

Guideline to Safe Web Browsing

1. Introduction

Security threats are not targeting on systems and networks only but they are also affecting web browsers. Malicious hackers and virus writers can take advantage of low security settings in your Web browsing software to infect and attack your computers. They can do this by enticing you to visit a malicious Web site and plant malicious codes into your browser while browsing even without your knowledge.

In June 24 2004, a new Trojan was released to the net, the Download.Ject that affects customers using Microsoft Internet Explorer, a component of Microsoft Windows.

When a user visits a Web site hosted on a server that is infected with Download.Ject, the Web pages download a Trojan horse to the user's computer. This Trojan horse is named Backdoor:W32/Berbew, also known as Backdoor-AXJ, Webber, or Padodor. When this Trojan horse runs on the user's computer, it may perform several actions, including monitoring Internet access to capture sensitive information such as logon names and passwords, or opening fake dialog boxes that prompt the user to enter confidential information such as ATM card codes, credit card numbers, or other confidential information. Microsoft has released a tool to help you remove Backdoor:W32/Berbew Trojan horse variants from your computer.

In October 2 2003, hackers have found another way to exploit an unpatched hole in Internet Explorer Web browser, using a specially designed attack Web site to install a Trojan horse program on vulnerable Windows machines.

The Trojan program changes the Domain Name System (DNS) configuration on the Windows machine so that requests for popular Web search engines like Google and AltaVista bring the Web surfer to a Web site maintained by the hackers instead, according to warnings from leading security companies.

The above scenarios/incidents explains the threats and implications posed against web browsers. The trend in the threats may get more sophisticated in the near forth. Though you can arm your computers with wide variety of free/commercial tools or softwares , but you need a proper overall guideline on browser security.

2. Threats & consequences related to Web Browsing

2.1 Unauthenticated/fake sites

Phishing scam is an example of how users can be duped into browsing an unauthenticated and fake website. Phishing scam is an activity where an attacker (phisher), fools or spoofs the original emails or websites, mainly Financial Institutions' websites, and try to convince the recipients or customers of certain organization (usually banks) to provide sensitive data such as credit card numbers, username and passwords, social security numbers , etc. According to a research done by Antiphishing working group, nearly 5 percent of total number of certain online bankings, online retailers and credit card companies customers are being convinced by this attack.

2.2 Browser exploit/malicious code

It has been a normal thing , an application will have a bug. Since, a state of the art application that uses massive functionality and involves tremendous lines of code will accidentally invent a hole or bug. Lack of proper software engineering and line of code checking will certainly bring up the hole.

And usually if the bug found by external party, it will create a major problem to the developer of this software. Usually as a culture of bug finding, the bug finder will normally reports it to the developer of the particular software, and the developer will respond in a manner of releasing certain patch for the bug.

If this is not the case, say the bug is being kept low by the finder and the bug itself will definitely create a high level security bug. This is where usually the malicious code will take advantage the bug or hole. For example, a buffer overflow in Internet Explorer CA-2002-04 <http://www.cert.org/advisories/CA-2002-04.html> . The bug is the buffer overflow vulnerability of Internet Explorer when handling embedded objects in HTML documents. This vulnerability could allow an attacker to execute arbitrary code on the victim's system when the victim visits a web page or views an html email message.

2.3 Explicit Content

The world of internet is considered as a broad and free .The meaning of free here is, not only for its availability but the content of the web also is free. Any people can write or develop their own web page regardless of topics, languages, purposes and representing the content for their own or attached to an organization. The early idea of this freedom is actually to make the netizens to be more creative, independent, more informative than the conservative media, and the most important thing is, the ability of sharing much and variety of information. Thus we can say here, the content of the internet is not filtered and can be to the extent of negative aspects.

For example of negative information that can be depicted from internet are, sexual nudity, inhumanity culture, negative propaganda and etc. A newflash from USA Today http://www.usatoday.com/tech/webguide/internetlife/2004-06-03-popular-porn_x.htm proves that, most of the users of the internet has abused the initial objective of Internet. From a very useful technology that derived from educational culture, nowadays turns to be a field for pornographic and some of the people throughout the world makes this as a major industrial income.

For most cases, this so called adult entertainment can actually become a very poisonous media for the young generation and the access to such material is very easy and efficient. Are we willing to have a next generation that grows with this kind of negative culture?

2.4 Man in the middle attack

Analogically, this type of attack is eavesdropping a conversation between two people. Say person A talk to person B and person C act as an eavesdropper and he can actually hear what ever being talked by person A and B. In the computer world, eavesdropping is done thru a network device such as network interface cards (NIC). On a regular usage, the NIC is set to deliver data from sender to the intended destination, without any third party involvement. For example, if I want to send a data to John Doe, only John Doe is the one who is eligible for this data.

But when it comes to, Man in the middle attack, data from me to John Doe are being intercepted by another party. And he can actually, read and probably reconstruct those data. In the network term, this behavior is also known as sniffing. If the data that travels to and from the network is somewhat low sensitive data, it should not be any problem but what if the data that flows is username and password of the CEO of a company? This attack is actually a very major threat to an organization, since the activity is hard to be detected and usually the sniffing activity is for network testing purposes. Again, a good intention of a technology has been turned into somewhat unethical.

3. Countermeasures to These Threats

3.1 Patch your browser

In order for us to overcome the bugs and exploits problem, patching up software are the best thing to implement. Usually when a vulnerability is found out, the developer will as fast as they can to create a patch to the hole. Each developer has their own ways of patching up system. Please refer to particular vendor on patching up your system. But within this discussion we will cover the wonders of how Microsoft deploy and release their patch.

Before we go in depth on how to retrieve a patch, we are certainly required to know where and how to notice a bugs or vulnerability. Here are a set of urls , that are widely use by the users and customers.

- <http://www.us-cert.gov/>
- <http://www.microsoft.com/security/default.mspix>
- <http://www.mycert.org.my>
- <http://www.incidents.org>
- <http://www.securityfocus.com/> (previously know as bugtraq)

For Microsoft users, the relevant site where they can get patches is at:

<http://v5.windowsupdate.microsoft.com>



Picture 1

When browsing to the site,the users will be pop up a window, requesting an input whether to continue or not installing the updates. It is very important to click on the certificate link on the windows, to make sure the validity of the page. Once you are comfort with the certificate, proceed the installation by following the guidance of the web pages.

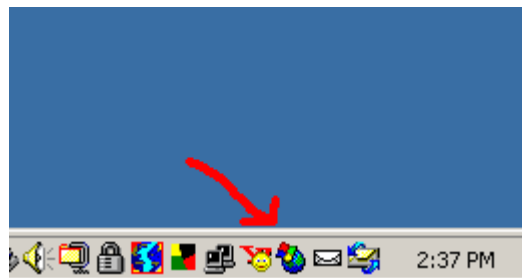
After, installation you may check the history or what have been installed on your computer by entering the Add/Remove program menu. Go to Start → Control Panel → Add/Remove programs. The lists of the installed patches are listed, and you may remove if the patch doesn't suits your system. (Some patches will not work perfectly with some other third party program.

Therefore at certain situation, you will need to contact the vendor or the Microsoft representative to verify the patch before you deploy it.)

As a good practice, the industry always performs a testing period on non-operational machines before they can actually install the patches. This is to avoid any major glitches right after the patch is up. If you can't afford such facility, it is a good way of finding information about the latest patch via a mailing list or forum that discusses this type of patch. For example:

<http://communities.microsoft.com/newsgroups/default.asp?icp=xpsp2&slcid=us>

Or you can also find a small icon on the right of the desktop to reach the windows update.

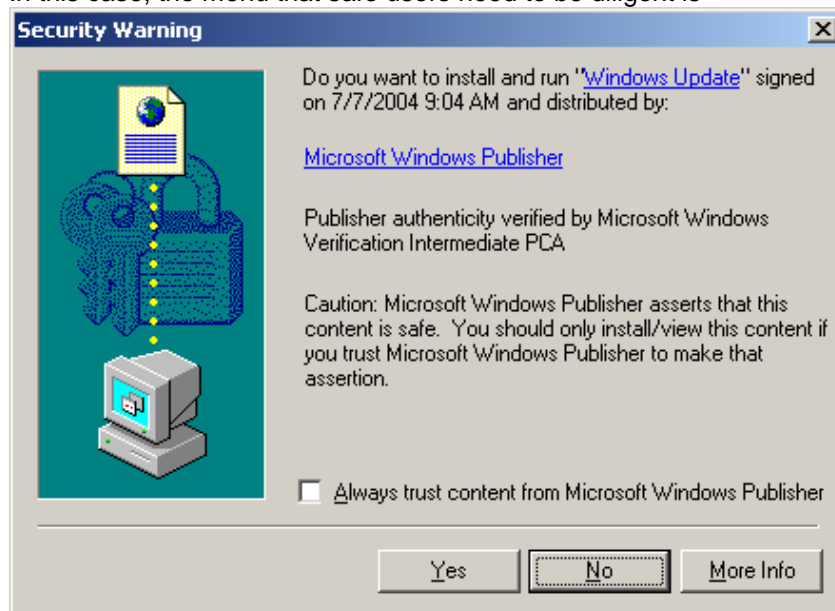


Picture 2

3.2 Verify the sites you're browsing is authenticates site

When you browse to a website, it is hard to tell whether the site is a valid or is it actually an original site of the page that you have requested. Since there are lots of techniques out there to spoof a website, the technology of certificate is introduced. Actually by default, the browser will always ask the user whether to accept or not to accept connection from a certain website. But most of the case people will just click OK and proceed to view the site of the URL that they have typed in.

In this case, the menu that safe users need to be diligent is




Picture 3

If you click on the Microsoft Windows Publisher link , a certificate will be pop up. Proceed whenever you can see the certificate is valid.

3.3 Verify that a Website is Secure

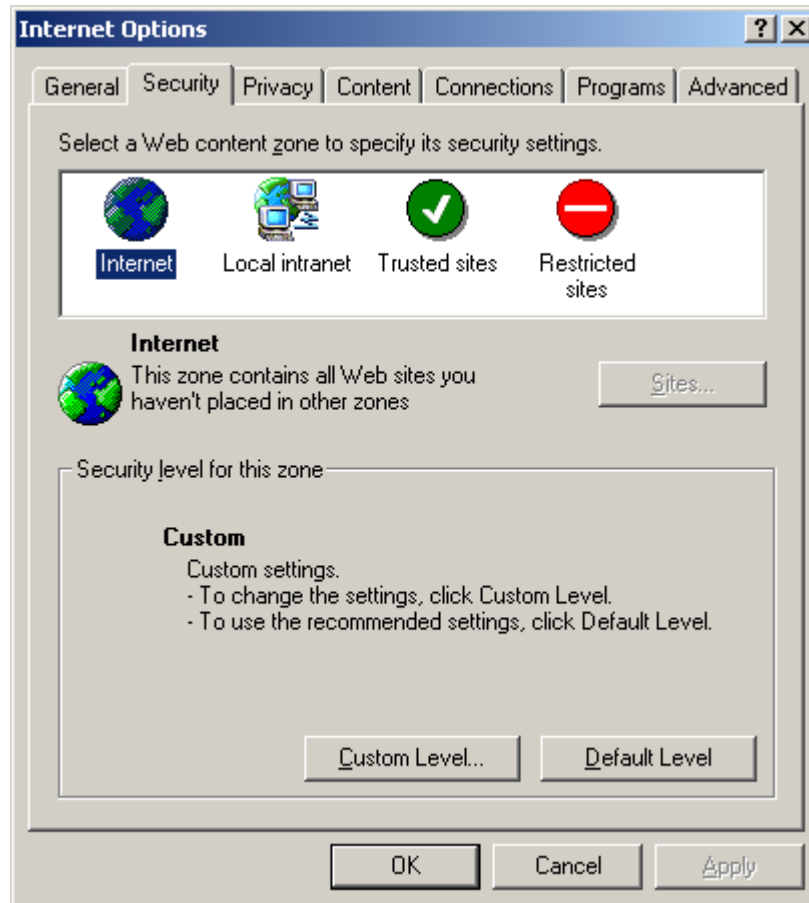
Before you're browsing a website especially if you need to make a purchase or share sensitive personal information over the Internet, make sure you verify the website is using encryption to protect information you are submitting. Check for these security measures:

- Make sure you see https:// in the web address (URL) of the website.
- Look for a lock image (example: ) in the lower right hand corner of your web browser, indicating that the web page is using a security certificate to encrypt the information you will submit.
- Click on the lock image in the browser, or on a "security certificate information" link, usually prominently displayed on secure websites. The link will verify the identity, validity, and security of the site, as well as provide status of the security certificate. For example, on Ent Federal's online banking site, you will see the "Verisign Secure Site" image link at the bottom of every page. If you click on this image link, you can verify that Ent Federal's security certificate is current and in use throughout our online banking website.

3.4 Configure browser to High Security

Most of the current security breaches came from ActiveX, Java and scripting. By default all these scripting is being accepted by browser. But due to high risk of security came from certain sites. It's a good thing to customize again the security level of your browser. Even though, customizing this security level doesn't fully secure yourselves from the threat from the net. But it could somehow provide mitigation against it. And be sure to enable other security mechanism such as antivirus, firewall and intrusion detection system.

In the case of internet explorer, the menu for adjusting this level of security is within the Security tab inside the browser. Goto Tools→Internet Options → Security.



Picture 4

For Internet Connection security level, click the icon pictured world. And if you click default, the setting will assign as accepting those scriptings. And we are really want this to be disable. Therefore, goto custom and you will presented with options regarding the features that you want to enable , disable or prompt. Prompt here means that if the feature is occurred t the web, say a script tries to get in, the browser will pop up a menu, and waiting for approval for the script to be executed or not. While, disable and enable just give a way or not a certain feature without prompting any notices.

In Internet explorer the default level value is medium. And the settings are as follow:

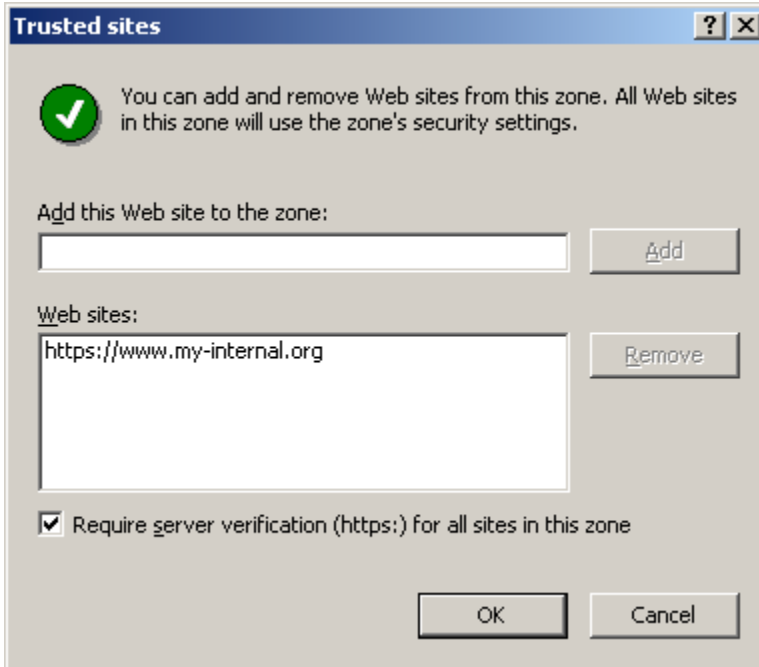
- ActiveX controls and plug-ins
 - Download signed ActiveX controls: Prompt
 - Run ActiveX controls and plug-ins: Enable
 - Script ActiveX controls marked safe for scripting: Enable
- Downloads
 - Font Download: Enable
- Microsoft VM
 - Java permissions: High safety
- Miscellaneous
 - Allow META REFRESH: Enable
 - Display mixed content: Prompt

- Drag and drop or copy and paste files: Prompt
- Installation of desktop items: Prompt
- Launching programs and files in an IFRAME: Prompt
- Navigate sub-frames across different domains: Enable
- Software channel permissions: Medium Safety
- Userdata persistence: Enable
- Scripting
 - Active scripting: Enable
 - Allow paste operations via script: Enable
 - Scripting of Java applets: Enable
- User Authentication: Automatic logon only in Intranet zone

In order to make us more secure, we just disables the features that are relevant to scripts. And it turns to be like as below.

- ActiveX controls and plug-ins
 - Download signed ActiveX controls: Disable
 - Run ActiveX controls and plug-ins: Disable
 - Script ActiveX controls marked safe for scripting: Disable
- Downloads
 - Font Download: Disable
- Microsoft VM
 - Java permissions: Disable Java
- Miscellaneous
 - Allow META REFRESH: Disable
 - Display mixed content: Disable
 - Drag and drop or copy and paste files: Disable
 - Installation of desktop items: Disable
 - Launching programs and files in an IFRAME: Disable
 - Navigate sub-frames across different domains: Disable
 - Software channel permissions: High Safety
 - Userdata persistence: Disable
- Scripting
 - Active scripting: Disable
 - Allow paste operations via script: Disable
 - Scripting of Java applets: Disable
- User Authentication: Automatic logon with current username and password

What about if you want to enable scripts for certain sites? Say, your internal web based system requires scripts to be enabled. The answer to this is that, you can just add them into the trusted sites.



Picture 5

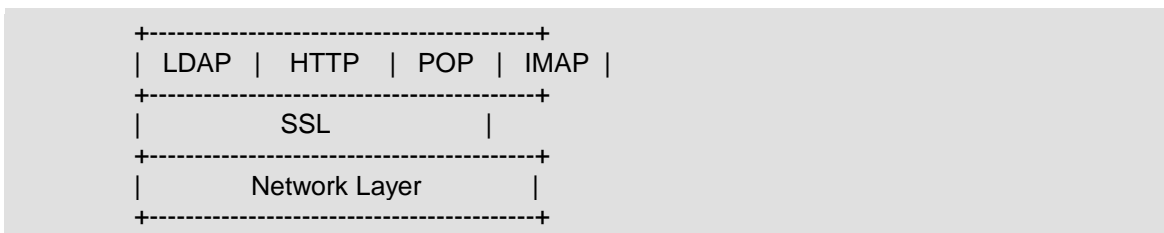
And the script only enabled, if you visit to these trusted sites.

3.4 Use SSL for secure transaction

Users of the internet are always vulnerable to sniffing attack, since most of the protocol like http, imap, pop are in clear text transaction. This kind of attack is called “man in the middle attack” (which has been explained earlier). In order for us to make it unreadable to human, computer scientists have invented encryption. This technology could mitigate the effort of sniffing data across the network. And previously the clear text data, only can be seen as a set of garbled (unreadable) data. The data is actually valid, once the correct recipient receives it.

SSL or Secure socket Layer, is a technology that adopting the advantage of encryption. It is a protocol layer that exists between the Network Layer and Application layer. As the name suggest SSL provides a mechanism for encrypting all kinds of traffic - LDAP, POP, IMAP and most importantly HTTP.

The following is a over-simplified structure of the layers involved in SSL.



Picture 6

SSL works by using a private key. For example, if John Doe (sender) wants to send data to Jenny (recipient), first the sender will encrypt the data by using his private key. And the result of this process is CipherText1. Secondly, the recipient will encrypt it again with her public key and

results the CipherText2.Next the SHA1 message digest of the "clear text" is then created. This SHA1 message digest is then being encrypted, using Sender's private key. And the result of it is called, Digital Signature of the "Clear text". Finally both Digital Signature and CipherText2 are send to the recipient.

Once the data is received by the recipient, Cipher Text 2 will be decrypted by Recipient's Private key. This data is then called CipherText1.Again, it will be decrypted and resulting Clear text data. Here the SHA1 of the clear text message is created. The "Digital Signature" is then decrypted using Sender's Public Key, resulting the "SHA 1 MSG Digest".The "SHA1 MsgDigest #1" is then compared against "SHA1 MsgDigest #2". If they are equal, the data was not modified during transmission, and the integrity of the Original "Clear Text" has been maintained.

Within this process, the data is not being readable by the 3rd party person. And if the data is being intercepted, the actual content of it cannot be exposed. Furthermore, by the use of this SSL technology, the integrity data can be identified.

3.5 Download relevant tools – To Block Pop up Windows



Above news cut is actually a malware that affects the users of sensitive websites thru a pop up. The malware actually can install itself on computers and record all the keystrokes that users have typed in. Besides that, pop ups also considered as a very annoying behavior and usually it is an advertisement of products and brands.

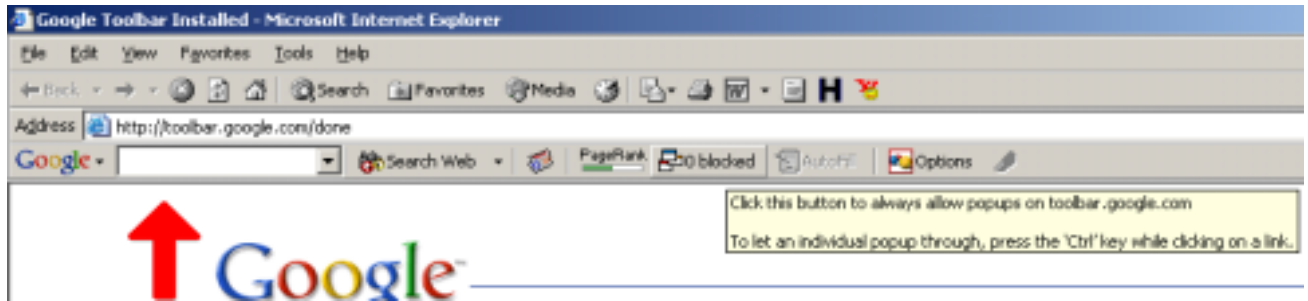
Actually there are lots of software that fights this pop up ads. For example:

- 1.Pop up stopper by panicware
- 2.Pop up blocker by earthlink.net
- 3.Noaware by noaware.net
- 4.Google toolbar.

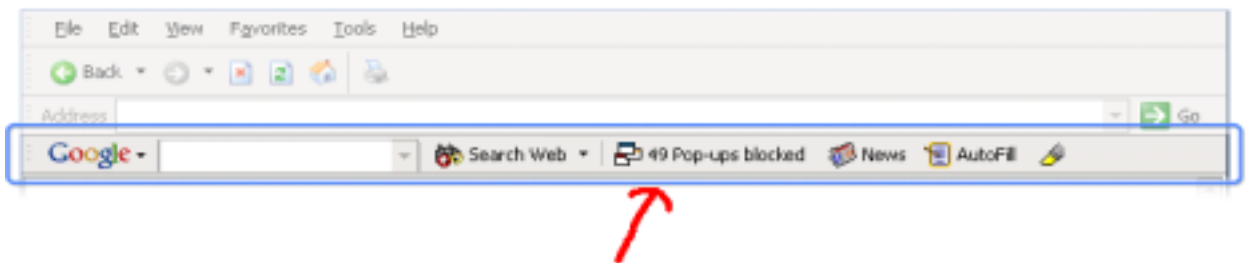
Since most of the users around the world uses google as search engine.We will take a look at google toolbars as our pop up blocker.

Download google toolbar for free at <http://toolbar.google.com/>

After getting thru with all the installation, a toolbar will appear right on top of your internet explorer bar.(See Picture 8)



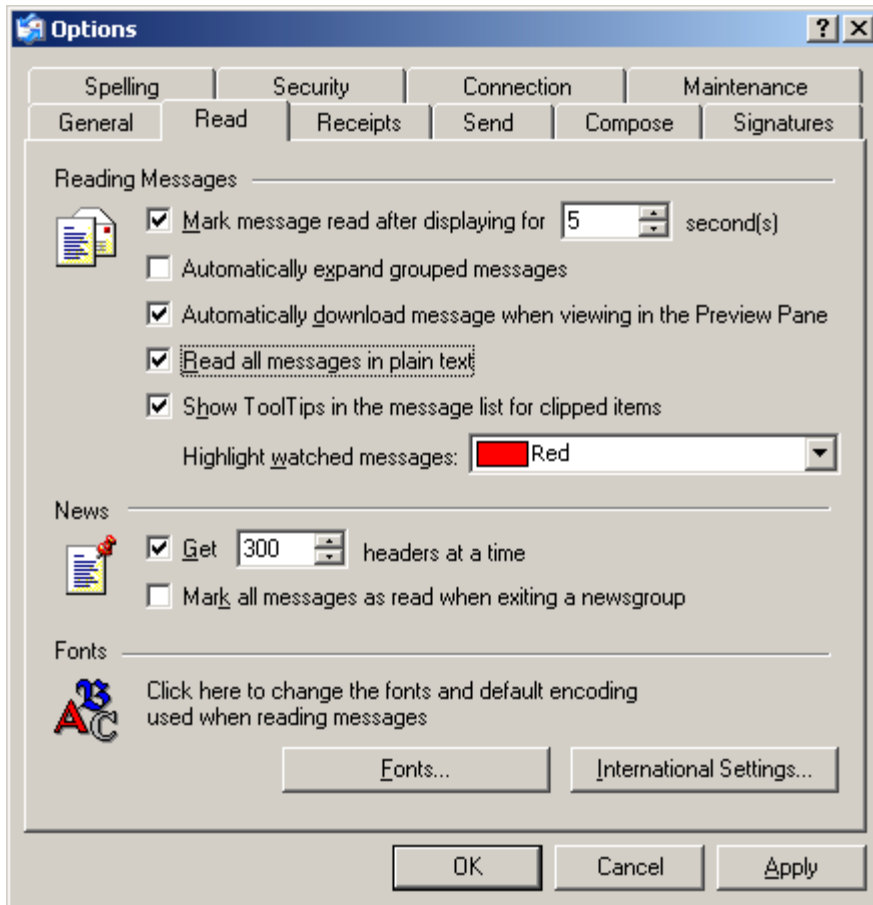
To use the pop up blocker is pretty straight forward. Once you click the button, the pop up blocker will understand it as allowing the pop ups. But when the button is unblocked, the toolbar will automatically blocks all pop up that appears. And the count of blocked pop ups will also appeared at the button.(See picture 8)



3.6 Use plain text to read emails

There are few ways viruses, malicious codes, exploits that can be spread to internet users. Emails, is one of the favorite way of an evil hacker to spread their notorious scripts and programs. The main idea here is to make the user to execute the code that they have sent. Therefore, most of it is spread thru html based emails. If you are using text based email like Pine, this kind of threat is not a problem. But the targets are at Microsoft based client like Microsoft outlook, which has the feature of executable html. As a countermeasure against this, it is proposed that the html feature will be disabled. Here is an example on how to disable html on Microsoft outlook. Other clients may vary, and do consult each vendor on how to do the same thing.

1. In Microsoft outlook, go to Tools→ Options → and tab Read.



Picture 9

2. Then tick option “Read all messages in plain text”.

Now your Microsoft Outlook, will only reads plain text email, and if an html email comes in, it will only show html tags (a non active html).