Security for Microsoft Internet Explorer

Some software features that provide functionality for a browser such as ActiveX, Java, and Scripting (JavaScript, VBScript ...) can also cause vulnerabilities to computer systems. They can arise from the poverty of protocol, design and software

IV, Make planes to protect your browser

Some software features that provide functionality for a browser such as ActiveX, Java, and Scripting (JavaScript, VBScript .) can also cause vulnerabilities to computer systems. They can arise from the poor of protocols, designs and software that are written or configured insecure. For many reasons, you should understand which browser supports what features and what risks can happen to them. Many browsers allow you to disable these technologies while others can only allow you to reduce their functionality.

In this section, we will show you how to safely configure the most popular browsers and how to disable the features that might cause the vulnerability mentioned above. If a company doesn't provide documentation for how you can protect the browser, we recommend that you contact them and ask them about it.

Browsers are regularly upgraded. Depending on the version of the software, features and options may vary.

A, Microsoft Internet Explorer

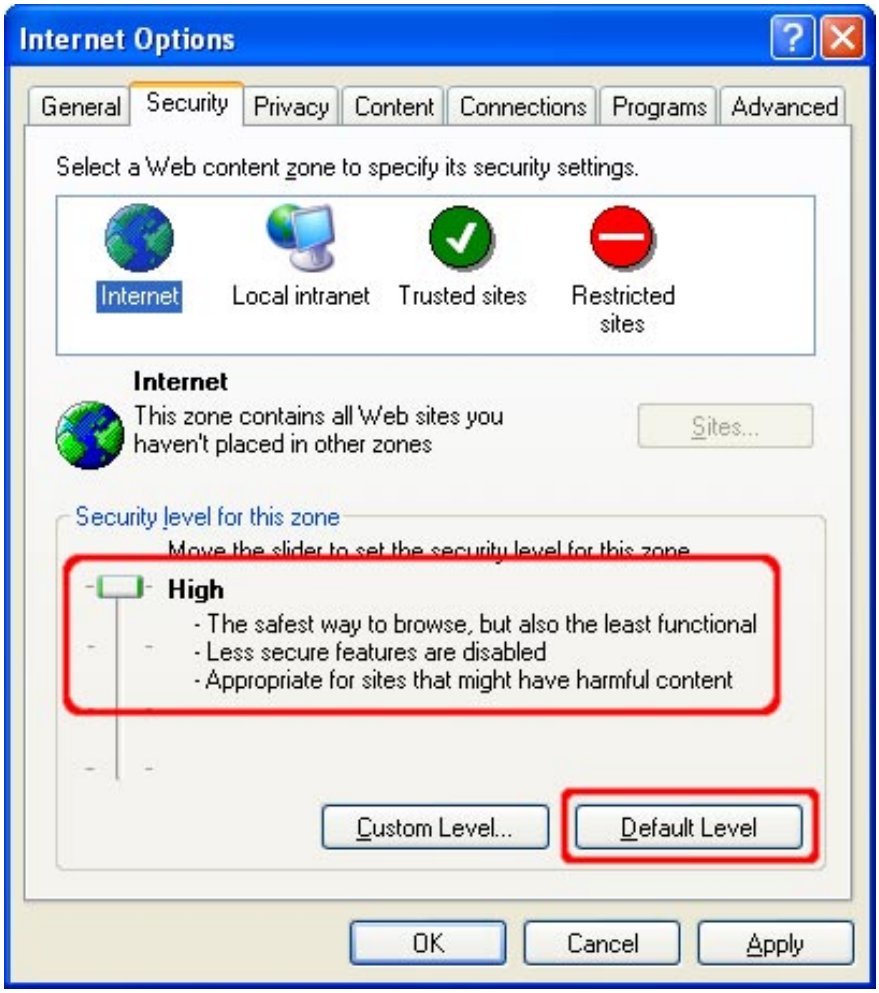
Microsoft Internet Explorer is a browser built into the Microsoft Windows operating system. Therefore, removing this application is completely unrealistic.

In addition, the browser supports Java, script execution scripts and other forms of active components and Internet Explorer also add ActiveX technology. When any application has a potential vulnerability, it is possible to significantly reduce the number of dangerous vulnerabilities by using a browser that does not support ActiveX controls. However, using a number of alternate browsers may affect the functionality of some pages that require ActiveX controls. Note that using another browser will not remove Internet Explorer or other components from the system. Other software such as the user's email browsing software may involve Internet Explorer, browser ActiveX controls or MSHTML. Using these products may be as risky as described above. The 2000 CERT / CC ActiveX conference results can be found at http://www.cert.org/reports/activeX_report.pdf for further research.

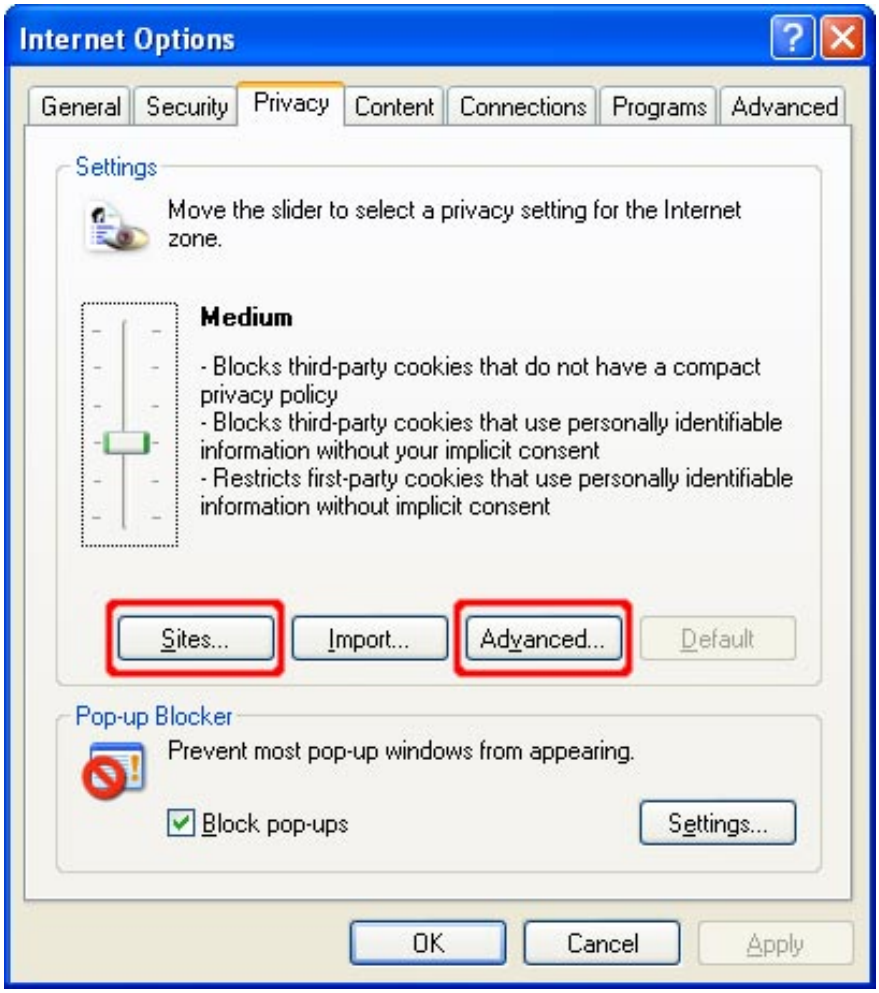
Here are some steps to disable features in Internet Explorer. Note that the options menu may vary for different versions of Internet Explorer, so you should adjust the steps below accordingly.

To change settings for Internet Explorer, select ***Tools*** then ***Internet Explorer .***

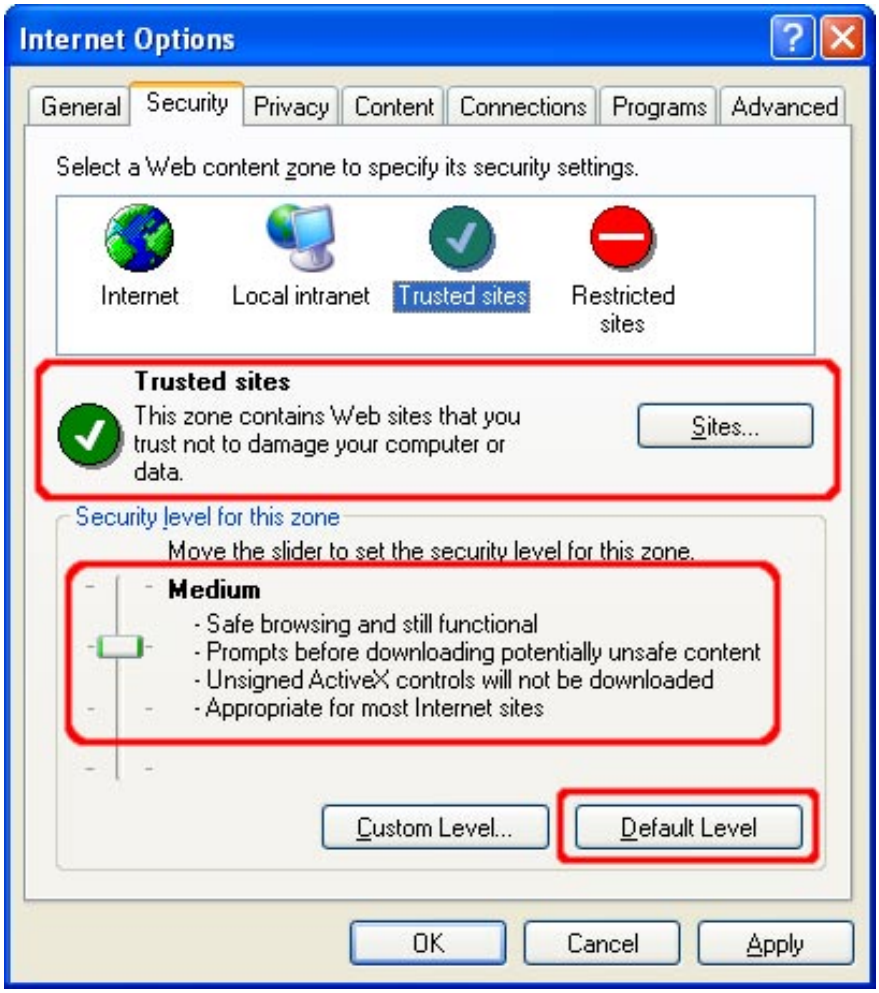
Select the ***Security*** tab. On this tab you will find in the above section a list of different security areas that Internet Explorer uses. You can go to ***Setting Up Security Zones address*** to get more information about security zone. For each region, you can choose an optional level of protection. Click the ***Custom Level*** button and you will see the second window opened and allow you to select the protection settings for those areas. The Internet zone is where all web sites start to be approved. The security settings for this zone are applied to all pages not listed in another security zone. We recommend using the ***High*** level for this area. With ***High*** select, some features including ***ActiveX*** , ***Active scripting*** and ***Java*** will be disabled. With the features disabled, your browser will be more secure. Click the ***Default Level*** button and then drag the control bar to ***High*** .

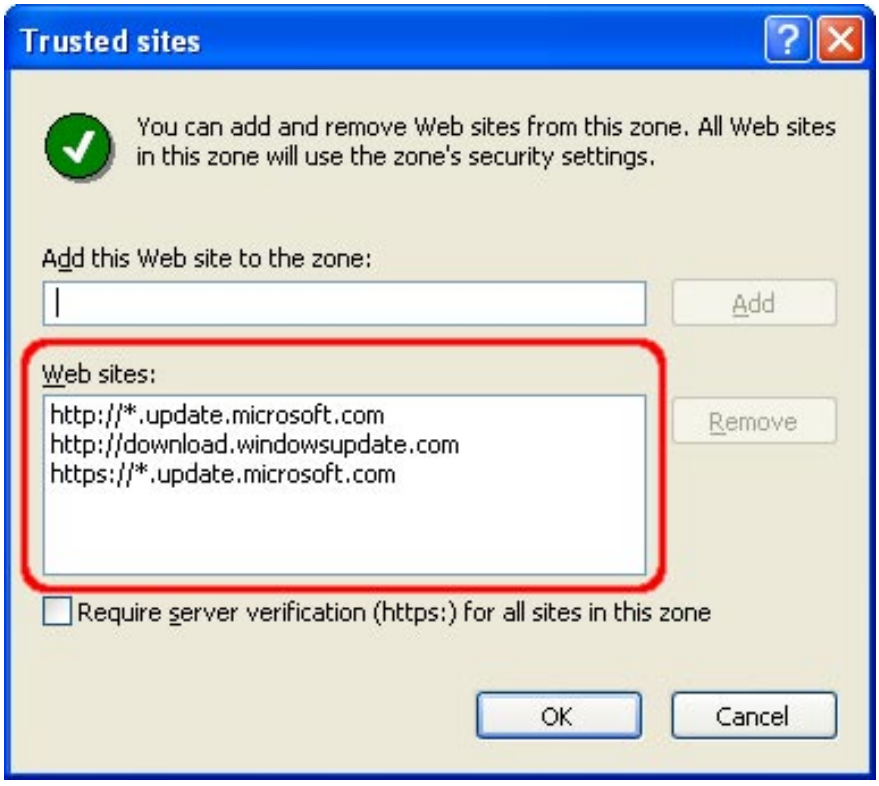


To adjust the features in each zone, click the ***Custom Level*** button. Here you can control specific security options that apply to that area. The default values ??for high security settings can be selected by selecting ***High*** and clicking the ***Reset*** button to accept the change.



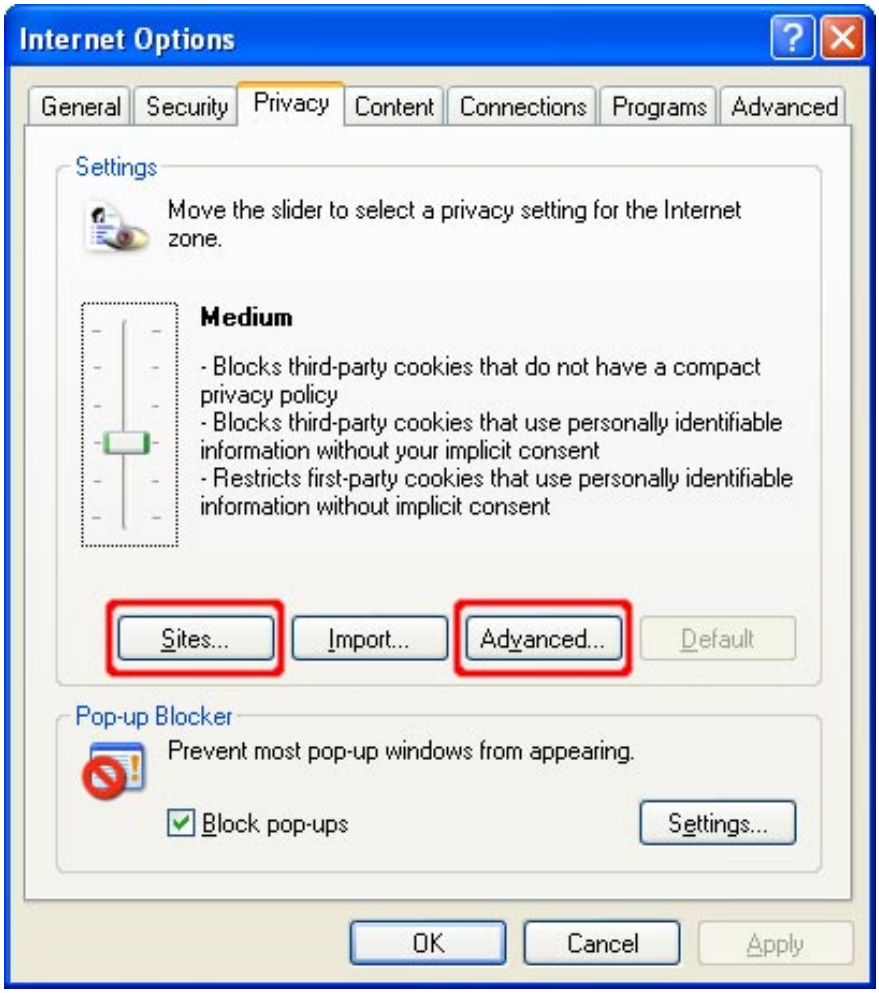
Trusted sites are a secure area for websites you trust that have been designed to be safe and reliable. To add or remove pages from this zone, you can click the ***Sites*** button . This will help you open a new window and will list you with a list of sites that you trust and allow you to add or remove pages here. You can also request that only these pages be added with ***Secure Sockets Layer*** (SSL) that can be enabled in this zone. This allows you to verify that the page you are visiting is a secure site.


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Select a Web content zone to specify its security settings.
Internet
Local intranet
Trusted sites
Restricted sites
Trusted sites
This zone contains Web sites that you trust not to damage your computer or data.
Sites...
Security level for this zone
Move the slider to set the security level for this zone.
Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites
Custom Level...
Default Level
OK
Cancel
Apply

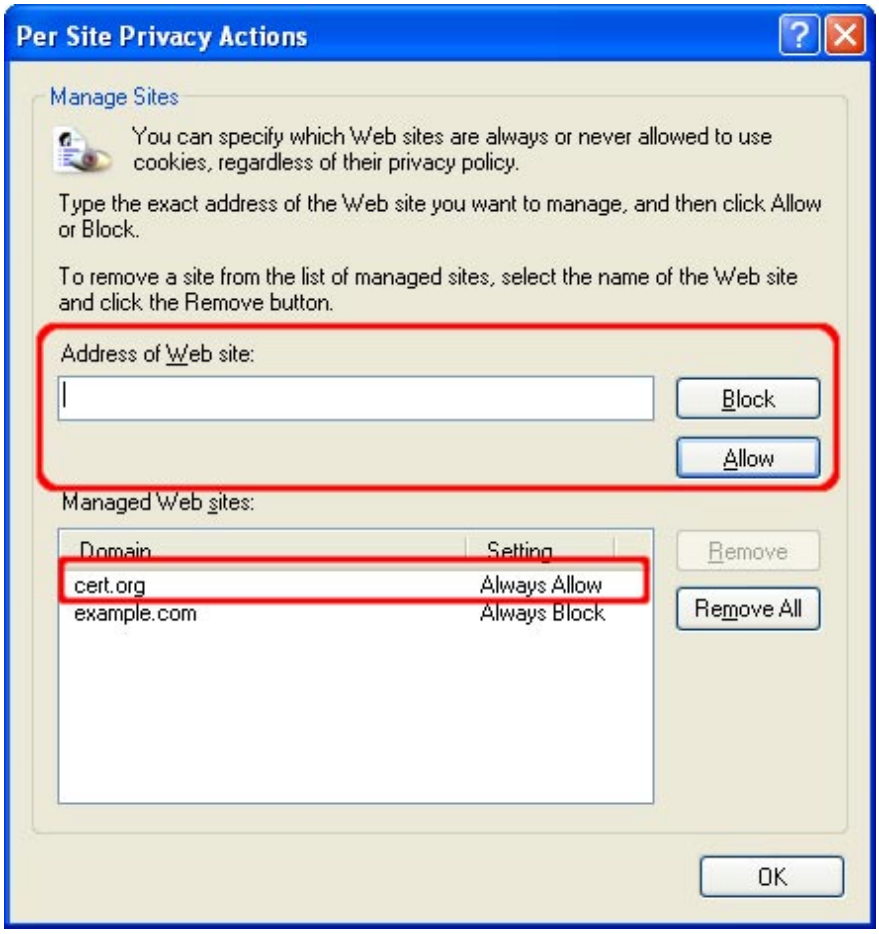

Trusted sites
You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.
Add this Web site to the zone:
Add
Web sites:
http://*.update.microsoft.com
http://download.windowsupdate.com
https://*.update.microsoft.com
Remove
Require server verification (https:) for all sites in this zone
OK
Cancel

We recommend setting security levels for ***Trusted sites*** in ***Medium*** mode. When ***Internet Zone*** is set to a high level, you may encounter problems that pages do not have enough of their functions due to one or more related security settings. This is where Trusted sites can help you. If you believe that the site will not contain malicious code, you can add it to the list of sites in the Trusted sites area. When a page is added, features like ActiveX and active scripting will be activated. The benefit of this type of configuration is that Internet Explorer will be more secure and pages can be 'whitelisted' in the Trusted sites to increase functionality.

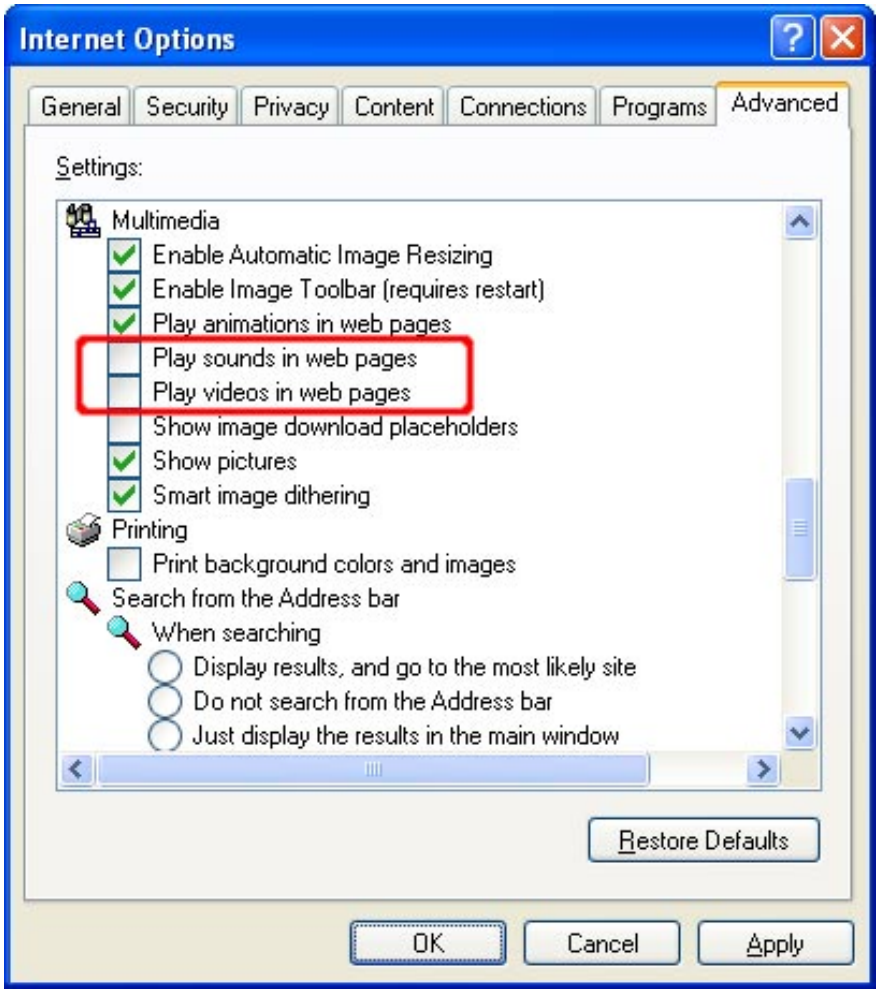
The ***Privacy*** tab includes settings for cookies. Cookies are text files placed on your computer for different pages that you visit them directly or indirectly through, for example, banner ads. A Cookie may contain any data that a site saves it for its own purposes. It is often used to check your computer when you move through a website and save information like hobby. We recommend that you select the ***Advanced*** button and select ***Override automatic cookie handling*** . Then select ***Prompt*** for both first and third group cookies. This will remind you every time a website tries to place a cookie on your computer. You can then evaluate the original page, want to accept or restrict cookies and what actions to take in the future (always accept, always lock or continue to ask).



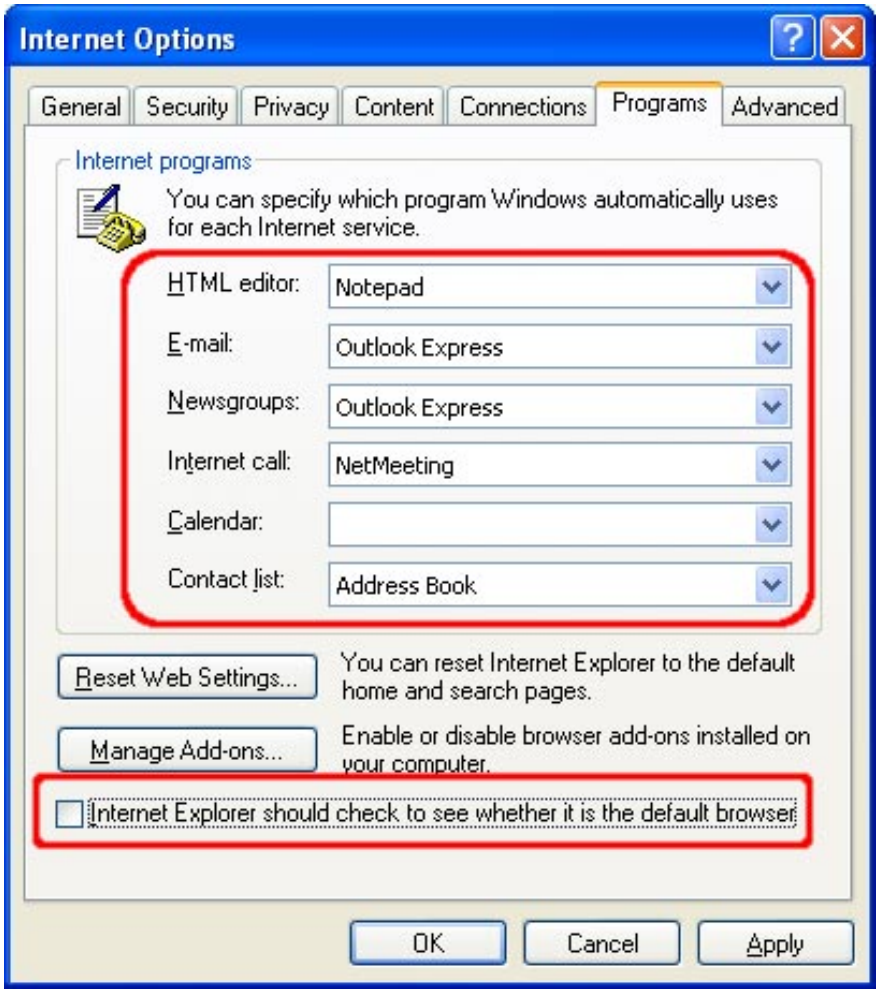
By selecting the ***Sites*** button **.** , you can manage cookie settings for specific pages. You can add or remove pages, you can change the current settings for existing pages. The bottom of this window will indicate the area of ??the page and the action needed when the page wants to place a cookie on your computer. You can use the upper part of the window to change the settings.



The ***Advanced*** tab contains settings used for all regions. The settings included in the ***Multimedia*** section have features that you can adjust to protect against other potential vulnerabilities. For example, attackers can check your computer usage habits or exploit the software you use to play multimedia data. We recommend disabling the option to listen to music and watch videos.



Under the ***Programs*** tab, you can specify applications that are viewed in websites, e-mail, and other network-related tasks. You can also protect Internet Explorer from showing you a message asking about your default web browser.



If you do not use Internet Explorer, you can continue to watch the following sections. See the following article: **Secure Mozilla Firefox** .

You finished reading the article "**Security for Microsoft Internet Explorer**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
