7 ways to protect your web browser from network attacks

Use these tips to protect your web browser from attackers, whether they use adware or malicious websites.

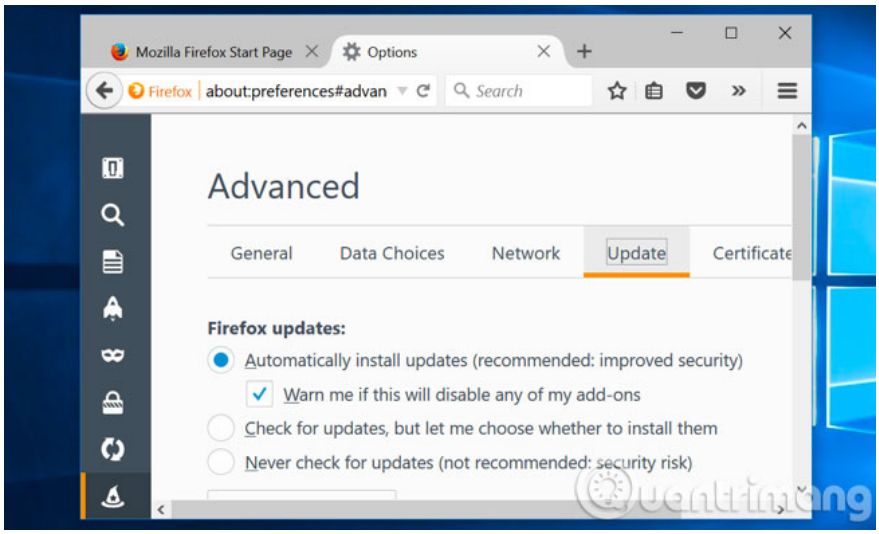
Your web browser is being placed under network attacks. In addition to being as simple as tricking you into downloading and running malicious software, attackers primarily target browser holes and its plugins to infiltrate the computer. Through malicious code installed on the computer, an attacker not only launches network attacks, but can steal personal information, destroy data and perform other dangerous actions.

1. 9 misconceptions about security and how to resolve
2. Instructions for removing DNS Unlocker adware
3. Security tips for Google, Facebook and online services

Use the tips below to protect your web browser from attackers, whether they use adware or malicious websites.

Always update your browser

Use the latest browser now and enable auto update mode for it. Stop using old browsers like Safari for Windows or old Internet Explorer versions. Instead, use **Google Chrome** , **Firefox** and let them automatically update, but if you're installing **Windows 10** , then "use" **Microsoft Edge** .



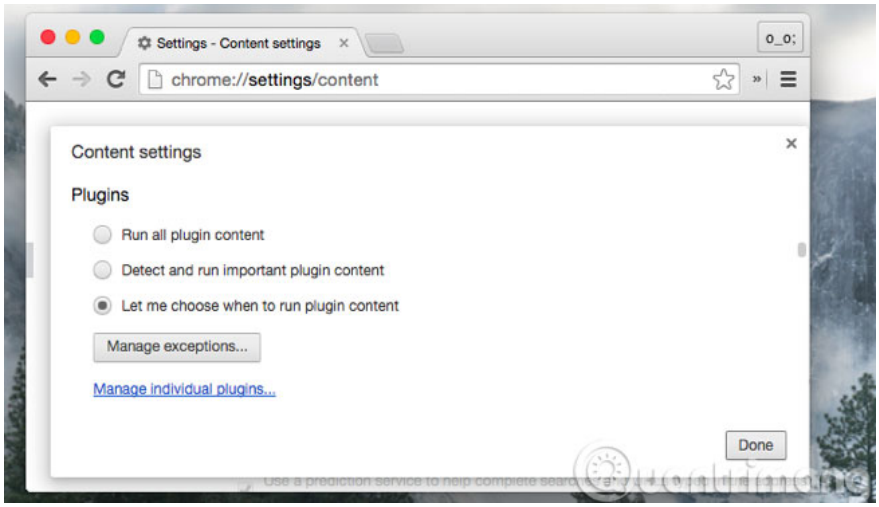
Configure security and security settings for the browser

Review your browser's security and security settings to make sure you're protected. For example, see if the browser blocks third-party cookies. These cookies may allow advertisers to track your online activities.

Reference: How to block ads when surfing the web

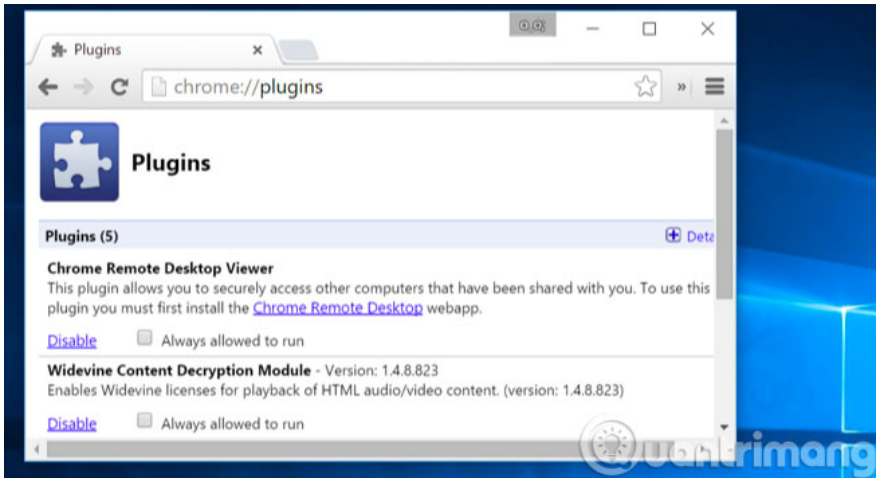
Activate Click to Play for plugins (Plug-in)

Activate the **Click to play option** on your browser, which will make the site load faster and save CPU cycles and battery power. It also has an important protective effect. Attackers will not be able to exploit the plug-in vulnerabilities in the browser because you only allow them to download when needed.



Remove unnecessary plugins

Remove plugins that you feel are unnecessary, like Java, Silverlight, Flash. The worst case scenario is that you may have to reinstall it when accessing a certain website, but this is very unlikely.



Keep the plugins up to date

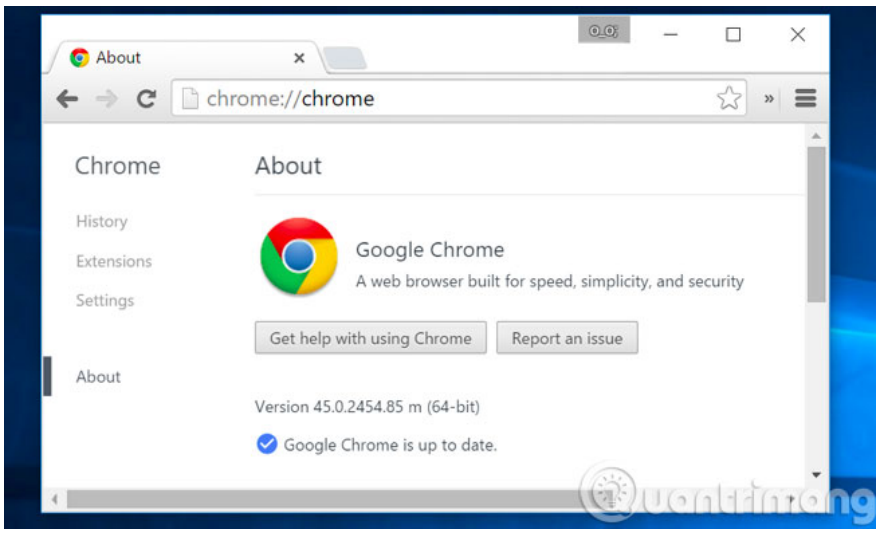
Any add-on that you need should be automatically updated like **Adobe Flash** . Google Chrome and Windows 10 can automatically update its own Flash, but for other Flash versions, you must update it automatically.

Use a 64 bit web browser

64-bit programs are often better protected against network attacks. Assuming you are installing a 64-bit version of Windows, you should use a 64-bit browser. The random address space layout will be more efficient with 64-bit programs.

Google Chrome has both 32-bit and 64-bit versions, check which version you are using. If you are using a 32-bit version, you should download the 64-bit version for use.

The stable 64-bit version of Firefox is not yet available, although you can use the developer version. Mozilar plans to develop a 64-bit version of Firefox through a stable channel in Firefox 41.



Run an anti-exploit program for security vulnerabilities

The anti-exploit vulnerability programs make your web browser more rigid against attacks, instead of relying on a list of antivirus types for a specific software and behavior, these programs will prevent abnormal behavior from happening.

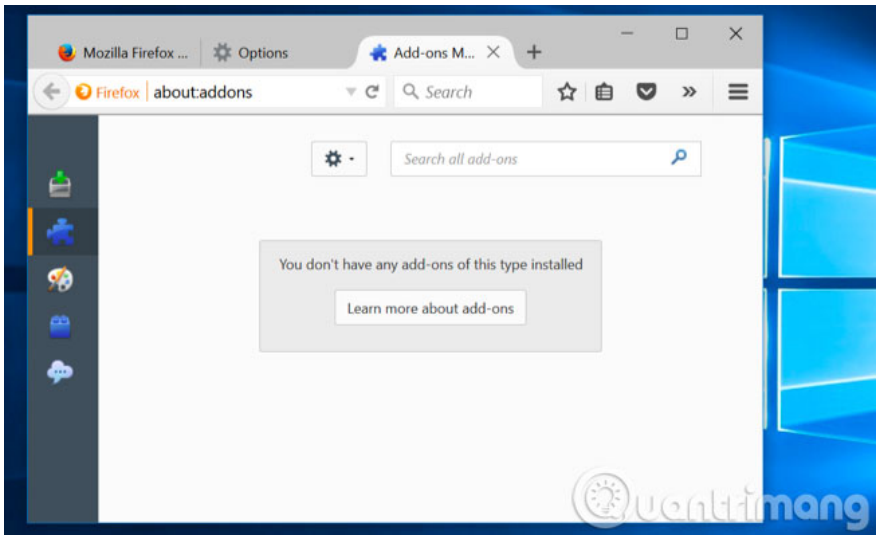
There are 2 options for you: Microsoft's Emet and **Malwarebytes Anti-Exploit** . Both are free but the Anti Exploit is easier to use.

You can still use antivirus software but can't rely entirely on them.

Use caution when using extensions

Browser-based utilities are often used to customize the browser and website, but at the same time, it also has a certain effect. Fake utilities can insert ads on websites you visit or track activities on your browser.

Try to use as few extensions as possible, it will make the browser work better.

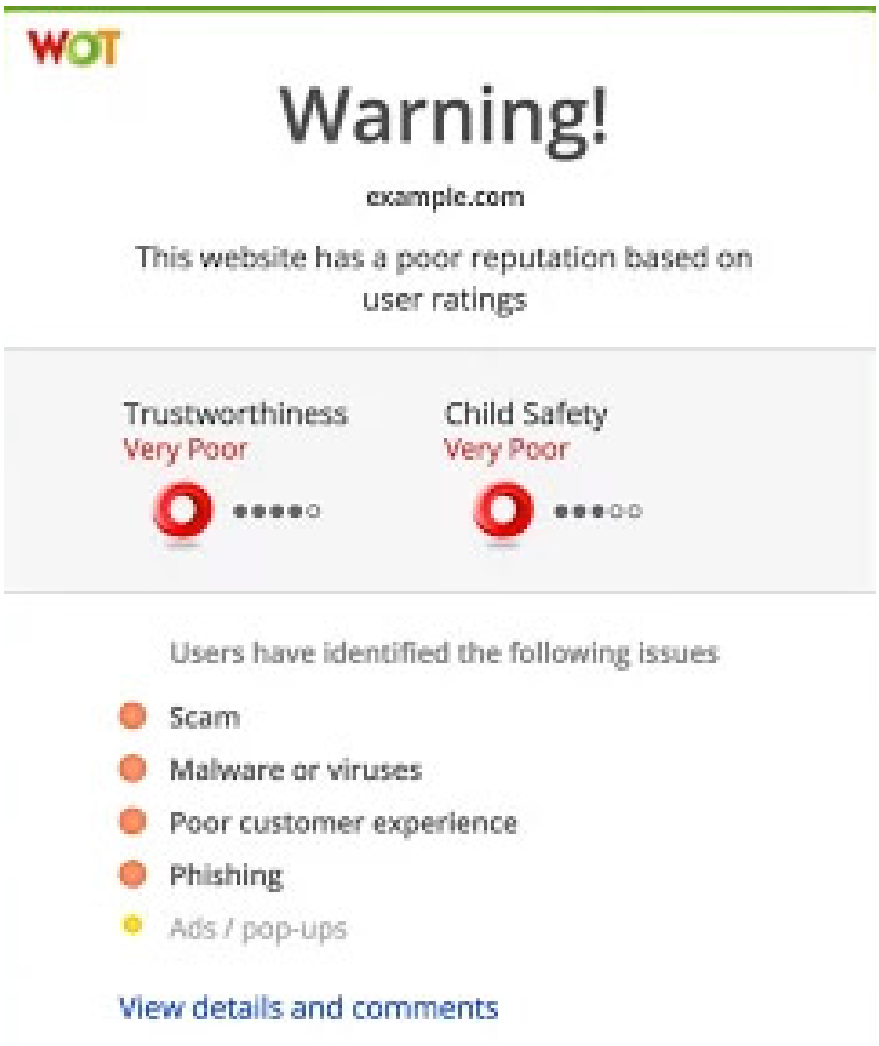


Protecting browser software is only one part, and it is important to avoid phishing and "dirty" software sites. Many websites try to trick you into downloading junk programs instead of the software you are looking for, even legitimate programs often come with potentially dangerous "junk".

Install security plug-in

Not all plugins and plug-ins are bad, there are many plugins that even enhance the browser security. Here are three free extensions and should be used to make your browser safer:

1. **HTTPS Everywhere:** This add-on was created by The Electronic Frontier Foundation and The Tor Project, it works in Firefox, Chrome and Opera. HTTPS is a communication protocol that ensures security on computer networks. This protocol is much safer than traditional HTTP protocols, which have been widely used. The letter S in HTTPS stands for secure. If the website you are visiting does not use HTTPS, HTTPS Everywhere will be a good solution, it encrypts communication between you and the web so that they are not read by the curious.
    1. **Download HTTPS Everywhere for Chrome:** https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp
    2. **Download HTTPS Everywhere for Firefox:** https://addons.mozilla.org/en/firefox/addon/https-everywhere/
2. **Web of Trust or WOT:** This extension is available for large browsers, helping you determine if a website is safe to browse. WOT displays the signal symbol by color next to the URL and the link, green means that the page is safe and reliable. Yellow reminds you to be cautious about the site and red means insecure, should not be accessed. Evaluating this site is quite reliable because it is implemented by WOT's own user community around the world and is supported by trusted third parties, such as a library of websites that contain codes The poison is always refreshed.



Good luck!

You finished reading the article "**7 ways to protect your web browser from network attacks**" 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.