



National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline For Securing Your Web Browser



CERT-MU

**National Computer Board
Mauritius**

Table of Contents

1.0 Introduction.....	7
1.1 Purpose and Scope	7
1.2 Audience.....	7
1.3 Document Structure.....	7
2.0 Background.....	8
3.0 Types of Web Browsers.....	9
3.1 Microsoft Internet Explorer.....	9
3.2 Mozilla Firefox.....	9
3.3 Safari	9
3.4 Chrome.....	10
3.5 Opera.....	10
3.6 Netscape Navigator	10
4.0 Web Browser Features and Risks	11
4.1 ActiveX	11
4.2 Java.....	11
4.3 Plug-ins.....	12
4.4 Cookies.....	12
4.5 JavaScript	12
4.6 VBScript.....	12
4.6.1 Cross-Site Scripting (XSS).....	13
4.6.2 Cross-Zone and Cross-Domain Vulnerabilities	13
4.6.3 Detection evasion	13
5.0 How to Secure Your Web Browser	14
5.1 Microsoft Internet Explorer.....	14
5.1.1 Security Zones.....	15
5.1.2 Trusted Sites.....	17
5.1.3 Managing Cookies.....	18
5.1.4 Advanced Privacy Settings.....	21
5.1.5 Setting Default Applications	22
5.2 Mozilla Firefox.....	23
5.2.1 Browser History and Cookies	24
5.2.2 Add-on Options	25
5.2.3 Download Settings	27
5.2.4 Privacy Feature.....	28

5.2.5 NoScript Feature	29
5.2.6 Plugins Feature	30
5.3 Apple Safari.....	31
5.3.1 Preferences Menu.....	32
5.3.2 AutoFill Feature	32
5.3.3 Security Options.....	33
5.4 Google Chrome	34
5.4.1 Privacy Settings.....	35
5.4.2 Phishing and malware detection.....	36
5.4.3 Images, JavaScript, and other Web Content Settings.....	37
5.4.4 Managing Exceptions.....	38
5.5 Opera	38
5.5.1 The Address Field (1).....	38
5.5.2. Opera's Security Badge (2).....	39
5.5.3 Security Information	40
5.6 Netscape Navigator	42
6.0 Conclusion	43
7.0 References.....	44
Appendix A.....	45
Security Terms Explained	45

Tables and Figures

Tables

Table 1 Phishing and Malware Alerts in Chrome.....	37
Table 2 Security Badges in Opera	39

Figures

Figure 1 The “Tools” Tab in Internet Explorer 7	15
Figure 2 The “Security” Tab in Internet Explorer 7	16
Figure 3 The “Security” Settings in Internet Explorer 7.....	16
Figure 4 The “Trusted sites” zone in Internet Explorer 7	17
Figure 5 Adding secure sites to the “Trusted sites” zone.	17
Figure 6 The “Privacy” Tab in Internet Explorer 7	18
Figure 7 The “Advanced Privacy” Settings in Internet Explorer 7	19
Figure 8 The “Privacy” alert in Internet Explorer 7	19
Figure 9 The “Per Site Privacy Actions” in Internet Explorer 7.....	20
Figure 10 The “Internet” Options in Internet Explorer 7.....	20
Figure 11 The “Enable third-party browser extensions” setting in Internet Explorer 7	21
Figure 12 “Encoded addresses” and “sounds” in Internet Explorer 7	22
Figure 13 The “Programs” Tab in Internet Explorer 7	22
Figure 14 The “Tools” Tab in Mozilla Firefox.....	23
Figure 15 The “Main” Tab in Mozilla Firefox	24
Figure 16 The “Privacy” Tab in Mozilla Firefox.....	24
Figure 17 The “Cookie” setting in Mozilla Firefox.....	25
Figure 18 The “Security” Tab in Mozilla Firefox	26
Figure 19 The “Content” Tab in Mozilla Firefox	26
Figure 20 The “Advanced JavaScript” Settings in Mozilla Firefox	27
Figure 21 The “Manage” button in Mozilla Firefox.....	27
Figure 22 The “Download Actions” dialog box in Mozilla Firefox	28
Figure 23 The “Change Action” dialog box in Mozilla Firefox	28
Figure 24 The “Clear Private Data” option in Mozilla Firefox	29
Figure 25 The available options for clearing private data in Mozilla Firefox	29
Figure 26 The “NoScript” Menu in Mozilla Firefox	30
Figure 27 The “Plugins” Tab in Mozilla Firefox.....	30
Figure 28 The “plugins” options in Mozilla Firefox	31

Figure 29 The “Preferences” option in Safari.....32

Figure 30 The “General” Tab in Safari.....32

Figure 31 The “AutoFill” Tab in Safari.....33

Figure 32 The “Security” Tab in Safari34

Figure 33 The “Address” Field in Opera38

Figure 34 Security Information in Opera.....40

Figure 35 The “Security Information” dialog box in Opera40

DISCLAIMER: *This guideline is provided “as is” for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This guideline covers web browsers usage, the security risks associated with them and the controls required to secure them. The process of configuring a web browser security features is rather simple for the average computer user and is well worth the investment of a few minutes of our time. This document helps you understand the features offered by different web browsers, how they affect your web browser's functionality and security of your computer.

1.2 Audience

The intended audience of this document includes home Internet users, students, small business workers, web site owners, webmasters, security professionals, managers and anyone who make use of the Internet for business or personal purposes.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on web browsers.

Section 3 provides the types of existing web browsers.

Section 4 discusses the web browser features and risks.

Section 5 details the security measures for securing the web browsers introduced in *Section 3*.

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

Appendix A provides a list of acronyms used in this document.

Appendix B presents a list of security terms referred to in this guideline.

2.0 Background

A Web browser is a computer application used for retrieving, presenting and transmitting information resources on the World Wide Web (Internet). It is also helpful in accessing information provided by web servers within private networks or files in file systems. The most common web browsers in use are Windows Internet Explorer, Mozilla Firefox and Google Chrome.

Web browsers are among the most commonly used applications on our computer. Those which come along with your computer's operating system do not normally have security features configured by default; therefore it is up to you to enable the security options for secure Web browsing. Not doing so can support hackers to easily take over your computer, as well as allow malicious software (malware) such as viruses, spyware and adware to be downloaded. Many users fail to set up their Web browser security settings, by mere negligence or ignorance. On average, people who surf on the Internet will click on ads and links without bothering about how secure is the website or the consequences of clicking on a malicious link. Users generally make the most of the advantages that Web browsers bring along and do not consider the overall security aspects.

New computers with pre-installed Web browsers usually contain other types of software bundled together, that might increase the vulnerability to unscrupulous attacks. Many websites require the download of add-ons such as ActiveX¹ for added features. These also increase the vulnerability of your Web browser. Sometimes bugs in Web browsers are discovered once the software has been released. Until there are patches to solve the issue, the application is vulnerable and prone to software attacks.

Vulnerabilities in Web browsers can help hackers to take control of your computer, steal your identity and credentials, spy on your surfing habits, and also damage your computer. Exploiting vulnerabilities in systems is also a low-cost way of doing all of the above.

¹ ActiveX: is a framework for defining reusable software components in a programming language independent way. Software applications can then be composed from one or more of these components in order to provide their functionality

3.0 Types of Web Browsers



3.1 Microsoft Internet Explorer

Since its first release, Microsoft has added features and technologies such as basic table display (in version 1.5); “XMLHttpRequest”² (in version 5), which aids creation of dynamic web pages; and Internationalised Domain Names³ (in version 7), which allow Web sites to have native-language addresses with non-Latin characters. The browser has also been subject to review throughout security and privacy vulnerabilities. The latest stable release is Internet Explorer 9, which is available as a free update for Windows 7, Windows Vista SP2, Windows Server 2008 and Windows Server 2008 R2.



3.2 Mozilla Firefox

Mozilla Firefox is a free and open source web browser derived from the Mozilla Application Suite and managed by Mozilla Corporation. To display web pages, Firefox uses the Gecko layout engine, which implements most current web standards and several features that are planned to become potential additions to the standards. The latest Firefox features include tabbed browsing, spell checking, incremental find, live bookmarking, a download manager, private browsing, location-aware browsing (also known as "geolocation") based entirely on a Google service and an incorporated search system that uses Google by default in most locations. Functions can be added through extensions, created by third-party developers, of which there is range of choice, a feature that has appealed many of Firefox's users. Firefox works on various operating systems including Microsoft Windows, GNU/Linux, Mac OS X, FreeBSD, and many other platforms.



3.3 Safari

The Safari Web Browser is a Web browser developed by Apple Inc. and included with the Mac OS X and iOS operating systems. First released as a public beta on January 7, 2003 on the company's Mac OS X operating system, it became Apple's default browser beginning with Mac OS X v10.3 “Panther”. Safari is also the main browser for iOS. There is also a version of Safari for the Microsoft Windows operating system, which supports Windows XP, Windows Vista, and Windows 7. The most stable release of the browser is 5.0.5, which is available as a free download for both Mac OS X and Microsoft Windows.

² XMLHttpRequest: is an API available in web browser scripting languages such as JavaScript. It is used to send HTTP or HTTPS requests directly to a web server and load the server response data directly back into the script

³ Internationalised Domain Name: is an Internet domain name that contains at least one label that is displayed in software applications, in whole or in part, in a language-specific script or alphabet, such as Arabic, Chinese, Russian, Hindi or the Latin alphabet-based characters with diacritics, such as French.

3.4 Chrome

Chrome is a Web browser developed by Google that uses the WebKit⁴ layout engine. The name comes from the graphical user interface frame, or "chrome", of web browsers. Chromium is an open source project developed by Google by making part of Chrome's source code, including its V8 JavaScript⁵ engine, available to the public. It implements the same feature set as Chrome, but lacks built-in automatic updates and Google branding, and also has a blue-coloured logo in place of the multicoloured Google logo.

3.5 Opera

Opera is a Web browser and Internet suite developed by Opera Software. The browser supports common Internet-related tasks such as displaying web sites, sending and receiving e-mail messages, managing contacts, chatting on IRC⁶, downloading files via BitTorrent⁷, and reading web feeds⁸. It is free of charge for personal computers and mobile phones, and comes on its own, that is, not packed up with any desktop operating system. It is well-known for introducing many features later taken up by other web browsers. It runs on a variety of personal computer operating systems, including Microsoft Windows, Mac OS X, Linux, and FreeBSD. It is the only commercial web browser available for the Nintendo DS and Wii gaming systems.

3.6 Netscape Navigator

Netscape was the general name for a series of web browsers originally produced by Netscape Communications Corporation, now a subsidiary of America Online (AOL). The original browser was once the leading browser in terms of usage share, but as a result of the first browser war it lost virtually its entire share to Internet Explorer.

Netscape was discontinued and support for all Netscape browsers and client products was ended on March 1, 2008.

⁴ WebKit: is a layout engine designed to allow web browsers to render web pages

⁵ JavaScript: is a prototype-based, object-oriented scripting language that is dynamic, weakly typed and has first-class functions.

⁶ IRC: Internet Relay Chat (IRC) is a form of real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion forums, called *channels*, but also allows one-to-one communication via private messages as well as chat and data transfer, including file sharing.

⁷ BitTorrent: BitTorrent is a peer-to-peer file sharing protocol used for distributing large amounts of data

⁸ Web Feeds: data format used for providing users with frequently updated content.

4.0 Web Browser Risks

Understanding how your Web browser works is very important. Sometimes enabling some web browser features may have a negative effect on the security of the system. Very often, vendors enable features by default to enhance browsing experience, but this may make the computer more open to security risks. An attacker can create a malicious web page that will install Trojans or spyware which can steal your data. A malicious website can passively compromise a system when a user clicks on the fake link. This type of attack does not actively target and attack vulnerable systems. A malicious e-mail can also be sent to victims. This is commonly known as “*Phishing*”. In such cases, opening the e-mail or attachment can compromise the system. Below are some web browser features and the risks they involve.

4.1 ActiveX

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows systems. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or a site may provide the component as a downloadable object. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented. ActiveX has been plagued with various vulnerabilities and implementation issues. One problem with using ActiveX in a web browser is that it greatly increases the attack surface, or “attackability,” of a system. Installing any Windows application introduces the possibility of new ActiveX controls being installed. Vulnerabilities in ActiveX objects may be exploited via Internet Explorer, even if the object was never designed to be used in a web browser. Many vulnerabilities with respect to ActiveX controls lead to severe impacts. Often an attacker can take control of the computer.

4.2 Java

Java is an object-oriented programming language that can be used to develop active content for web sites. A Java Virtual Machine, or JVM, is used to execute the Java code, or “*applet*”⁹, provided by the web site. Some operating systems come with a JVM, while others require a JVM to be installed before Java can be used. Java applets are operating system independent. Java applets usually execute within a “sandbox”¹⁰ where the interaction with the rest of the system is limited. However, various implementations of the JVM contain

⁹ Applet: An applet is a program written in the Java programming language that can be included in an HTML page, much in the same way an image is included.

¹⁰ Sandbox: is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third-parties, suppliers and untrusted users.

vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute.

4.3 Plug-ins

Plug-ins are applications intended for use in the web browser. Netscape has developed the NPAPI standard for developing plug-ins, but this standard is used by multiple web browsers, including Mozilla Firefox and Safari. Plug-ins are similar to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash is an example of an application that is available as a plug-in. Plug-ins can contain programming flaws such as buffer overflows¹¹, or they may contain design flaws such as cross-domain violations, which arises when the same origin policy is not followed.

4.4 Cookies

Cookies are files placed on your system to store data for specific web sites. A cookie can contain any information that a web site is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the web site that created the cookie. Session cookies are cleared when the browser is closed, and persistent cookies will remain on the computer until the specified expiration date is reached. Cookies can be used to uniquely identify visitors of a web site, which some people consider a violation of privacy. If a web site uses cookies for authentication, then an attacker may be able to acquire unauthorized access to that site by obtaining the cookie. Persistent cookies pose a higher risk than session cookies because they remain on the computer longer.

4.5 JavaScript

JavaScript also known as ECMAScript, is a scripting language that is used to make web sites more interactive. There are specifications in the JavaScript standard that restrict certain features such as accessing local files.

4.6 VBScript

VBScript is another scripting language that is unique to Microsoft Windows Internet Explorer. VBScript is similar to JavaScript, but it is not as widely used in web sites because of limited compatibility with other browsers. The ability to run a scripting language such as JavaScript or VBScript allows web page authors to add a significant amount of features and

¹¹ Buffer Overflows: anomalies where programs, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety.

interactivity to a web page. However, this same capability can be abused by attackers. The default configuration for most web browsers enables scripting support, which can introduce multiple vulnerabilities, such as the following:

4.6.1 Cross-Site Scripting (XSS)

XSS is web site vulnerability which allows an attacker to influence the trust relationship that you have with that site. This is not caused by a failure in the web browser, but by the way websites are designed.

4.6.2 Cross-Zone and Cross-Domain Vulnerabilities

Web browsers usually make use of security models to prevent script in a web site from accessing data in a different domain. Vulnerabilities that infringe these security models can be used to perform actions that a site could not perform under normal conditions. The impact can be identical to a cross-site scripting vulnerability. However, if a vulnerability gives way to an attacker access the local machine zone or other protected areas, the attacker may be able to execute arbitrary commands on the vulnerable system.

4.6.3 Detection evasion

Anti-virus, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) work by looking for heuristics (specific patterns) in content. If a “known bad” pattern is detected, then the appropriate actions can take place to protect the user. Yet, scripting in web pages can be used to evade such protective systems due the dynamic nature of programming languages.

5.0 How to Secure Your Web Browser

Software features such as ActiveX, Java¹², Scripting (JavaScript, VBScript, etc) add value to a web browser, but can also introduce vulnerabilities to the computer system. This is usually due to poor implementation, poor design, or bad configuration. For these reasons, it is vital that you know which browsers support which features and the risks they bring along. Some web browsers offer the possibility to fully disable the use of these technologies, while others may allow you to enable features on a per-site basis.

Multiple web browsers may be installed on your computer. Other software applications on your computer, such as e-mail clients or document viewers, may use a different browser than the one you normally use to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser for manually interacting with web sites does not mean other applications will automatically use the same browser. Thus, it is important to securely configure each web browser that may be installed on your computer. One of the advantages of having multiple web browsers is that one browser can be used for only sensitive activities such as online banking, and the other can be used for general purpose web browsing. This can reduce the chances of a vulnerability in a web browser, web site, or related software being exploited to compromise sensitive information.

Web browsers are frequently updated. Depending on the version of your software, the features and options may move or change. The following sub sections shows you how to securely configure the web browsers mentioned previously and how to disable features that can cause vulnerabilities.

5.1 Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. Removal of this application is not practical.

In addition to supporting Java, scripting and other forms of active content, Internet Explorer implements ActiveX technology. While any application is potentially vulnerable to attack, it is possible to mitigate a number of serious vulnerabilities by using a web browser that does not support ActiveX controls. However, using an alternate browser may affect the functionality of some sites that require the use of ActiveX controls. Note that using a different web browser will not remove IE, or other Windows components from the system.

¹² Java: Java is a programming language originally developed by James Gosling at Sun Microsystems (which is now a subsidiary of Oracle Corporation)

Other software, such as e-mail clients, may use IE, the Web Browser ActiveX control (WebOC), or the IE HTML rendering engine (MSHTML).

Below are some steps to disable various features in **Internet Explorer 7**. Note that menu options may vary between versions of IE, so you should adapt the steps below as appropriate. In order to change settings for Internet Explorer, select “*Tools*” then “*Internet Options*”

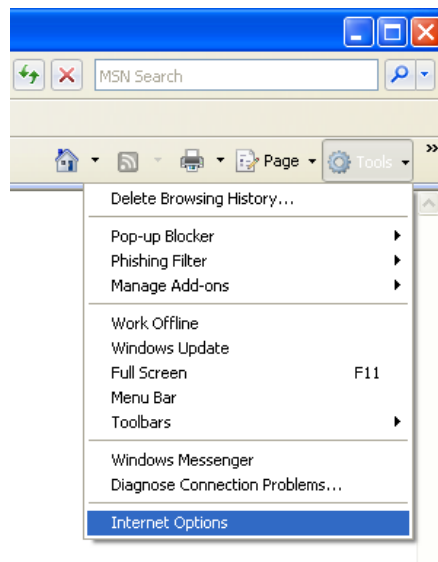


Figure 1 The “Tools” Tab in Internet Explorer 7

5.1.1 Security Zones

Select the “*Security*” tab. On this tab you will find a section at the top that presents the various security zones that Internet Explorer uses.

For each of these zones, you can select a Custom Level of protection. When clicking the “*Custom Level*” button, a second window will open and allow you to select different security settings for that zone. The “*Internet*” zone is where all sites firstly start off. The security settings for this zone apply to all the websites that are not listed in the other security zones. The “*High*” security setting for this zone means more security. By selecting the “*High*” security setting, several features including ActiveX, Active scripting, and Java will be disabled. With these features disabled, the browser will be more secure. Click the “*Default Level*” button and then drag the slider control up to “*High*”.

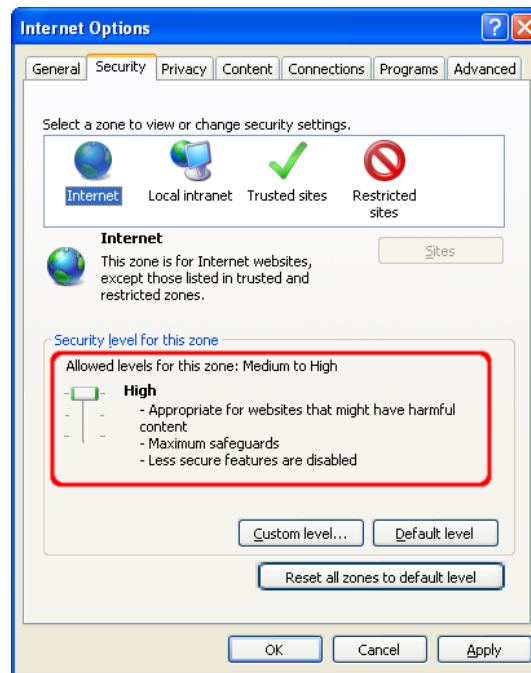


Figure 2 The “Security” Tab in Internet Explorer 7

For more customised control over allowed features in the zone, click the “*Custom Level*” button. Here you can control the specific security options that apply to the current zone. For example, ActiveX can be disabled by selecting “*Disable*” for “*Run ActiveX controls and plug-ins*”. Default values for the “*High*” security setting can be selected by choosing “*High*” and clicking the “*Reset*” button to apply the changes.

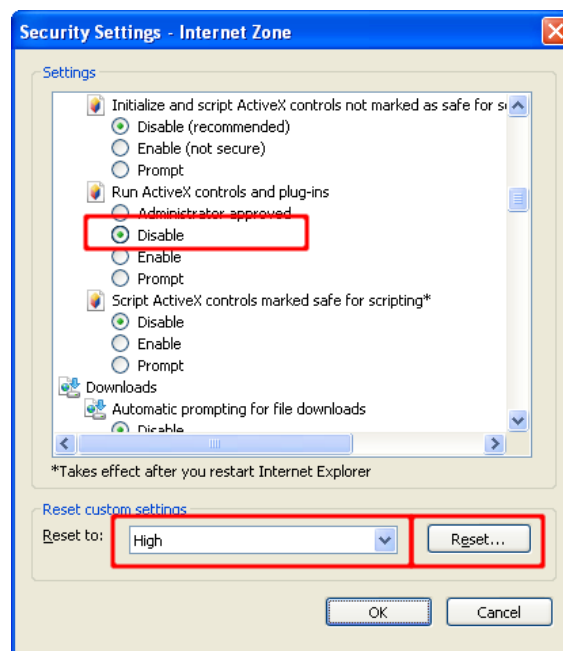


Figure 3 The “Security” Settings in Internet Explorer 7

5.1.2 Trusted Sites

The “*Trusted sites*” zone is a security zone for sites that you consider as safe. You believe that the site is designed with security in mind and that it can be trusted not to contain malicious content. To add or remove sites from this zone, you can click the “*Sites*” button. This will open another window listing the sites that you trust and enabling you to add or remove them. You may also require that only verified sites (HTTPS) can be included in this zone. This gives you greater assurance that the site you are visiting is the site that it claims to be.

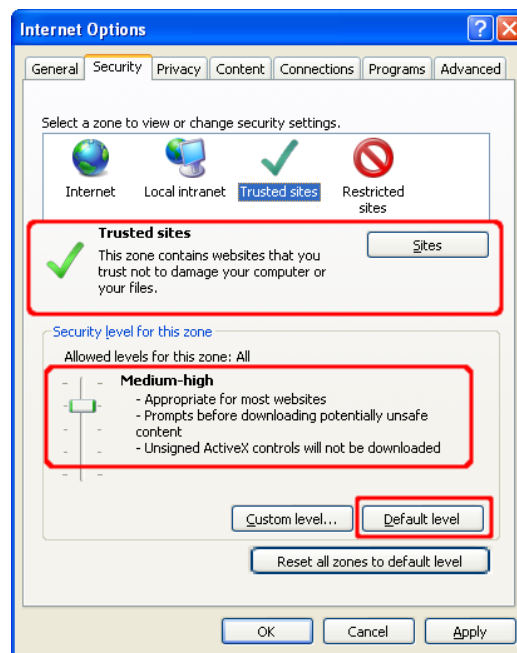


Figure 4 The “Trusted sites” zone in Internet Explorer 7

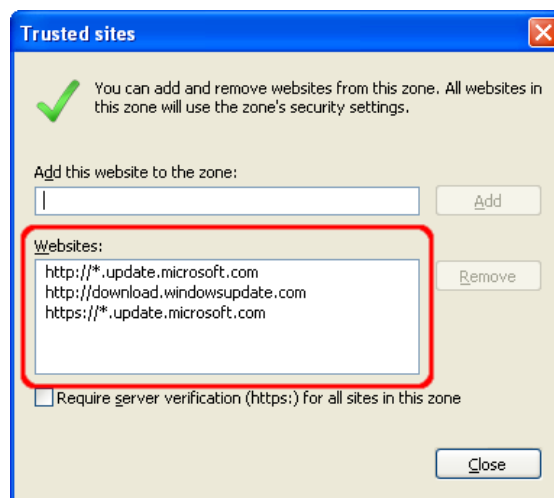


Figure 5 Adding secure sites to the “Trusted sites” zone.

Setting the security level for the “*Trusted sites*” zone to “*Medium-high*” (or “*Medium*” for Internet Explorer 6 and earlier) is recommended. When the “*Internet*” zone is set to “*High*”,

you may encounter websites that do not display properly due to the security settings. This is where the “*Trusted sites*” zone can help. If you trust that the site will not contain malicious content, you can add it to the list of sites in the “*Trusted sites*” zone. Once a site is added to this zone, features such as ActiveX and Active scripting will be enabled for the site. The benefit of this type of configuration is that IE will be more secure by default, and sites can be “whitelisted¹³” in the “*Trusted sites*” zone to gain extra functionality.

5.1.3 Managing Cookies

The “*Privacy*” tab contains settings for cookies. Cookies are text files placed on your computer by various sites that you visit either directly (first-party) or indirectly (third-party) through ad banners, for example. A cookie can contain any data that a site wishes to store. It is often used to track your computer as you move through a web site and store information such as preferences or credentials. A good idea would be to select the “*Advanced*” button and “*Override automatic cookie handling*”. Then select “*Prompt*” for both first and third-party cookies. This will prompt you each time a site tries to place a cookie on your machine. If the number of cookie prompts is too high, the option “*Always allow session cookies*” can be enabled. This will allow non-persistent cookies to be accepted without user interaction. Session cookies have less risk than persistent cookies.

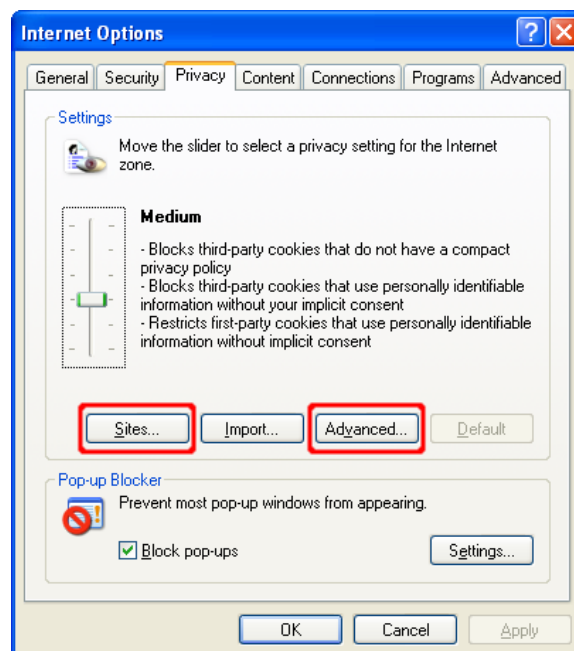


Figure 6 The “*Privacy*” Tab in Internet Explorer 7

¹³ Whitelisted: authorised access or granted membership.

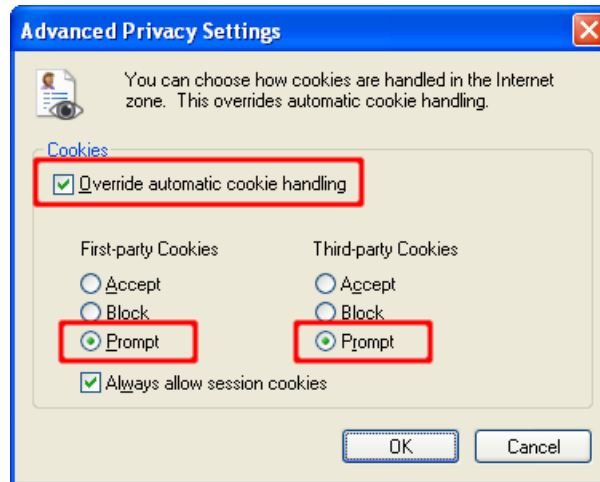


Figure 7 The “Advanced Privacy” Settings in Internet Explorer 7

You can then assess the originating site, whether you wish to accept or deny the cookie, and what action to take (allow or block, with the option to remember the decision for all future cookies from that web site). For example, if visiting a web site causes a cookie prompt from a web domain that is associated with advertising, you may wish to click “*Block Cookie*” to prevent that domain from being able to set cookies on your computer, for privacy reasons.

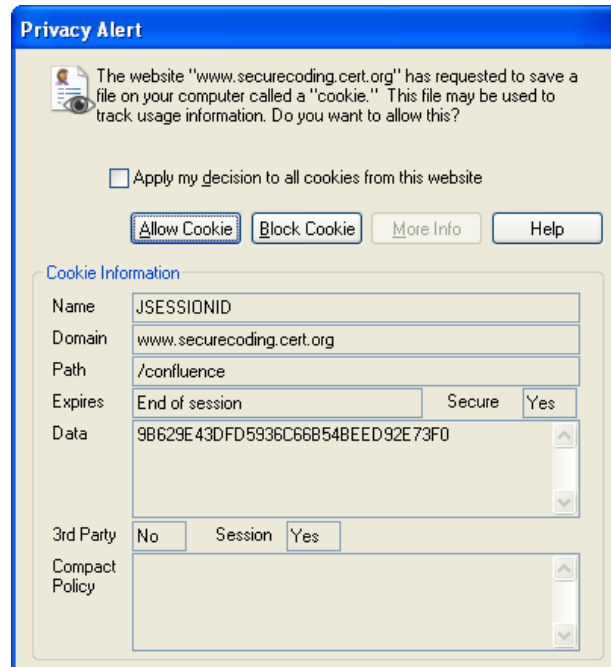


Figure 8 The “Privacy” alert in Internet Explorer 7

By selecting the “*Sites*” button, you can control the cookie settings for specific sites. You can add or remove sites, and you can change the current settings for existing sites. The bottom section of this window will specify the domain of the site and the action (“*Allow*” or

“Block”) to take when that site wants to place a cookie on your machine. You can use the upper section of this window to change these settings.

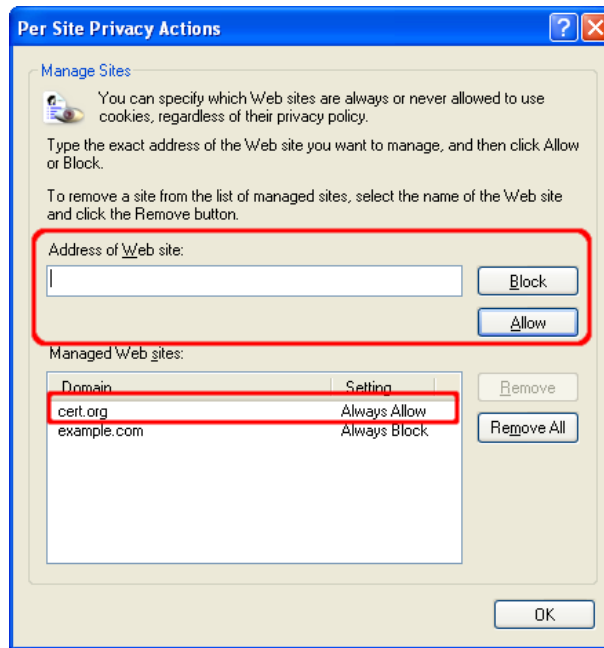


Figure 9 The “Per Site Privacy Actions” in Internet Explorer 7

If you do not wish to receive warning dialogs when a site attempts to set a cookie, you can use Internet Explorer's pre-set privacy rules. Click the “Default” button and then drag the slider up to “High”. Note that some web sites may fail to function properly with the “High” setting. In such cases, you may add the site to the list of sites for which cookies are allowed, as described above.

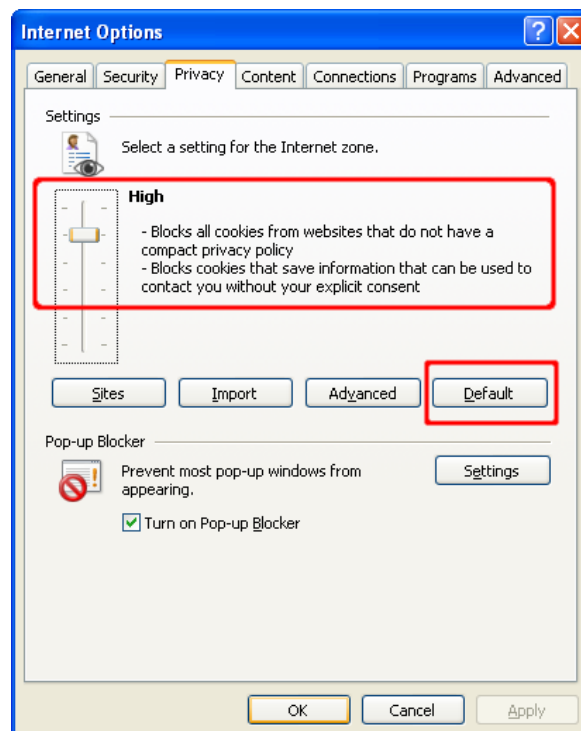


Figure 10 The “Internet” Options in Internet Explorer 7

5.1.4 Advanced Privacy Settings

The “*Advanced*” tab contains settings that apply to all of the security zones. The “*Enable third-party browser extensions*” option should be disabled for added security. This option includes toolbars and Browser Helper Objects¹⁴ (BHOs). While some add-ons can be useful, they can also violate your privacy. For example, a browser add-on may monitor your web browsing habits, or even change the contents of web pages in an attempt to gather personal information.

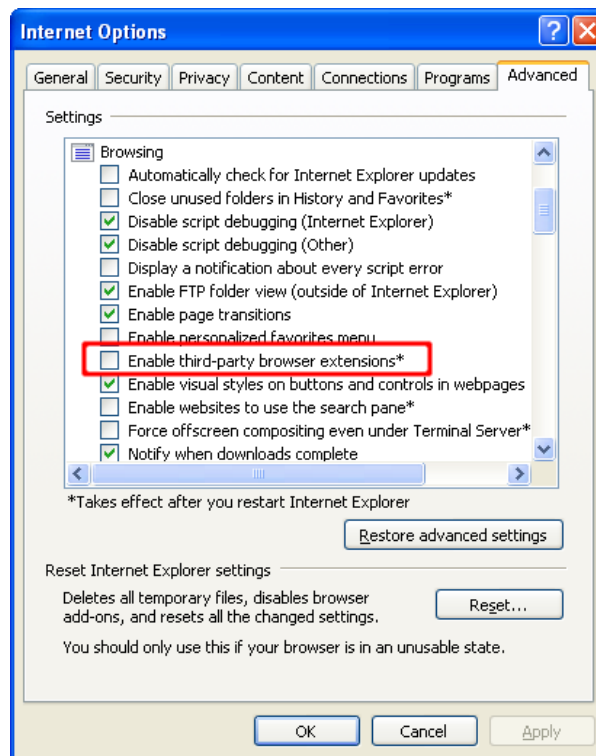


Figure 11 The “Enable third-party browser extensions” setting in Internet Explorer 7

Internationalised Domain Names (IDN) can be abused to allow spoofing of web page addresses. This can allow phishing attacks to be more convincing.

To protect against IDN spoofing in Internet Explorer, enable the “*Always show encoded addresses*” option. This will cause IDN addresses to be displayed in an encoded form in the Internet Explorer address bar and status bar, which will remove the visual similarity to the spoofing target address.

The “*Play sounds in webpages*” option should also be disabled. Sounds in Web pages are not essential to web page content. In fact, they may introduce security risks by having the browser process additional untrusted data. This option is for Internet Explorer's ability to

¹⁴ Browser Helper Objects: DLL modules designed as plug-ins for Microsoft's Internet Explorer web browser to provide added functionality.

natively manage sounds. It will not interfere with other software, such as Adobe Flash or Apple QuickTime.

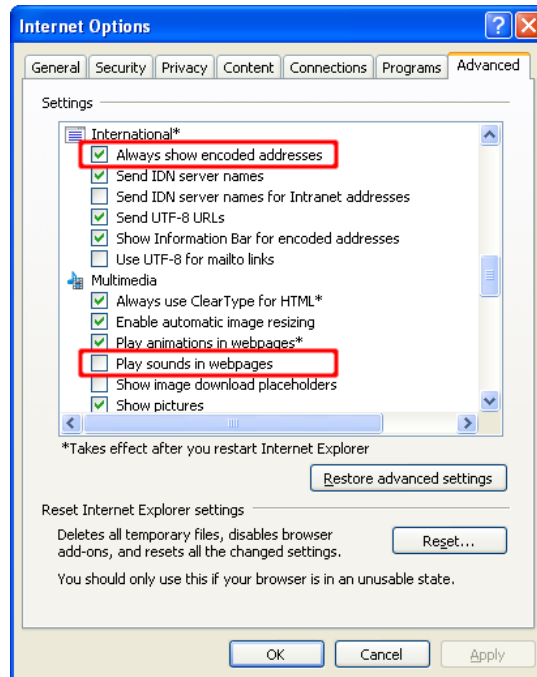


Figure 12 “Encoded addresses” and “sounds” in Internet Explorer 7

5.1.5 Setting Default Applications

Under the “*Programs*” tab, you can state your default applications for viewing web sites, e-mail messages and other network related tasks. Under that option, you can also choose whether to set Internet Explorer as your default Web browser or not.

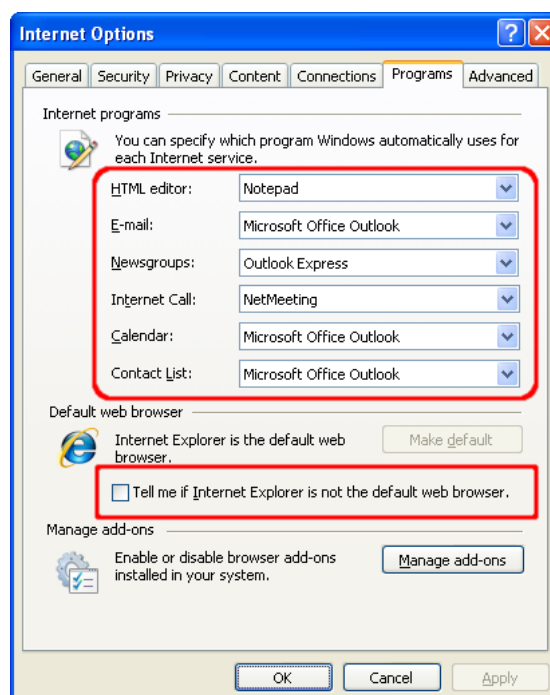


Figure 13 The “Programs” Tab in Internet Explorer 7

5.2 Mozilla Firefox

Mozilla Firefox supports many of the features of Internet Explorer, except for ActiveX and the Security Zone model. Mozilla Firefox does have the basic support for configurable security policies (CAPS), which is similar to Internet Explorer's Security Zone model, however there is no graphical user interface for setting these options.

The following are some steps to disable different features in Mozilla Firefox. Note that some menu options may change between versions or may appear in different locations depending on the host operating system. You should adapt the steps below as appropriate.

To edit the settings for Mozilla Firefox, select “Tools”, then “Options...”

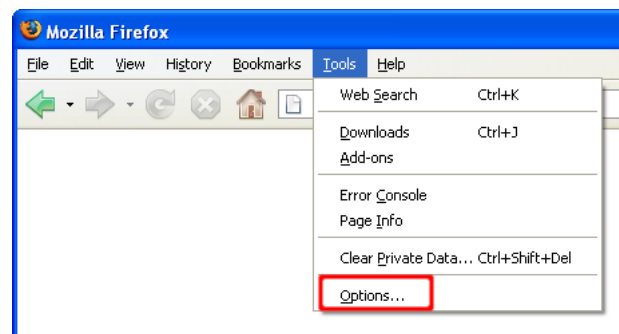


Figure 14 The “Tools” Tab in Mozilla Firefox

You will then see an Options window that has a Category row at the top and the features for that category below. The first category of interest is the “General” category. Under this section, you can set Firefox as your default browser. Also select the option “Always ask me where to save files”. This will make it noticeable when a web page attempts to save a file to your computer.

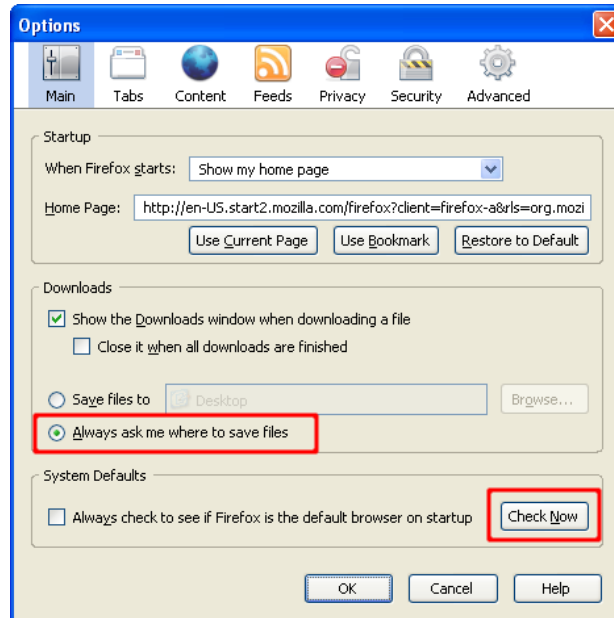


Figure 15 The “Main” Tab in Mozilla Firefox

5.2.1 Browser History and Cookies

Under the “Privacy” category, you will find options for browser “History” and “Cookies”. In the “History” section, disable the option to “Remember what I enter in forms and the search bar”. If the browser remembers these options, it can violate your privacy, especially if the browser is used in a shared environment. Visited page and download history can as well be disabled under that option.

In the Cookie section, select “ask me every time”. This will help make it obvious when a web site is trying to set a cookie.

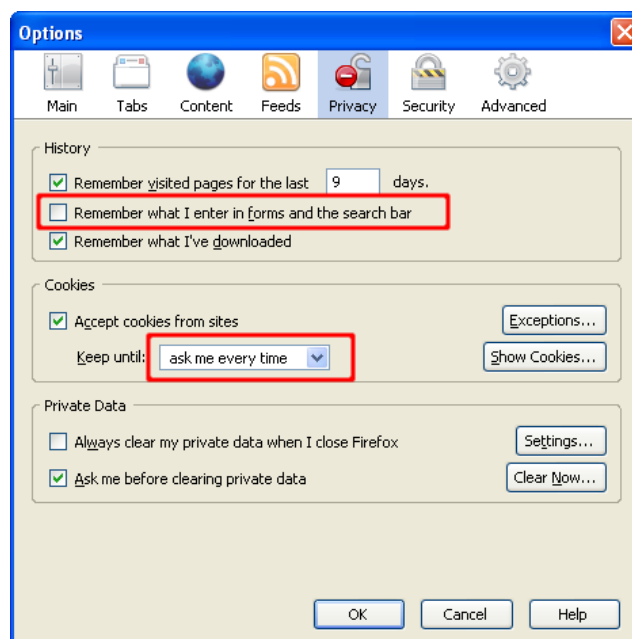


Figure 16 The “Privacy” Tab in Mozilla Firefox

When the user is prompted, the contents of the cookie can be viewed and the user can select the following options: “Deny”, “Allow for Session”, or “Allow”. This gives the user more information about what sites are using cookies and also gives better control of cookies as opposed to globally enabling them. Select “Use my choice for all cookies from this site” to have the browser remember your choice so that you will not be prompted each time you return to the site. Clicking the “Allow for Session” button will cause the cookie to be cleared when the browser is restarted. If prompting for each cookie is too excessive, you may wish to select the “Keep until: I close Firefox” option. This will prevent web sites from being able to set persistent cookies.

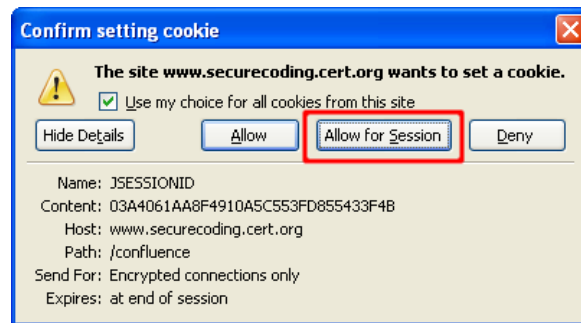


Figure 17 The “Cookie” setting in Mozilla Firefox

Many web browsers will offer the ability to store login information, but this can be risky sometimes. If you want to make use of that feature, ensure that you use the measures available to protect the password data on your computer. Under the “Security” category, the “Passwords” section contains various options to manage stored passwords, and a “Master Password” feature to encrypt the data on your system.

5.2.2 Add-on Options

The “Warn me when sites try to install add-ons” option will display a warning bar at the top of the browser when a web site attempts to take such an action.

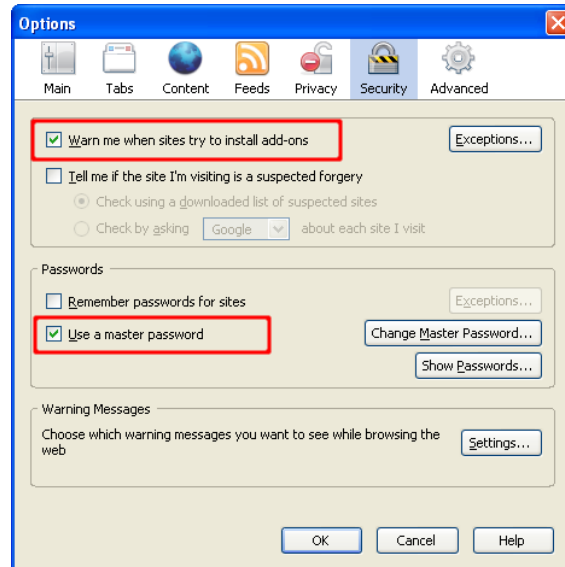


Figure 18 The “Security” Tab in Mozilla Firefox

The “Content” category contains an option to “*Enable Java*”. Java normally allows website designers to run applications on your computer. This feature should be disabled unless required by the trusted site you wish to visit. Again, you should verify if this site is trustworthy and whether you want to enable Java to view the site’s content. Once you have finished visiting the site, Java should be disabled until needed again.

Press the “*Advanced*” button to disable specific JavaScript features. All of the options displayed in this dialog box should be disabled when not needed.

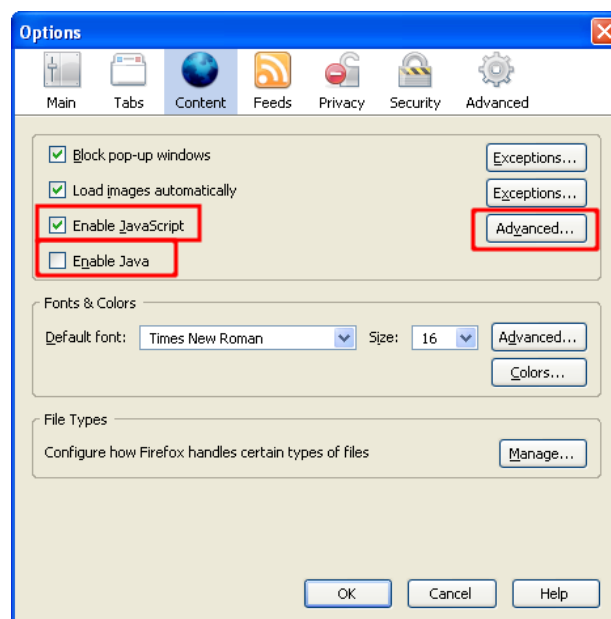


Figure 19 The “Content” Tab in Mozilla Firefox

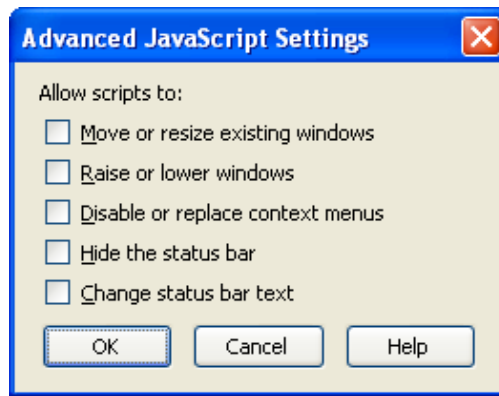


Figure 20 The “Advanced JavaScript” Settings in Mozilla Firefox

The “Content” section has an option to alter actions taken when files are downloaded. Each time a file type is configured to automatically open with an associated application, this can make the browser more dangerous to use. Vulnerabilities in these associated applications can be exploited more easily when they are configured to automatically open. Click the “Manage” button to view the current download settings and modify them if necessary.

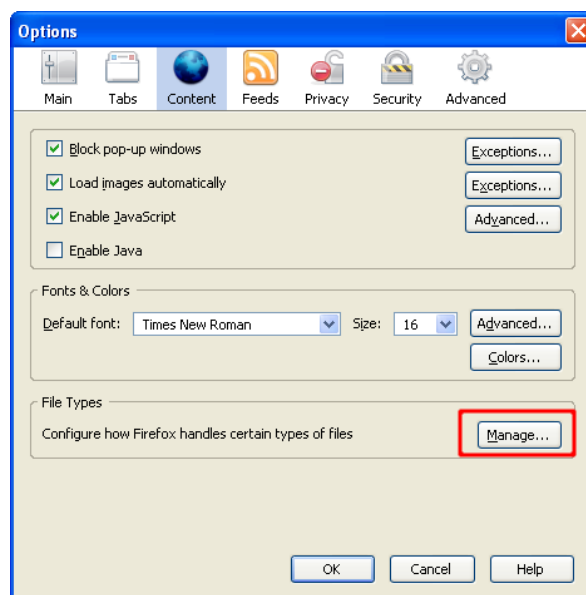


Figure 21 The “Manage” button in Mozilla Firefox

5.2.3 Download Settings

The “Download Actions” dialog box will show the file types and the currently configured actions to take when the browser encounters such a file. For all listed file types, either select “Remove Action” or “Change Action...” to modify the action to save the file to the computer. This increases the amount of user action required to launch the related applications, and will therefore help prevent automated exploitation of vulnerabilities that may exist in these applications.

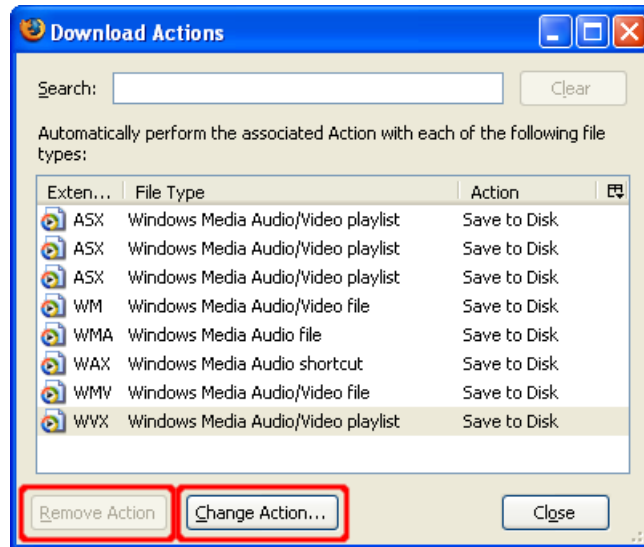


Figure 22 The “Download Actions” dialog box in Mozilla Firefox

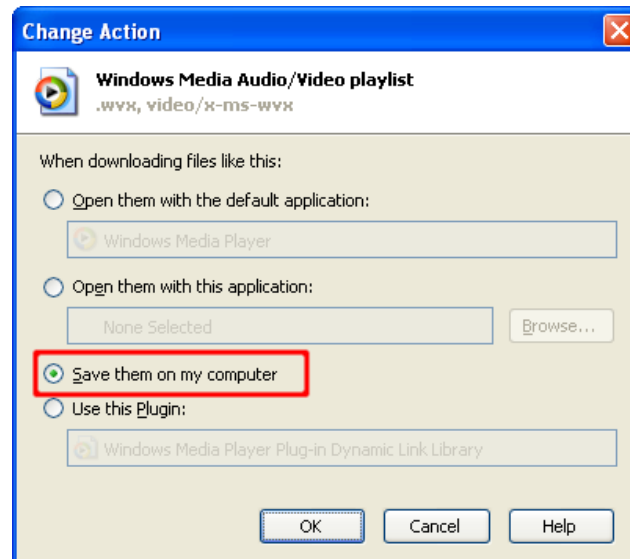


Figure 23 The “Change Action” dialog box in Mozilla Firefox

5.2.4 Privacy Feature

Firefox 1.5 and later include a feature to clear private data. This option can remove sensitive information from the web browser. Select “*Clear Private Data...*” from the “*Tools*” menu to use this privacy feature.

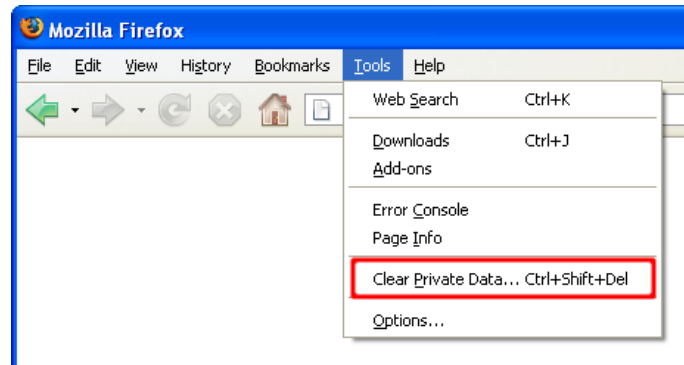


Figure 24 The “Clear Private Data” option in Mozilla Firefox

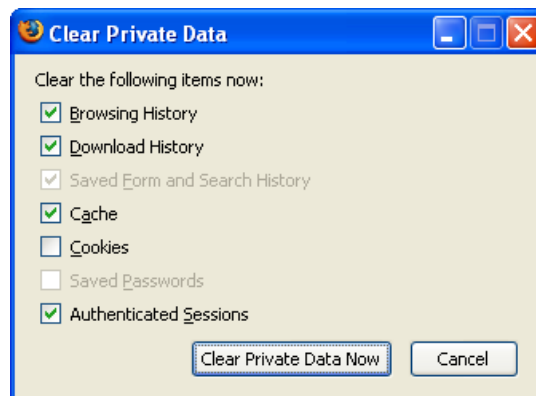


Figure 25 The available options for clearing private data in Mozilla Firefox

5.2.5 NoScript Feature

Because Firefox does not have easily-configured security zones like Internet Explorer, it can be tricky to configure the web browser options on a per-site basis. For example, a user may wish to enable JavaScript for a specific, trusted site, but have it disabled for all other sites. This functionality can be added to Firefox with an add-on, such as “*NoScript*”.

With “*NoScript*” installed, JavaScript will be disabled for sites by default. The user can allow scripts for a web site by using the “*NoScript*” icon menu. Scripts can be allowed for a site on a temporary or a more permanent basis. If “*Temporarily allow*” is selected, then scripts are enabled for that site until the browser is closed.

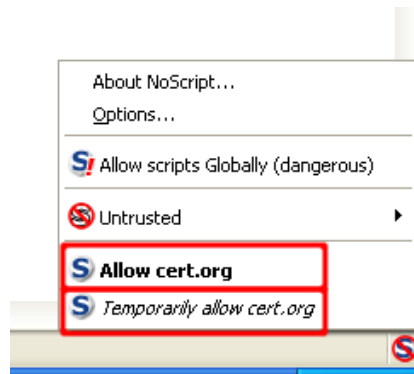


Figure 26 The “NoScript” Menu in Mozilla Firefox

Many Web browser vulnerabilities require scripting, hence, configuring the browser to have scripting disabled by default greatly reduces the chances of exploitation. To enhance this protection, “NoScript” can be configured to also block Java, Flash, and other plug-ins by default. This can help to mitigate any vulnerabilities in these plug-in technologies. “NoScript” will replace these elements with a placeholder icon, which can be clicked to enable the element. Click the “NoScript” icon and then click “Options...” to get to the “NoScript” configuration screen.

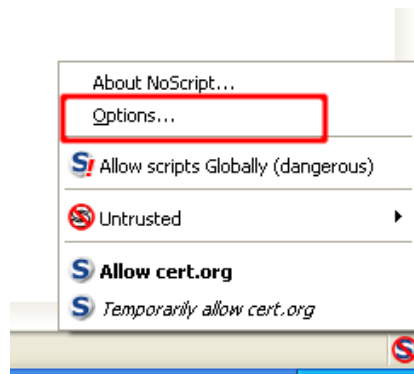


Figure 27 The “Plugins” Tab in Mozilla Firefox

5.2.6 Plugins Feature

On the “Plugins” tab, select the options as follows:

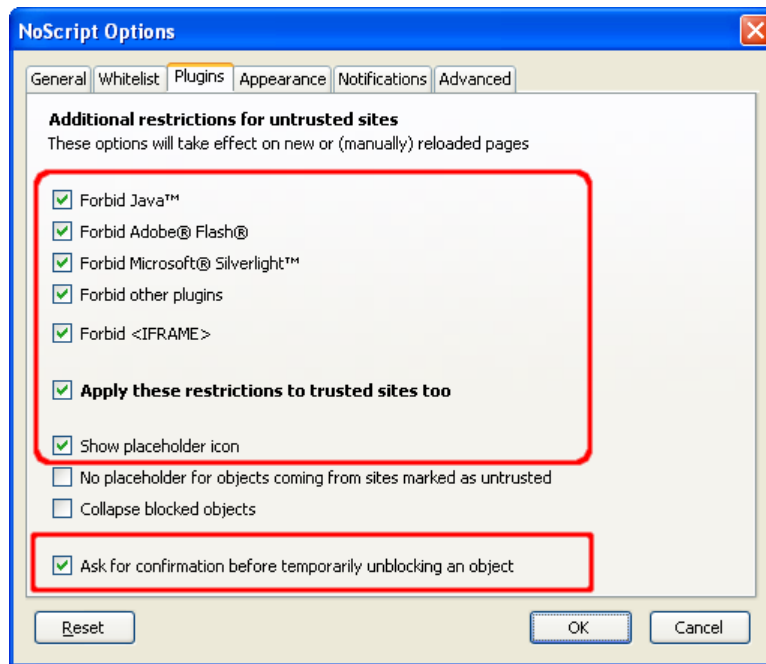


Figure 28 The “plugins” options in Mozilla Firefox

Apart from visiting malicious websites, users can also be put at risk when a legitimate, trusted site is compromised. Hence, you should select “*Apply these restrictions to trusted sites too*”. If enabling this option is too annoying, it can be turned off at the cost of increased risk.

5.3 Apple Safari

The Safari Web browser is very much similar to Mozilla Firefox in terms of the features it supports. Below are some steps to disable several features in Safari on Mac OS X. The options for Safari for Microsoft Windows may differ slightly. Also note that some menu options may change over time, and you should adapt the steps below as appropriate.

In order to change settings for Safari, select “*Safari*” then “*Preferences...*”. On the Safari menu, you can also select the option “*Block Pop-up Windows*”.

This option will prevent sites from opening another window by making use of scripting or active content. While Pop-up Windows are often associated with advertisements, some sites may attempt to display relevant content in a new window. Therefore, setting this option may disable the functionality of some sites.

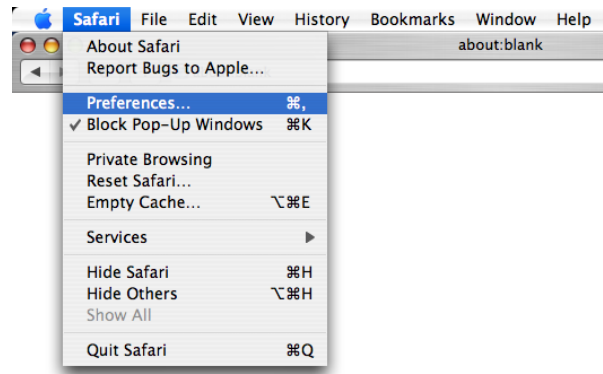


Figure 29 The “Preferences” option in Safari

5.3.1 Preferences Menu

Once you select the “*Preferences*” menu, the window below will open. The first tab to look at is the “*General*” tab. On this tab you can set up many options such as “*Save downloaded files to:*” and “*Open “safe” files after downloading*”. Files should ideally be downloaded to a folder that you create for that purpose. The option “*Open “safe” files after downloading*” should also be deselected.

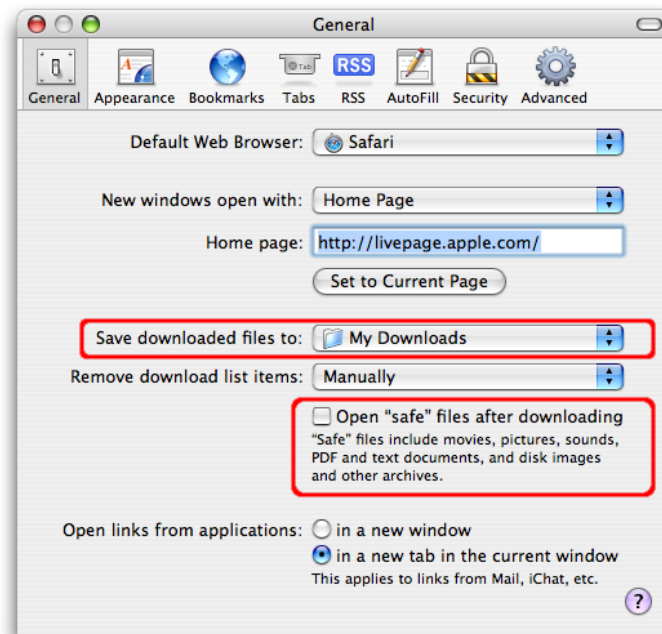


Figure 30 The “General” Tab in Safari

5.3.2 AutoFill Feature

On the “*AutoFill*” tab, you can select what types of forms your browser will automatically fill in. In general, using “*AutoFill*” features is not really a good idea. If someone can gain access to your machine, or the “*AutoFill*” data files, then the “*AutoFill*” feature may allow them to use the stored credentials to access other sites that they would not otherwise have

access to. However, if used with appropriate protective measures, it may be adequate to enable “*AutoFill*”. Filesystem encryption software such as **OS X FileVault** could be used along with the “*Use secure virtual memory*” option to provide additional security for files that reside in a user's home directory.

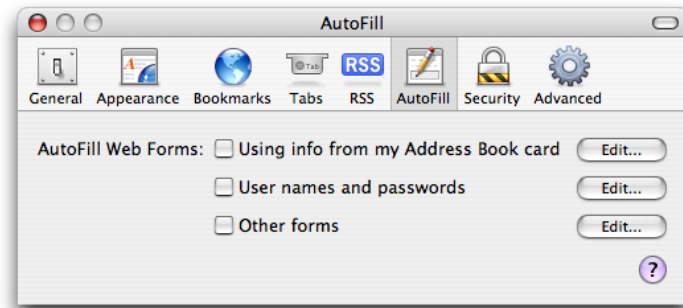


Figure 31 The “AutoFill” Tab in Safari

5.3.3 Security Options

The “*Security*” tab offers several options. The “*Web Content*” section allows you to enable or disable various forms of scripting and active content. It is advised to disable the first three options in this section, and only enabling them based on site-specific cases. It is also recommended to select the “*Block Pop-up Windows*” option. This option will prevent sites from opening another window through the use of scripting, or active content. Again, while Pop-up Windows are often associated with advertisements, some sites may attempt to display relevant content in a new window. Therefore, setting this option may disable the functionality of some sites.

It is safer to use Safari without plug-ins and Java, so disabling the options “*Enable plug-ins*” and “*Enable Java*” is a good advice. It is also safer to disable JavaScript. However, many web sites require JavaScript for proper operation.

In this dialog box, you can disable cookies and also view or remove cookies that have been set. In general we should disable cookies, and enable them only when you visit a site that requires their use. At this point, you should determine if the site is trustworthy and whether you want to enable cookies to view the site's content. After having visited the site, the cookies should be disabled until needed again. You can choose to only accept cookies from the sites that visit by selecting the “*Only from sites you navigate to*” option. This will permit sites that you visit to set cookies, but not third-party sites. Finally, selecting the “*Ask before sending a non-secure form to a secure website*” option is highly recommended. This will

prompt you before sending unencrypted form data when viewing an HTTPS-secured web site.

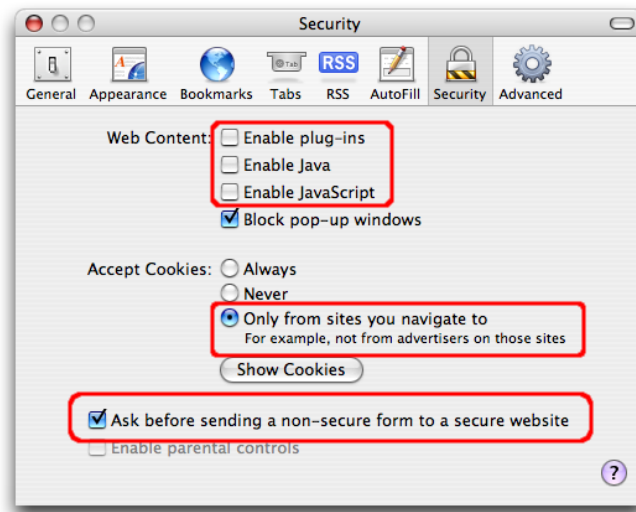



Figure 32 The “Security” Tab in Safari

5.4 Google Chrome

Google Chrome has security measures in place to help protect you as you surf the Internet. Follow these steps to adjust these settings:

1. Click the wrench icon  on the browser toolbar.
2. Select “Options” (“Preferences” on Mac and Linux; “Settings” on Chrome OS).
3. Click the “Under the Hood” tab.

Here are the various settings you can adjust (Do not change these settings unless you are confident about what you are doing. You can always click “Reset to defaults” in the Options dialog to clear any changes you have made):

- **Phishing and malware protection:**
This option is enabled by default in the "Privacy" section. When enabled, Google Chrome warns you if it detects that the site you are trying to visit is potentially a phishing one or contains malware.
- **SSL certificates and settings:**
Go to the “Security” section to manage your SSL certificates and settings.
- **Web content settings:**

Click “Content settings” in the “Privacy” section to set your permissions for cookies, images, JavaScript, plug-ins, pop-ups, and location sharing. All Web contents, except for pop-ups, are allowed by default.

5.4.1 Privacy Settings

Several Google Chrome features use your personal information, such as the web pages you are visiting, to enhance and protect your experience on the Web. These features are described below:

- **Suggestions for navigation errors**

In cases where the web address does not resolve or a connection cannot be established, Google Chrome can show suggestions for the page you were trying to reach. The browser sends Google the URL of the page you are trying to reach in order to provide you suggestions of alternative or similar Web pages.

- **Predictions in the address bar**

The browser can use a prediction service to show you related queries, matches from your browsing history, and popular websites as you type in the address bar. If your default search engine uses Google's prediction service, Google Chrome sends the text you type in the address bar to Google in order to retrieve suggested searches and sites, which are then displayed in the address bar menu. Google only records a random two percent of this information received from all users and the information is anonymised within 24 hours.

- **DNS pre-fetching**

DNS pre-fetching stands for Domain Name System pre-fetching. When you visit a webpage, Google Chrome can look up, or pre-fetch, the IP addresses of all links on the webpage. Browsers use the IP address to load a webpage, so by looking up this information in advance, any links you click on the webpage will load faster.

- **Phishing and malware protection**

Get an instant alert whenever Google Chrome detects that the website you are going to may be harmful. The browser sends a partial copy of the URL you are visiting to Google to check it against a list of known phishing and malware sites.

- **Usage statistics and crash reports**

These are meant to help Google prioritise the features and improvements they should work on. You could allow your browser to send Google information about your installation of the browser and information from files, applications, and services that are running whenever you experience a browser crash. Google

Chrome does not send other personal information, such as name, email address, or Google Account information.

- **Cookie settings**

By default, Google Chrome saves all cookies onto your computer, but you can restrict how it handles different types of cookies.

All of these features (except usage statistics and crash reports) are enabled by default. You can always choose to disable them by clicking the wrench icon  and selecting “Options” (“Preferences” on Mac and Linux) > “Under the Hood” tab.

5.4.2 Phishing and malware detection

Google’s “Safe Browsing” technology is used in Chrome mainly to warn you if the site you are trying to visit is suspected of phishing or malware.

- **Google Chrome phishing and malware alerts**

These messages appear when phishing and malware detection is enabled:


Message	Meaning
Warning: Something's Not Right Here!	This message appears if Google Chrome detects that the site you are trying to visit may have malware.
This is probably not the site you are looking for!	This message appears when the URL listed in the site's certificate does not match the site's actual URL. The site you are trying to visit may be pretending to be another site.
The site's security certificate is not trusted!	This message appears if the certificate was not issued by a recognised third-party organisation. Since anyone can create a certificate, Google Chrome checks to see whether a site's certificate came from a trusted organisation.

<p>The site's security certificate has expired!</p> <p>or</p> <p>The server's security certificate is not yet valid!</p>	<p>These messages appear if the site's certificate is not up-to-date. Therefore, Google Chrome cannot verify that the site is secure.</p>
<p>The server's security certificate is revoked!</p>	<p>This message appears if the third-party organisation that issued the site's certificate has marked the certificate as invalid. Therefore, Google Chrome cannot verify that the site is secure.</p>

Table 1 Phishing and Malware Alerts in Chrome


- **Disable phishing and malware detection**

The following instructions apply to Google Chrome on Windows, Mac, Linux, and Chrome Operating System.

1. Click the wrench icon  on the browser toolbar.
2. Select “Options” (“Preferences” on Mac and Linux; “Settings” on Chrome OS).
3. Click the “Under the Hood” tab and find the “Privacy” section.
4. Deselect the “Enable phishing and malware protection” checkbox.

5.4.3 Images, JavaScript, and other Web Content Settings

Use the “Content Settings” dialog to manage the following settings: cookies, images, JavaScript, plug-ins, pop-ups, location sharing, and notifications. Follow the steps below to adjust these settings. These steps apply to Google Chrome on Windows, Mac, Linux, and Chrome OS.

1. Click the wrench icon  on the browser toolbar.
2. Select “Options” (“Preferences” on Mac and Linux; “Settings” on Chrome OS).
3. Click the “Under the Hood” tab.
4. Click “Content settings” in the “Privacy” section.

5.4.4 Managing Exceptions

Click “*Manage exceptions*” in any section to customise how resources for specific websites should be handled. You can enter hostnames and IP addresses, as well as specific domain masks (for example enter `[*].google.com` to match everything from `google.com` and `www.google.com`, but not `othergoogle.com`).

5.5 Opera

This section is about the different security information that is displayed in the Opera browser. This information helps you to decide if each website is the right site and is trustworthy, which is especially important when entering private or financial information. The security information to look for in the browser is shown and described below.

5.5.1 The Address Field (1)

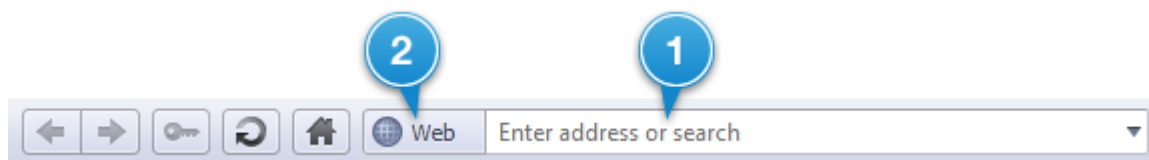


Figure 33 The “Address” Field in Opera

The address for the webpage is displayed in the address field. This contains the registered name of a company, organisation or person that identifies the specific computer on the Internet that is storing the webpage you requested. This is called a domain name, and ends with a suffix, such as `.com`, `.org`, `.gov`, or `.edu`, to indicate the type of organisation. To make it even easier for you to see exactly where you are, the most important part of the address is highlighted. The protocol, such as HyperText Transfer Protocol (HTTP), and some parameter details are hidden. To see the full address, click the address field. You can disable this feature and display the full URL for all Web pages. From the menu, select “*Settings*” > “*Preferences*” > “*Advanced*” > “*Browsing*” and select “*Show full URL in address field*”.


Opera supports internationalised domain names (IDN), which allows domain names in languages such as Russian and Chinese to be written in their own native scripts. Opera will always display domain names in such a way that no two domains will look alike.

Tips:

- Before providing sensitive information, check whether the highlighted part of the address looks like where you expected to be. If it looks wrong, investigate further or consider carefully before entering personal information.

- If you arrived at this website using links from another webpage or e-mail, type the web address into the address field yourself. This ensures that you are directed to the correct website and have not been misdirected.

5.5.2. Opera's Security Badge (2)

The security badge indicates the security of the website. Always look for a badge containing a padlock symbol , which indicates a webpage with a good level of protection. Some websites automatically open a separate window with the address bar hidden. In this case, Opera displays the security bar as a collapsed address bar that shows the domain to which that the window belongs. Check that the domain matches the domain that you were expecting and click the collapsed bar to show the full address bar and security bar. Also, avoid using shortcuts that hide the address bar, such as “*F11*” for full screen mode in Opera, if you want to view the security information of a website.

The table below describes the security badges used in the Opera browser:

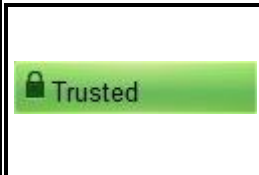
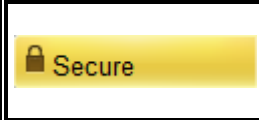
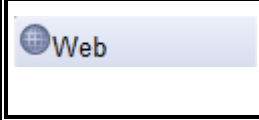
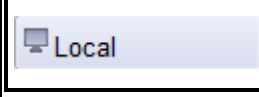
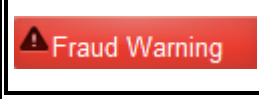

Security badge	Status
	Maximally secure site, with Extended Validation (EV) , where the identity of the owners of the website have been thoroughly verified
	Secure site, where the credentials of the site owner have been checked
	Normal site, or a site where there are problems with encryption, or where information is not available to enable verification
	File or folder on your computer
	Site that has been listed as a known fraudulent site
	Site that has been listed as a known malware site

Table 2 Security Badges in Opera

Note: The badge may also indicate that “*Opera Turbo*¹⁵” is enabled.

¹⁵ Opera Turbo: Opera Turbo Mode is a new feature in Opera 10 Browser that allows a page to load much faster by compressing the image.

5.5.3 Security Information

To see security information, click the security badge. Summary information displays, as shown in the example below.

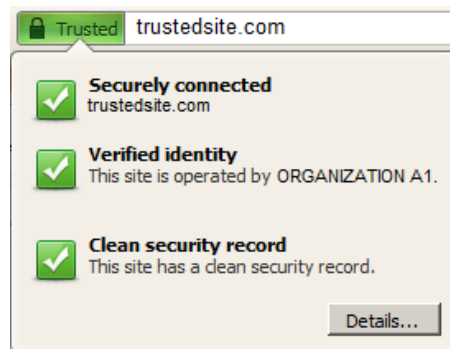


Figure 34 Security Information in Opera

The summary describes the type of connection and may provide notes about the security record or organisation running the site. For more information, click the “*Details...*” button. This displays the “*Security Information*” dialog, which provides information in three tabs, as shown and described below.

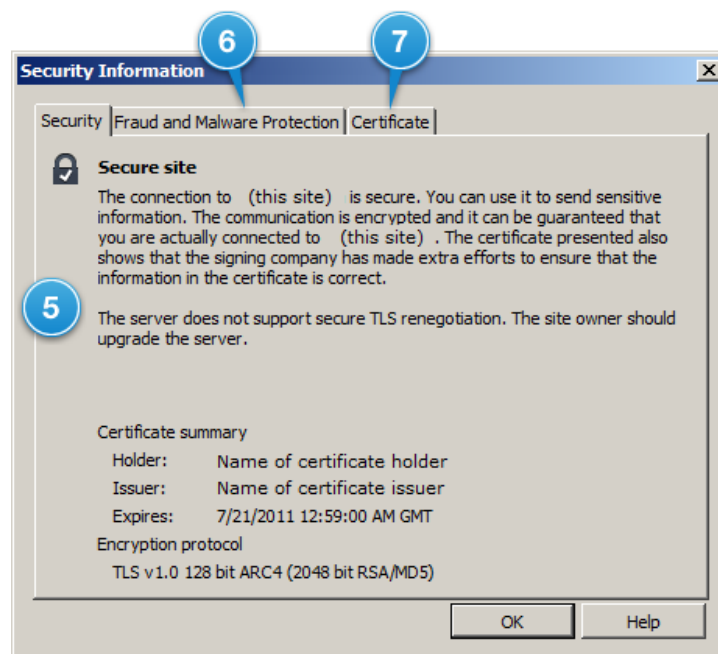


Figure 35 The “Security Information” dialog box in Opera

Security tab (5)

The “*Security*” tab tells you about the following:

- The level of security for the site
- The type of encryption used
- The security certificate summary


Fraud and Malware Protection tab (6)

When you select the “*Fraud and Malware Protection*” tab, it runs a check and tells you if the website has been reported as harmful or fraudulent. It also allows you to:

- Report the site for fraud or malware
- Disable/enable Opera’s Fraud and Malware Protection

With Opera “*Fraud and Malware Protection*” enabled, every webpage you request is subjected to phishing and malware filters. The security status of the page is displayed in a security badge in the address field. If a website is found on lists of known, suspicious sites, a warning page may display before the page is shown. You decide whether to visit the questionable website, to return safely to the browser home page, or to read additional information about the status of the page. If you open a phishing or malware page, it will be marked with a red “*Fraud Site*” or “*Malware site*” indicator, as shown in the table above.

A site is considered secure if it has the following features:

- Its encryption level should be good enough to protect the traffic between you and the website, so that a third party listening in will not be able to see the data that is transferred. This is indicated by a padlock .
- It should have a valid security certificate, which provides some assurance that you have reached the intended website and not some impostor.

Certificate tab (7)

The “*Certificate*” tab provides specific and detailed information about the security certificate, such as the server name of the secure site, the organisation name and country, the expiry date and who issued and signed the security certificate (Certificate Authority).

The rise in the number of fraudulent websites has highlighted the importance of certification. Opera is a member of “*CA/Browser Forum*”, a voluntary organisation of leading certification authorities (CAs) and browser vendors, and is part of the decision-making process in creating certificate standards.

If an organisation’s website looks suspicious, check the following:

- **Certificate validity**

Most of the time, certificates are fully valid. If there is something questionable about a certificate, a warning dialog will be displayed. You may choose to proceed, but full security cannot be guaranteed. Warnings include the following:

- ✓ **Server certificate expired**

Certificates have expiry dates, and they must be renewed on a regular basis by whoever maintains the site. Accepting an expired certificate does not necessarily reduce security, but consider the site you are visiting and how long it has been since the certificate expired, before accepting.

✓ **Wrong certificate name**

A certificate is issued by an authority for a single site to use, and sites cannot borrow certificates from each other, as this invalidates the whole concept of certificates. It is normally not advised to accept a certificate belonging to another site.

✓ **Certificate signer not found**

If the signer of a certificate is not found in your list of authorities, only accept the certificate if you are absolutely confident that whoever is running the site in question can be trusted.

• **Self-signed certificates**

Some certificates are self-signed, which means that they are signed by the website owners themselves, and not an independent authority. Be aware that the browser cannot certify that the certificate comes from the person or organisation stated. If you know that the signer can be trusted, and you want all sites using this signer to be considered as safe, install the certificate to add the signer to your list of authorities.

• **Manage certification**

Opera, like all secure browsers, comes with a list of authorities that can issue certificates. This is upgraded with each new release of the Opera browser. To display a list of the authorities currently being used and your installed certificates, click "*Manage certificates*".

5.6 Netscape Navigator

Note that official support for Netscape has ended on March 1st, 2008. If you are using Netscape, it would be wise to switch to a browser that is still supported.

6.0 Conclusion

Web browsers are used by almost everyone nowadays. Very often, they come out the box, without any security settings configured. The use of a Web browser with its default settings, that is, with no security, can lead to a variety of computer issues, ranging from spyware being installed on your computer without your knowledge, to intruders taking full control of your machine, performing all kinds of malicious activities. Therefore, it is very important that users know about the underlying risks and understand how to secure their Web browsers.

7.0 References

- Wikipdia: <http://en.wikipedia.org>
- Spamlaws: <http://www.spamlaws.com>
- US CERT: <http://www.us-cert.gov>
- CERT ORG: <https://www.cert.org>
- Google Chrome: <http://www.google.com/support/chrome>
- Opera: <http://www.opera.com>
- Netscape: <http://www.nsa.gov>
- Addictivetips: <http://www.addictivetips.com>

Appendix A

Security Terms Explained

Adware

Short for “Advertising-supported Software”, adware is any software package which automatically plays, displays, or downloads advertisements to a computer. These advertisements can be in the form of a pop-up. The object of the Adware is to generate revenue for its author.

Encryption

Encryption protects your data while it is being sent from your browser to the website. It is a way of scrambling information sent so that only a legitimate recipient of that information can make it readable again. The most common form of encryption today is public key encryption. Imagine a strongbox that has two keyholes and two separate keys.

Certificate Authority

A certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified.

HTTP

This is an abbreviation for “Hypertext Transfer Protocol” and is the most common method of accessing information on the Internet. When you request a webpage, information about your browser and the address of the requested page is sent to the receiving server. The server sends back some information about what you requested, for instance whether it is a webpage, just an image, or a file to be downloaded, as well as what you actually requested.

HTTPS

This is an abbreviation for “Hypertext Transfer Protocol Secure” and is a secure version of HTTP. HTTPS allows your web browser to verify the identity of the server from which it is getting information, as well as to encrypt the information so that nobody else would be able to understand it. While HTTPS is generally considered to be the more secure protocol, HTTPS does not automatically mean that you have a totally secure connection.

IDS

This is an abbreviation for “Intrusion Detection System” and is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

IPS

This is an abbreviation for “Intrusion Prevention System” and is a network security appliance that monitors network and/or system activities for malicious activity. The main functions of an intrusion prevention system are to identify malicious activity, log information about mentioned activity, attempt to block/stop activity, and report activity.

Malware

Short for “Malicious Software”, malware consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorised access to system resources, and other abusive behaviour.

Phishing

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

SSL

SSL stands for "secure sockets layer" and encrypts data with two keys. It is available as SSL versions 2 and 3. SSL version 3 is better than version 2, which is being phased out and is only used by a small number of websites these days.

Spyware

Spyware is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect.

TLS

TLS is short for "transport layer security", a security protocol based on its predecessor, SSL. This is considered the most secure protocol in common use today as versions TLS 1.0 and TLS 1.1.

Trojan

A Trojan is a destructive program that masquerades as a being application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but (perhaps in addition to the expected function) steals information or harms the system.

Vulnerability

A vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.