

Risk of virus infection from browser and prevention

Plugins are preferable targets. Plugin vulnerabilities can be exploited on all browsers and on many different operating systems. A Flash plugin vulnerability could be exploited to exploit Chrome, Firefox or Internet Explorer on computers running Windows, Linux or Mac operating systems.

You can 'pick up' the virus to your computer through your browser for unsafe plugins, use an outdated browser version, download downloaded files automatically . So how to prevent it?

Unsafe browser plugin

Most cases of virus infection through the browser are because the plugin is not secure. Oracle's Java plugin is the most dangerous culprit. Recently, Apple and Facebook's internal computers were hacked because they accessed websites with malicious Java applications. It is possible that their Java plugin is completely updated, but even the latest Java version still contains unpatched security holes.

To protect yourself, you should remove Java completely. If you must use the Java application on the desktop, at least you should turn off your browser's Java plugin.

Other browser plugins, especially Flash player and PDF reader, also often have to fix security holes. Compared to Oracle, Adobe often responds to and fixes the plugin vulnerability better, but occasionally a new Flash vulnerability is being exploited by hackers.

Plugins are preferable targets. Plugin vulnerabilities can be exploited on all browsers and on many different operating systems. A Flash plugin vulnerability could be exploited to exploit Chrome, Firefox or Internet Explorer on computers running Windows, Linux or Mac operating systems.

To protect yourself against plugin security holes, perform the following steps:

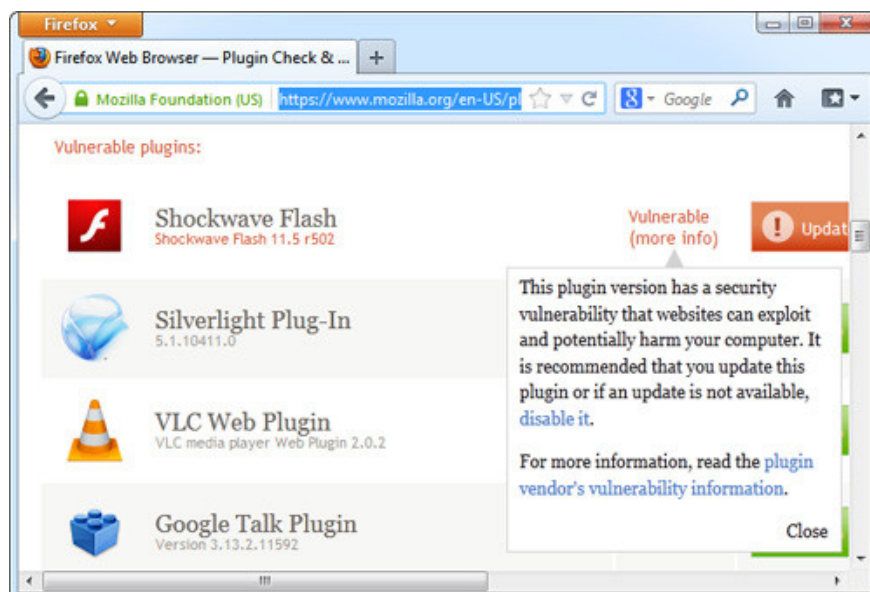
Step 1: Use Firefox's plugin check website to check if any browser plugins have not been updated (This website was created by Mozilla, but it works with both Chrome and some other browsers).

Step 2: Instantly update old plugins and turn on auto update mode for each plugin you have installed.

Step 3: Remove the plugins you don't use.

Step 4: Consider using the '*click-to-play*' plugin feature in Chrome or Firefox. This feature prevents the plugin from automatically running unless you require a specific plugin to be enabled.

Step 5: Make sure your computer has antivirus software installed. This is the final defense to prevent attackers from installing malicious software on a computer through a '*zero-day*' vulnerability in the browser plugin.



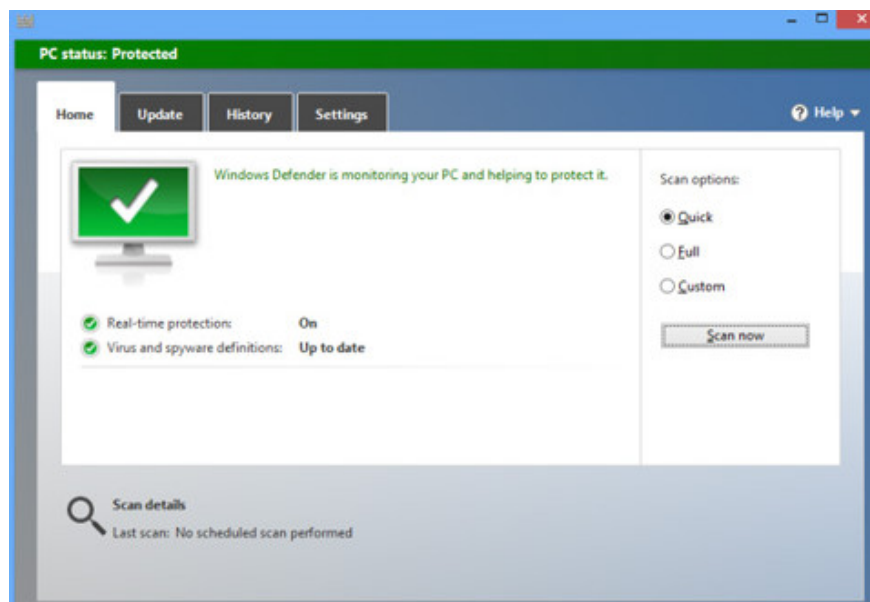
Avoid using an outdated browser version

If you use Internet Explorer 6 (this version is old and has not been patched yet) to access an unreliable website, the website may exploit vulnerabilities in the browser to install malicious software on your computer. .

To protect yourself against browser vulnerabilities, it's simple:

First , keep the web browser up to date. Currently, all major browsers automatically check for updates. Turn on **auto-update** (Internet Explorer browser updates via Windows Update.)

Second, make sure the computer has antivirus software installed. As with plugins, this is the last line of defense to prevent malware from entering your computer through a zero-day vulnerability in your browser.



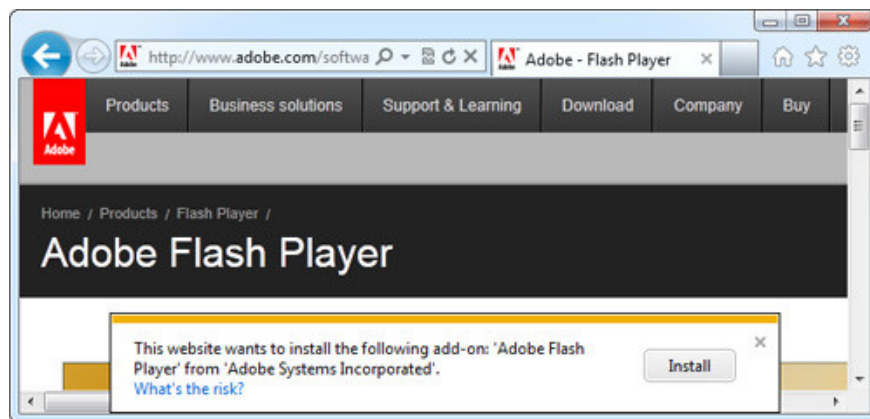
'Social engineering' attack

Malicious websites can use '*social engineering*' attacks to trick you into downloading and launching software that contains viruses. '*Social engineering*' attacks can occur in the following cases:

1. Trick users to download ActiveX Control

Internet Explorer uses ActiveX Control for browser plugins. Any website can prompt you to download an ActiveX Control and sometimes this is not harmful.

For example, you may need to download the ActiveX control Flash player the first time you open a Flash video in your browser. However, ActiveX controls, like other software, are allowed to bypass the browser and access the rest of the computer system. Therefore, ActiveX Control from the website contains malicious code that will endanger your computer. If in doubt, do not accept to run any ActiveX Control.

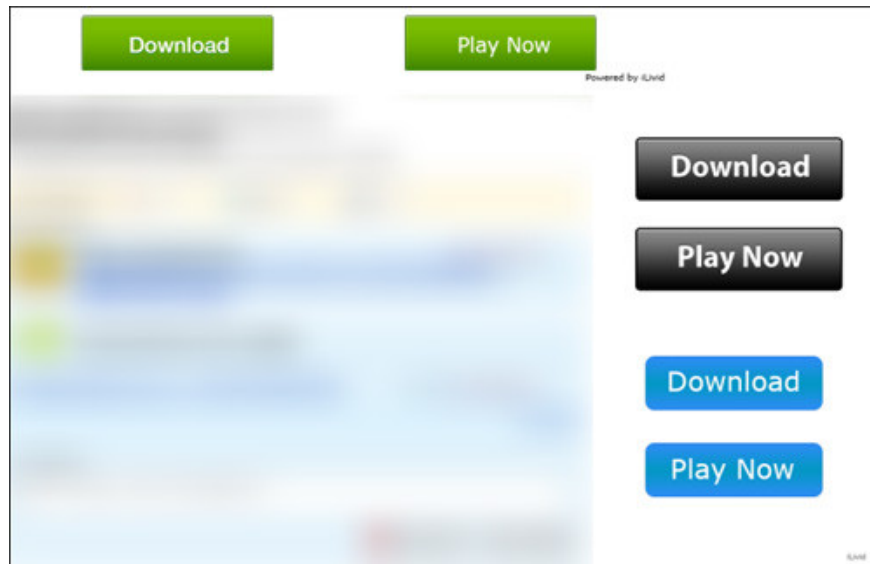


2. Automatically download files

A malicious website can find a way to automatically download an EXE file or other malicious files onto your computer. If users open this file, their computer will be infected with the virus. Unless you intend to download a specific software, do not accept files that automatically appear and ask you to save them.

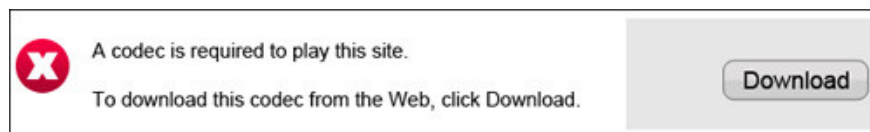
3. Fake download links

On websites containing pirated content, you often see many advertisements that mimic the download button. Those ads try to trick users into downloading unwanted content. There is a very high risk that these form links contain malicious code.



4. 'You Need a Plugin to Watch This Video'

If a website displays the *'You Need a Plugin to Watch This Video'* message (roughly translated: You need to install a new browser plugin to view this video), be careful. Sometimes, this may be necessary, for example you need Microsoft's Silverlight plugin to watch videos on Netflix. But if a website has no reputation that requires you to open an EXE file to view the video, chances are they're trying to spread the virus to your computer.



5. 'Your Computer is Infected'

You can see the message saying that the computer is infected with the virus and advise you to download an EXE file to clean the virus. If you download that EXE file and launch it, your computer will be attacked.

You finished reading the article "**Risk of virus infection from browser and prevention**" 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.