

Viruses, Spyware and Scams: Info to keep you safe.

Viruses - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

E-mail viruses - An e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. ****We never send emails from Barnard Team****

Worms - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

Trojan horses - A trojan horse program is a harmful piece of software that is disguised as legitimate software. Trojan horses cannot replicate themselves, in contrast to viruses or worms. A trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is useful. To complicate matters, some trojan horses can spread or activate other malware, such as viruses.

Backdoors - A backdoor is a secret or undocumented means of getting into a computer system. Many programs have backdoors placed by the programmer to allow them to gain access to troubleshoot or change the program. Some backdoors are placed by hackers once they gain access to allow themselves an easier way in next time or in case their original entrance is discovered.

Phishing – Phishing is a kind of spam email looks like it comes from a bank or some other trusted company or institution. The email claims to need personal information to update your account information. A link in the email will direct you to a legitimate-looking website that asks for your password, account number, or credit card information. There are a number of “URL spoofing” techniques including using

- (1) an IP address (eg <http://192.168.1.1/>), which relies on the user ignoring the URL completely or being confused by its complexity;
- (2) a completely different domain, which relies on the user not looking at the URL at all;
- (3) a plausible-sounding but fake domain (eg <https://www.paypayl-secure.com>), which relies on the user not knowing the exact domain name;
- (4) a visible-to-the-eye letter substitution (eg <https://www.paypa1.com>), which relies on the user not looking too closely at the URL's individual letters;
- (5) an invisible letter substitution, which is almost undetectable;
- (6) an address with a username that looks like a domain name (eg <http://www.paypal.com@www.evil.com>), which also relies on the user not knowing exactly what the domain should be.

Browser Hijacker – A hijacker is a program which changes some settings in your browser. Hijackers can be removed with a program called HijackThis!

* Browser Hijackers usually changes users start page. And most often its hard to change that start page to another page or blank page. After restart of the computer browser Hijackers sets their own page again. These changed start Pages usually leads to pay per click sites, where owners of browser hijacker earns money for every click or to the porn sites where owners also get paid for clicks;

* Browser Hijackers changes users 'search' page. All queries are passed to pay per click sites, where owners of browser hijacker earns money for every click or to the porn sites where owners also get paid for clicks;

* Browser Hijackers transmits all web pages user visits to the owners of the parasites.

Common Signs that you have a virus:

(Any of these symptoms could also point to problems with the operating system, software, hardware, adware, and/or spyware.)

- * Your computer is noticeably slower than it used to be, or seems to be busy doing something else.
- * Your network connection is slower than usual, or seems really busy (this can just as often be the network or ISP).
- * Your computer freezes or crashes repeatedly.
- * Your antivirus program stops running without an error message.
- * You notice strange processes running on your computer (this assumes you know what the usual processes are).
- * Folders on your computer start sharing themselves across the network.
- * Files start appearing on your hard drive, perhaps in multiple locations.
- * Microsoft Word or Excel suddenly start warning you about macros existing in your documents.
- * You can't access certain web pages like Symantec or Windows Updates, or you can't run LiveUpdate.

Antivirus Software - Antivirus software is a type of application you install to protect your system from viruses, worms and other malicious code.

Anti-virus software typically uses two different techniques to accomplish this:

- * Examining (scanning) files to look for known viruses matching definitions in a virus dictionary

* Identifying suspicious behavior from any computer program which might indicate infection

Most commercial anti-virus software uses both of these approaches, with an emphasis on the virus dictionary approach. Remember that your Antivirus software is only as good as its definition files! If you don't update your definitions (LiveUpdate), scans won't catch everything.

SYMANTEC TUTORIAL

Scheduled Scans> New Scheduled Scan

Configure> Enable Auto-Protect

File>Schedule Updates

You have a virus: what should you do?

View>Quarantine

Shows a list of all the viruses that Symantec found but could not delete. Make a list of all threats, including their name, filename, and original location. The Symantec website has instructions on how to delete all viruses it finds. Sometimes there is a patch you can download and run that will automatically get rid of the virus.

Spyware - Spyware is a piece of software that collects and sends information (such as browsing patterns in the more benign case or credit card numbers in more serious ones) on users. They usually work and spread like Trojan horses. The category of spyware is sometimes taken to include adware of the less-forthcoming sort.

Adware - Adware or advertising-supported software is any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen.

To get rid of adware and spyware, download AdAware and Spybot from the resnet website. AdAware and Spybot do not run on their own, you should run them once a week or if you notice more popups.

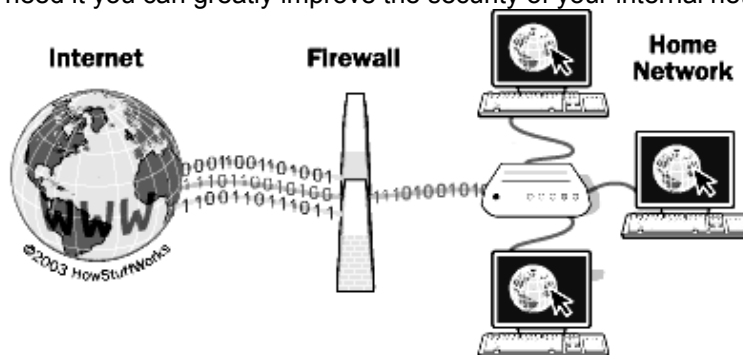
One way to prevent adware and spyware is to use a browser with pop-up protection like Mozilla or Mozilla Thunderbird.

<http://www.mozilla.org> You can also download software that blocks pop-ups.

Be aware that if you choose to block pop-up windows, you will need to tell your browser to accept them from websites like ebear or else they won't work correctly. To block unwanted pop-ups in Mozilla go to Edit>Preferences and select Privacy & Security/Popup Windows and check "Block unrequested popup windows"

Windows XP Service Pack 2 installs a popup blocker for Internet Explorer automatically.

Firewall - Basically, a firewall is a protective barrier between your computer, or internal network, and the outside world. Traffic into and out of the firewall is blocked or restricted as you choose. By blocking all unnecessary traffic and restricting other traffic to those protocols or individuals that need it you can greatly improve the security of your internal network.



Firewalls use one or more of three methods to control traffic flowing in and out of the network:

* Packet filtering - Packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.

* Proxy service - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.

* Stateful inspection - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Test your firewall/the security of your connection:

-ShieldsUp!

<http://www.grc.com/x/ne.dll?rh1dkyd2>

-LeakTest

<http://www.grc.com/lt/leaktest.htm>

Compiled by Esther White for
Academic Technologies
Barnard College