Improve Your Browser's Security Settings for Greater Protection while Browsing the Internet

Using the information given in this article you will be able to:

- ✓ Configure Edge, IE, Firefox and Chrome for perfect security,
- ✓ Remove the insecure add-ons that leave your browser vulnerable to attack,
- ✓ Boost your browser protection with registry tweaks.

Your web browser is the application you probably use most on your PC, but it is also the one that is most at risk. That is why it is so important to take steps to configure your browser's security settings to protect your PC from coming to harm. The vast majority of malware infections arrive via hijacked or fake websites, since Windows Firewall has blocked most of the other routes hackers used to take to infect PCs. This means that it has never been more important to secure your web browser against attacks. All the latest web browsers come with a raft of security features to help you do that but it is important to take the time to configure the features correctly. This will result in the highest level of protection possible from your browser. Follow the steps in this article for a perfectly configured web browser and enhanced online security.

Configure Edge for Best Security

Configure Edge for best security

If you want to stay safe while you are browsing the Web using Edge, you can activate and configure the security options as follows:

1. Click on the **three dot** icon in the top right-hand corner of the Edge window, then click on **Settings > View Advanced Settings**.
2. In order to stop annoying pop-up windows from being shown while you are surfing, you should activate the option **Block pop-ups**.
3. Adobe Flash Player is widely used on websites, and allows you to view videos online. Unfortunately, security problems in Flash Player make it a favourite target of malware writers. If you do not use Adobe Flash Player, you should switch off this feature.

   Turn off Flash Player

   To turn off Flash Player, simply move the relevant button to the **Off** position on the left. If you visit a website that does need Flash Player, you can quickly activate it by clicking on the **Flash Player** icon.
4. Practically every website you visit will record at least some of your browsing behaviour. Usually this is done to target advertising at you as you surf. Often this data is shared with other companies (usually online advertising brokers), who can use information from each site you visit to build up a picture of your browsing behaviour.

   Stop sites from tracking you

   If you don't want to see personalised adverts based on your browsing history, you should activate the option **Send Do Not Track** requests.
5. While you are surfing the Web, you will often see a notice displayed on a page telling you that cookies

are being used by the website. Cookies are small text files that are stored on your hard drive which contain information about your usage of a particular website.

In general, Edge allows all cookies to be stored on your PC, but you can customise the settings to block all cookies, or only those from third-party sites (which are often used for tracking purposes).

Set Up Internet Explorer for Optimised Security

Internet Explorer is targeted by hackers most often

Internet Explorer is the browser that is most often targeted by hackers, so it is no surprise that Microsoft have added some of the strongest security features to their browser in recent years.

The Smart Screen Filter in Internet Explorer works by scanning the websites you visit for malicious software and also checking them on a list of sites known to be infected with spyware and viruses. It also checks the files you download from the Web against known malicious software, to prevent viruses sneaking in this way.

SmartScreen Filter

By default, the SmartScreen Filter should be turned on. To manually check a website, follow these steps:

1. Click the **cog** icon in the top right-hand corner of the Internet Explorer window.
2. Point to the **Safety** option, and then click on **Check this website**.
3. The Microsoft SmartScreen Filter will check the website and tell you whether it is safe.

Look out for this text when a dangerous website is detected

Beware when you see this message: the website is dangerous

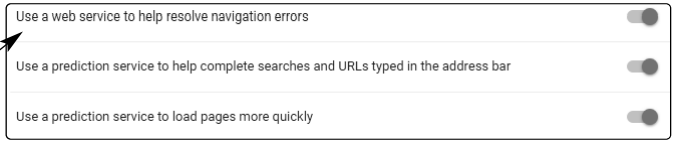
Boost the Security of Google's Chrome Browser

Make Chrome more secure

Google Chrome comes with both malware and phishing protection features built in, as well as a feature that corrects mistyped web addresses to avoid taking you to malicious websites (which often use misspelled URLs). To use these features, proceed as follows:

1. Click on the **three dot** icon in the top right-hand corner of the browser window and click **Settings**.
2. Scroll down to the **Privacy and security** section (if this isn't shown click on **Advanced**).
3. Activate the options **Use a web service to help resolve navigation errors**, **use a web service to help resolve spelling errors**, and also **Protect you and your device from dangerous sites**.

Enable the Chrome security options



Configure the security options in Google Chrome

4. To stop your websites from tracking your browsing, activate the option **Send a "Do Not Track" request with your browsing traffic.**
5. Activate the option **Automatically send some system information and page content to Google to help detect dangerous apps and sites.**
6. Click on the **Content settings** button.
7. Click on **Popups** then turn the **Blocked (recommended)** setting to **On.**

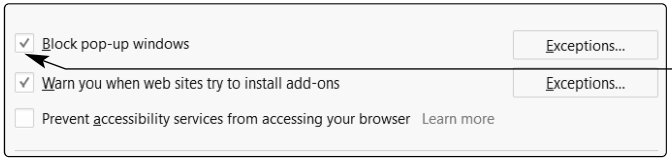
Block pop-ups in Chrome

Protect Firefox with Optimal Security Settings

Optimise your Firefox security settings

Firefox includes basic security and privacy features that protect you while surfing online, to block known dangerous websites and report web forgeries. To make sure you are safe online, it is important to check that all of these features are turned on. To do so:

1. Click the **three line** icon in the top right-hand corner of the browser and choose **Options.**
2. Click on **Privacy & Security.**
3. Tick **Block pop-up windows** and **Warn you when sites try to install add-ons.**



Enable all the Firefox security features

Set a master password

4. If you have Firefox configured to remember your passwords (with **Remember logins and passwords for web sites** ticked), you should set a master password. To do so, tick **Use a master password** then enter and repeat the password and click on **OK**.
5. Scroll down to the Tracking Protection section and select the option **Always** to prevent sites from tracking your activities.
6. Click on the **Security section** and tick the option **Block dangerous and deceptive content**.

Surf the Web Without Leaving a Trace

Erase traces of your browsing activity

All browsers have private browsing features that allow you to surf the Internet without leaving a trace on your hard drive. This prevents other users from seeing what sites you visited and when.

Enable private browsing

To activate this feature in Edge, click the **three dots** in the top right-hand corner and click **InPrivate Browsing**. In Internet Explorer, click the **tool (cog)** icon, then click **Safety > InPrivate Browsing**. In Firefox, click on the **three line** icon in the top right-hand corner of the browser window and choose New **Private Window**. In Chrome, click the **three dot** icon in the top right-hand corner of the browser and choose **New incognito window**.

Once you start private browsing, your browser will open a new browser window. The protection that private browsing provides is enabled while you are using this window and won't be enabled in any other browser windows that you have open.

You can use this window to open as many tabs as you want, all of which will be protected by private browsing.

Protect Your Browser in the Registry

Apply Internet Explorer protection measures in the registry

Allowing Internet Explorer to save your usernames and passwords makes it quick and easy to sign in to secure sites but it also means that anyone else who uses your computer – or potentially a hacker who gains access to your machine – can obtain your login credentials. With a quick tweak of the registry you can turn off the password caching feature, removing the possibility that you accidentally store a sensitive password and increasing your PCs security in turn.

To apply this tip, follow the steps below:

1. Press (Windows) + (R), type **REGEDIT** and click **OK**.
2. Navigate to the registry key: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**.
3. Check in the right-hand panel for the **Disable PasswordCaching** setting. If it doesn't exist, create it by right-clicking on a blank area of the right-hand panel and choosing **New > DWORD (32-bit) Value**.
4. Double-click on **DisablePasswordCaching**.
5. Change the Value data field to **1** and click **OK**.
6. Close the Registry Editor and restart Windows for the changes to take effect.

Block downloads from certain websites

Sites can try to fool you into installing software on your PC, usually through some JavaScript code that tries to force the download on to your machine. With a quick tweak of the registry

you can configure Internet Explorer to block downloads from certain websites, while still being able to visit those sites.

Here's how you can secure Internet Explorer against unwanted downloads:

1. Press (⊞) + (R), type **REGEDIT** and click **OK**.
2. Navigate to the registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains**. If the Domains key doesn't exist, you can create it by right-clicking on **ZoneMap** and choosing **New** > **Key**.
3. Right-click on **Domains** and choose **New** > **Key**.
4. Name the new key after the domain name of the site you want to block. For example, to block downloads from www.domain.com you would create a key named **domain.com**.
5. Click on the registry subkey that you just created, then right-click in a blank area of the right-hand panel and choose **New** > **DWORD Value**.
6. Name the new DWORD Value *****.
7. Double-click on ***** and change the **Value data field** to **4**, then click **OK**.
8. Close the Registry Editor and restart your PC for the changes to take effect.

Remove Add-ons that Lead to Browser Problems

Remove add-ons

Many programs embed themselves in your web browser in order to extend its functionality, and you can also add standalone extensions from the Web. But, your browser has

all of the basic features that you need, and your browser will be more secure if you turn off these third-party extensions. To do so, follow these steps:

Edge

1. Click on the **three dots** in the top right-hand corner then click **Extensions**.
2. Right-click on the add-on you want to remove and select **Remove**.

Internet Explorer

1. Open the Internet Explorer and click on **Tools** > **Manage add-ons**. If the **Tools** menu isn't shown, press the Alt key.
2. Using the **Show** drop-down list, select **All add-ons**. This will ensure that all of the add-ons installed on your computer are displayed, not just the ones that are currently active.
3. In the list of available add-ons, select any add-ons that you don't need which have the status **Enabled** and then click on **Disable**.
4. Once you have deactivated all the add-ons that you don't need in the list, click on **Close**.
5. Close Internet Explorer and restart it.

Firefox

1. Click on the **three line** icon in the top right-hand corner then click on **Add-ons**.
2. In the Add-on manager, work through the add-ons listed in the **Extensions** tab.

3. Select the add-on that you want to deactivate and click on the **Disable** button.

Restart Firefox

4. Close and restart Firefox for the changes to take effect.

Google Chrome

1. Click on the **three dot** icon in the top right-hand corner of the Chrome window, next to the address bar.
2. Click **Settings** and then **Extensions** when the **Settings** window opens.
3. Locate the add-on that you want to remove, then click on the **Remove** button.
4. Confirm the uninstallation by clicking on **Remove**.

IE Only: Boost Your Protection with Security Zones

Internet Explorer features in-built security mechanisms to protect your system from harmful content online.

Configure security zones for added IE protection

There are four default security zones and you can assign different sites to each of these zones, depending on the security risk they pose. To access the security zone settings, click on the **Tools** menu, then **Internet Options** (if you can't see the **Tools** menu, press Alt). In the window that opens, click on the **Security** tab.

Each security zone can be set to a different security level, which will determine what actions are possible in that zone. You can use the security level slider to set a predefined security level to a particular zone, without having to specify all of the security settings for the zone individually. In the **Internet** zone you can choose between **High**, **Medium-high** and **Medium** security settings. The Trusted Sites zone also allows you to choose from the additional levels **Medium-low** and **Low**.

The higher you set the security level, the more security restrictions are put in place. Selecting a level with the slider will show you what restrictions a setting puts in place.

Higher zones improve security

Setting a zone to a higher level will improve your security but you may find that some websites do not function properly and that certain types of content are not displayed.

A good balance between security and functionality when surfing the Internet will be had by setting the **Internet zone** to a security level of **Medium-high**. You can keep the **Trusted Sites** zone at a lower security setting, such as **Low** or **Medium-Low**.

Add secure sites to the Trusted Sites zone

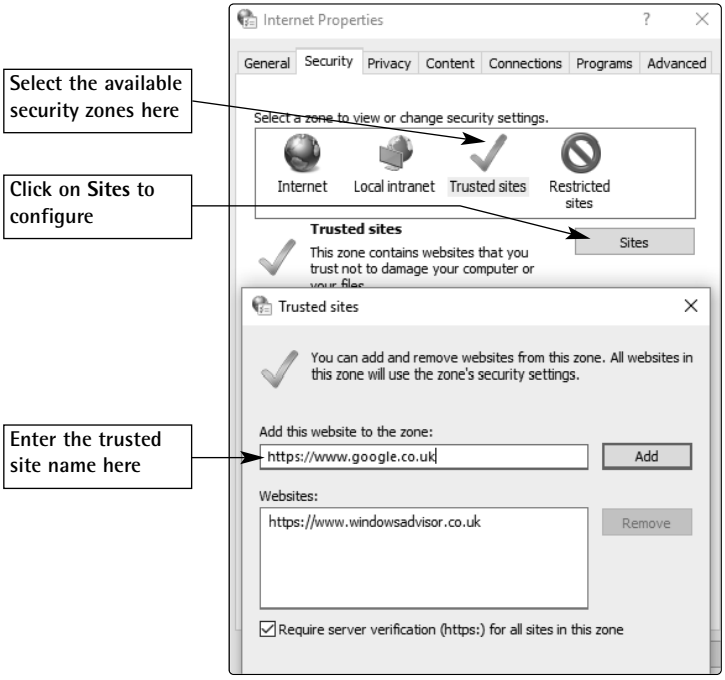
If you have sites that do not function normally, and which you trust, you can add them to this zone to enable the extra functionality needed. For example, if your online banking site uses ActiveX controls, add it to this zone. All of the security zones and their functionality are described in the table below:

Zone	Recommended Level	Description
Internet	Medium-high	All web pages that you visit that are not assigned to a particular zone will automatically be assigned to this zone.
Local Intranet	Medium	Any site that you visit on your local network will be assigned to this zone.
Trusted Sites	Low or Medium	You can add sites to this zone that you know to be safe to visit and which require lower security settings in order to display particular types of content.
Restricted Sites	High	Enter sites into this zone which you want to visit but which have dubious security (mobile phone ringtone download sites which display lots of pop-ups, for example).

S 491/12 Secure Browsing with the Correct Configuration

Add the https:// prefix to ensure the site is secure

To add a website to the Trusted Sites zone, click **Trusted Sites**, then click **Sites**. Enter the web address of the site you wish to add, with an **https://** prefix to guarantee that the site is secure, then click **Add**. To add sites that don't use the https protocol, untick the option at the bottom.



Add a website to the Trusted Sites zone

Summary

Your web browser is your window to the Internet and, just like the windows in your home, you have to secure it against burglars and other criminals. Applying the best possible security configuration to your browser will greatly enhance your protection while online and make it much more difficult for online crooks to attack your system.