Internet Defenses

DEFENSES THROUGH APPLICATIONS

If you wish to use the Internet safely you could simply control the infiltration of bad code into your system by using the control mechanisms built into your Internet applications. These controls include popup blockers, spam filters and the security settings in your e-mail applications.

Circle your wagons!

POPUP/POPUNDER BLOCKERS

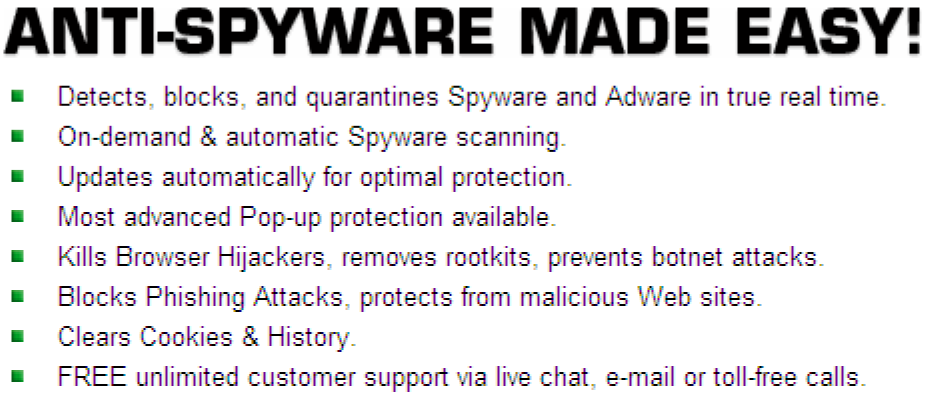
When an advertisement opens in a new window on top of (popup) or under (popunder) your existing web window it is often unwanted and, in the case of a popunder, not noticed until hours later.

Popups or popunders could contain adware, spyware or viruses and when the popup/popunder is clicked on or even mouse-overed your computer could get infected.

OPTIONS

To prevent infection you have to stop popups. Here are your options:

Option 1: Buy a popup blocker.



ANTI-SPYWARE MADE EASY!

- Detects, blocks, and quarantines Spyware and Adware in true real time.
- On-demand & automatic Spyware scanning.
- Updates automatically for optimal protection.
- Most advanced Pop-up protection available.
- Kills Browser Hijackers, removes rootkits, prevents botnet attacks.
- Blocks Phishing Attacks, protects from malicious Web sites.
- Clears Cookies & History.
- FREE unlimited customer support via live chat, e-mail or toll-free calls.

Option 2: Change your browser settings to control popups.

Click on the image or link below to see how this is done.

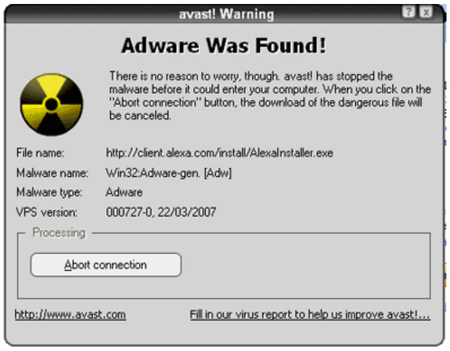
http://coursecontent.ntc.edu/CIT/husband/pois/lp3/BlockPopups/BlockPopups.html

WHAT SHOULD YOU DO IF YOU GET A POPUP?

Avoid touching it! Right-click the popup in the taskbar and close it. You can also terminate the process in your Task Manager (recommended).

Click on the image or link below to see how popups can be killed using the Task Manager.

If you get popups even when you are not on the Internet or when you are on a web site that does not have popups, then you have adware and/or spyware. This will have to be removed by an adware/spyware removal tool.



avast! Warning

Adware Was Found!

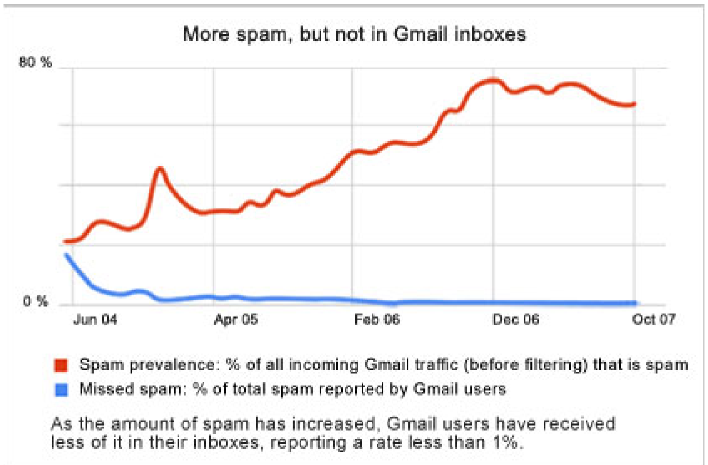
There is no reason to worry, though. avast! has stopped the malware before it could enter your computer. When you click on the "Abort connection" button, the download of the dangerous file will be canceled.

File name:	http://client.alexa.com/install/AlexaInstaller.exe
Malware name:	Win32:Adware-gen. [Adw]
Malware type:	Adware
VPS version:	000727-0, 22/03/2007

E-MAIL SECURITY SETTINGS

Spam is the most prevalent concern regarding e-mail. Spam can be filtered at a higher level such as the SMTP server that receives your email.

Gmail, for example, is quite good at blocking spam before it reaches your inbox.



As the amount of spam has increased, Gmail users have received less of it in their inboxes, reporting a rate less than 1%.

Source: http://gmailblog.blogspot.com/2007/10/how-our-spam-filter-works.html

The e-mail that you receive, even after filters are enabled, could still contain badware. There are additional settings that can be made to minimize the risk of exposure.

Click on the image or link below to get more information.

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/m31-emaildefenses.html

DEFENSES THROUGH BROWSER SETTINGS

Because of the browser's close proximity to the Internet, it stands to reason that it should have many ways of configuring security and privacy settings to protect you. Some of the browser’s settings that you need to become familiar with are security settings, security zones, and restricting cookies.

ADVANCED SECURITY SETTINGS

In IE 8.0 there are 19 advanced security settings. Many of these settings are enabled by default.

Click on the image or link below to get more information.

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/m32-AdvancedSecuritySettings.html

SECURITY ZONES

Security configuration settings are not statically set for all Internet access and to all web sites. You may have a need to restrict certain sites and not restrict others. Internet Explorer 8 gives you 4 zones by which you can fence in general Internet access and even specific sites.

Click on the image or link below to get more information.

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/m32-Zones.html

RESTRICTING COOKIES

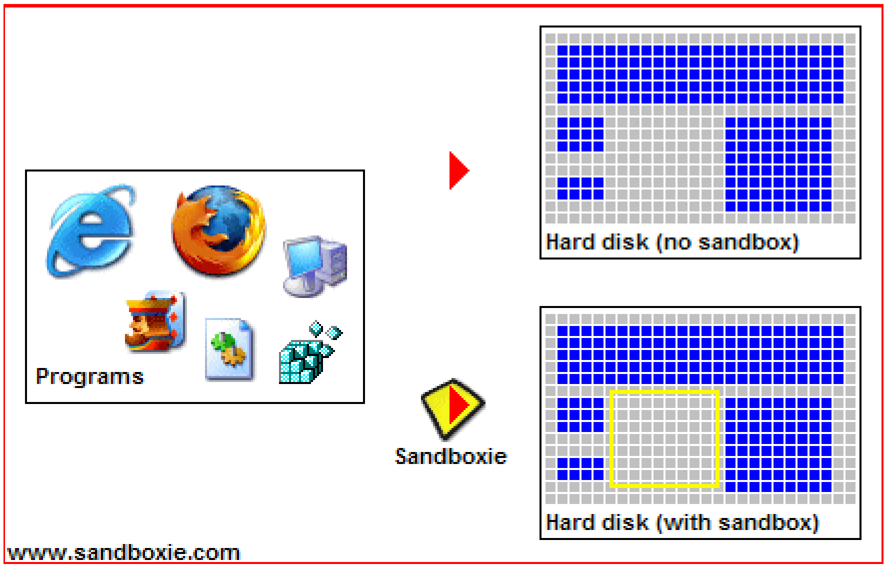
Restricting cookies is done through Internet Explorer privacy settings. There are six different levels of cookie control.

Click on the image or link below to get more information.

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/m32-cookies.html

SANDBOX YOUR BROWSER

The safest way to search the Internet is to Sandbox your browser's activities.   An ideal program that enables this feature is called Sandboxie (www.sandboxie.com).



The benefits are numerous (reference: www.sandboxie.com):

- Secure Web Browsing: Running your Web browser under the protection of a sandbox means that all malicious software downloaded by the browser is trapped in the sandbox and can be discarded trivially.
- Enhanced Privacy: Browsing history, cookies, and cached temporary files collected while Web browsing stay in the sandbox and don't leak into Windows.
- Secure E-mail: Viruses and other malicious software that might be hiding in your email can't break out of the sandbox and can't infect your real system.
- Windows Stays Lean: Prevent wear-and-tear in Windows by installing software into an isolated sandbox.

DEFENSES THROUGH GOOD PRACTICES

E-MAIL DEFENSES THROUGH GOOD PRACTICES

1. When dealing with attachments and embedded hyperlinks, know for sure who it is that sent it and that you are expecting it.
2. Use reading panes and previews when possible.

3. Never answer an e-mail request for personal information - place a phone call instead.

4. Treat e-mail cautiously.

INTERNET DEFENSE SUMMARY

When accessing information on the Internet you have to be very careful and use common sense. However, sometimes this is not enough and you have to incorporate the security and privacy settings that are part of your browser.

Click on the image or link below to view an interactive summary of this segment.

http://coursecontent.ntc.edu/CIT/husband/pois/lp3/m33-summary.html