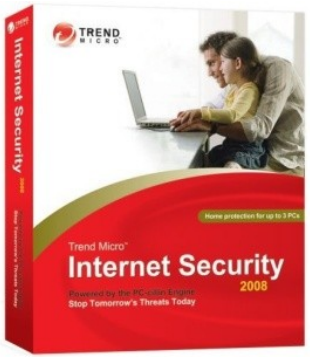
- **Spoofing** is when an individual or program mimics someone or something to deceive a target into revealing information or following misleading instructions.
- For example, an e-mail instructing you that your PayPal account is going to be closed unless you "Click on this link" to restore your account access may direct you to a 'look-a-like' website.
- Can you tell the difference between these two websites?
- The top one is fake and uses the website address www.paypai.com

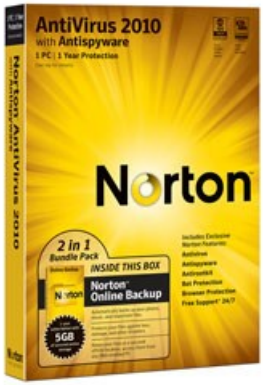


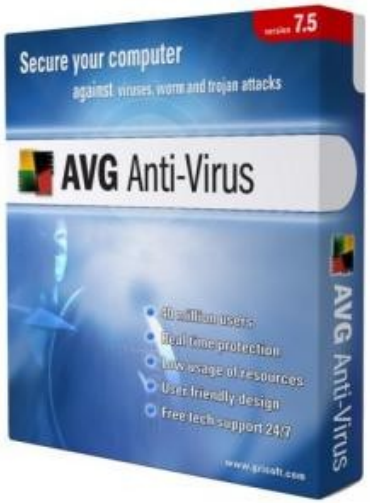


Combating the Treat

- Anti-Virus
  - There are various anti-virus software programs out there, but which ones are useful and which ones may cause more problems than they're worth? You should utilize tech websites to determine which tools bench technicians find useful in combating the computer security threats of today.







Combating the Treat

- Anti-Spyware
  - With spyware threats being as bad or worse than virus threats, we now need to protect our computers from this additional threat. Finding the appropriate software that fits your needs is crucial. Something that's efficient and easy to use is hard to find in the spyware game. You also need to be careful that you are not downloading a Spyware removal software that is actually spyware itself. It fakes threats and removal of those threats to keep you under the illusion that you are 'safe' from those threats.

Spyware Search & Destroy

Malwarebytes

- Like Anti-virus, read technical articles and find out which spyware removal software is free and efficient at removal of security threats.

Combating the Treat

Keewatin Academy
OF INFORMATION TECHNOLOGY

- Pop-up and Pop-under Blockers
  - Browsers now usually come equipped with their own pop-up blocker. You can configure those settings in the browser's options.
  - Be sure that you do not have multiple pop-up blockers running on your system as their overlap may pop-up legitimate pop-ups that are required to navigate some websites.
  - Also, do not disable or minimize the settings of your pop-up blocker too much or you may end up bypassing the effectiveness of the program and subject yourself to an overload of pop-ups and pop-unders.

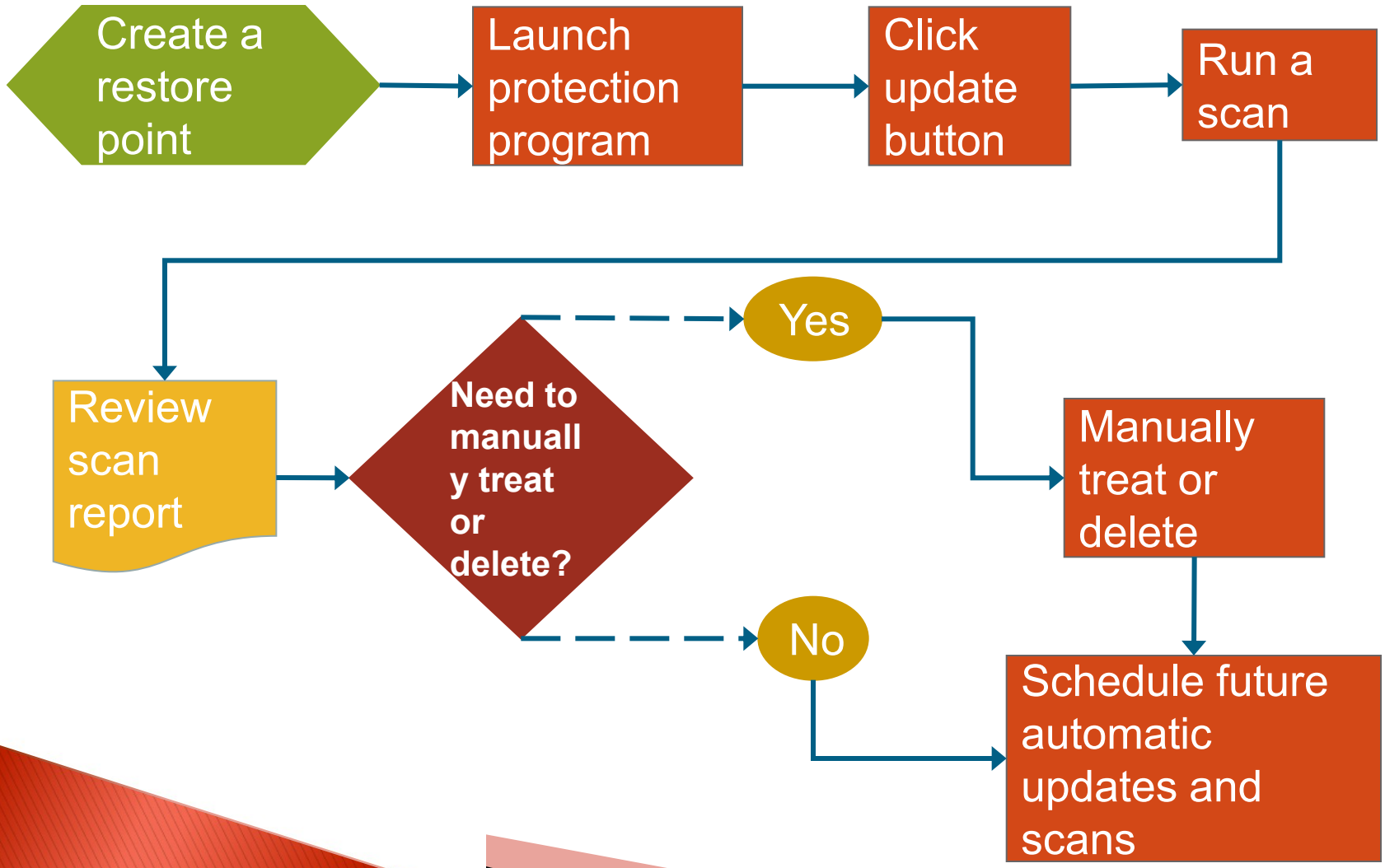
Combating the Treat

- Software Patches and Updates
  - Part of the combating the threat is prevention. Prevention of the threat or prevention of future threats. In order to do this effectively is to patch any vulnerabilities in the operating system and the software on your computer.
  - Each program may have its own updater that you need to click on once in awhile. For other programs you may need to **visit the vendor websites** to check for any available software updates.

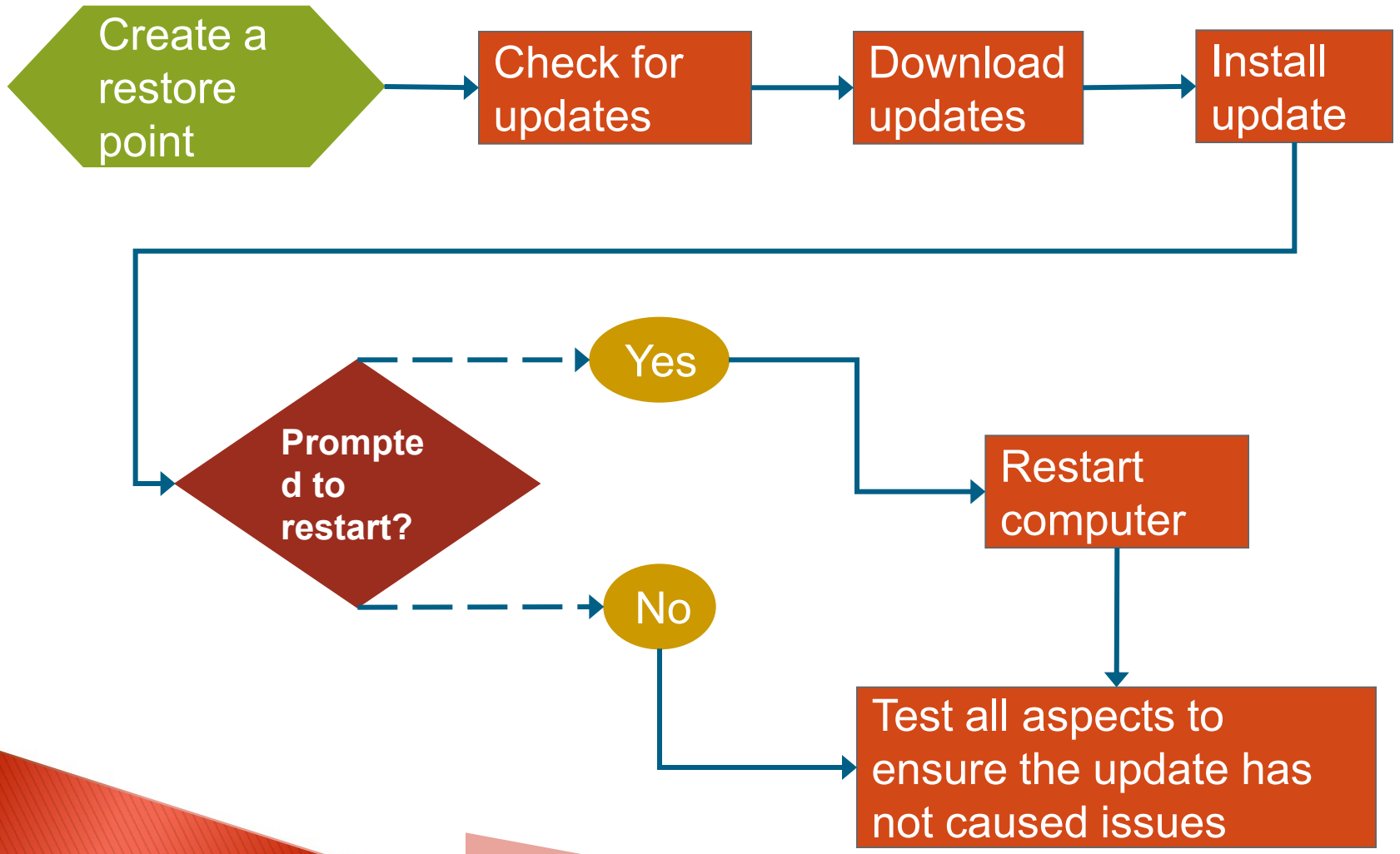
Microsoft Updater

Software Update or Patch

Updating Protection Programs



Operating System Updates and Patches



Additional Resources

- PC Mag's Security Watch Articles
  http://blogs.pcmag.com/securitywatch/
- How Stuff Works: The Computer Security Channels
  http://computer.howstuffworks.com/security-channel.htm
- Snopes.com: Virus Hoaxes & Realities
  http://www.snopes.com/computer/virus/virus.asp
- PC World: Security
  http://www.pcworld.com/topics/security.html

For an excellent site for security guides and to see if one of your processes is a virus, you can search at:

- Norton (Symantec) Threat Explorer
  http://www.symantec.com/norton/security_response/threatexplorer