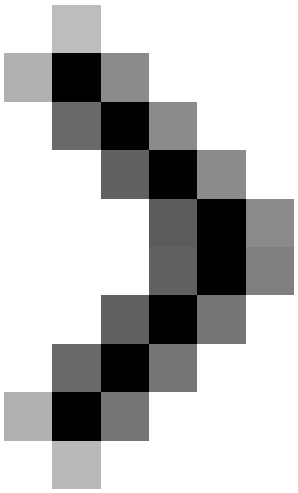
Protect yourself against IE security holes

To help you avoid attacks that exploit the newly discovered IE vulnerability, we recommend some tips to help you protect your data safely.

Network Administration - Like many other IE users, you've probably heard the phrase 'Security vulnerability in IE'! However, this is a completely new security hole, with this security vulnerability, a malicious website can take advantage of it to access data files on your computer. To help you avoid attacks that exploit this vulnerability, we recommend some tips to help you protect your data safely.



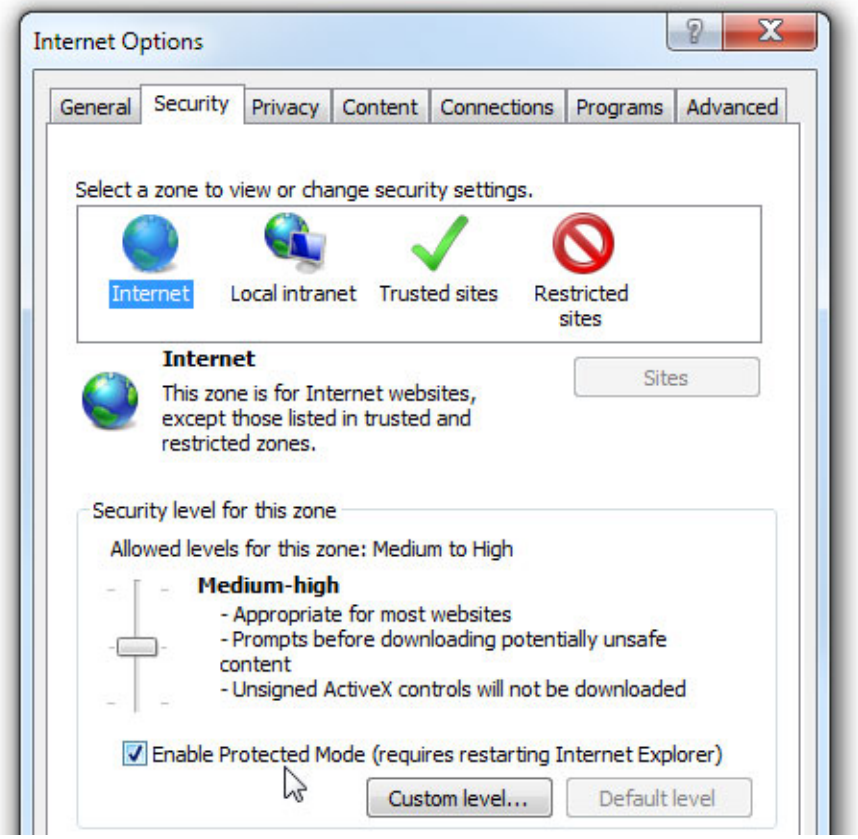
IE vulnerability threatens Windows XP users

Note that these tips are only useful for IE security vulnerabilities.

Make sure your Protected Mode protection is enabled

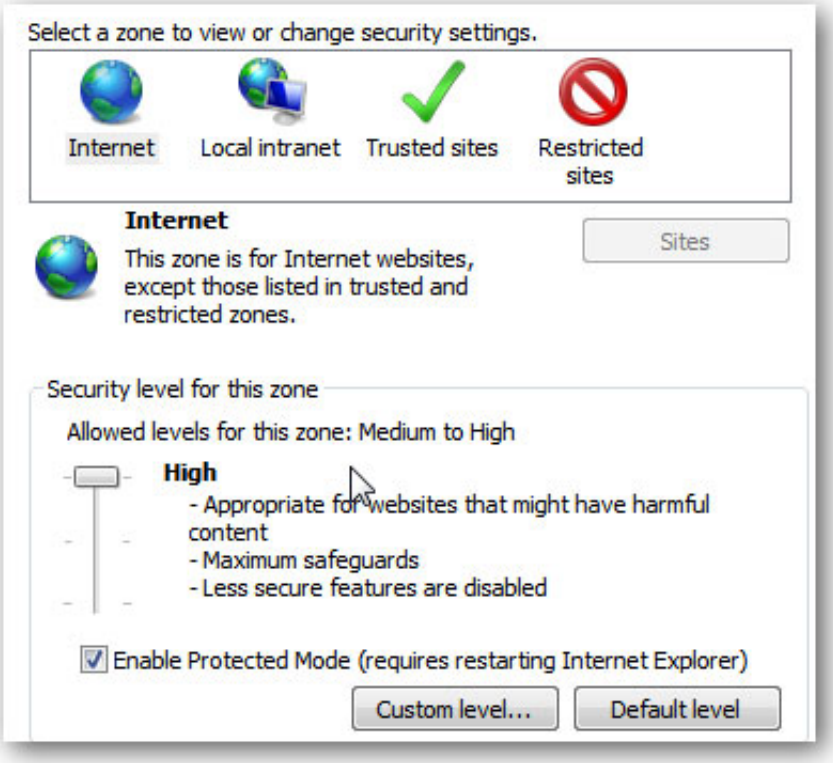
As with most IE security vulnerabilities, if you are running Windows 7 or Vista, you need to enable Protected Mode, which will run Internet Explorer in a sandbox - to protect you from pages. Web malicious code (though not all).

Go to **Internet Options** -> **Security** tab and check the checkbox to activate this mode.



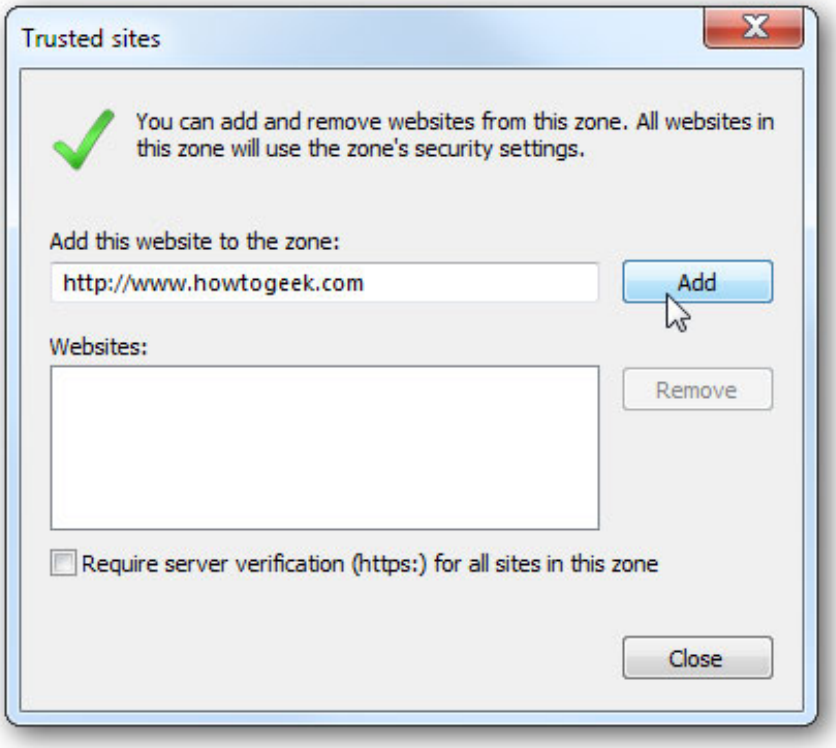
Set up ActiveX Controls in prompt mode (or disable them)

If you drag the slider in the image above to High, you will disable ActiveX Controls, not allowing it to automatically run.



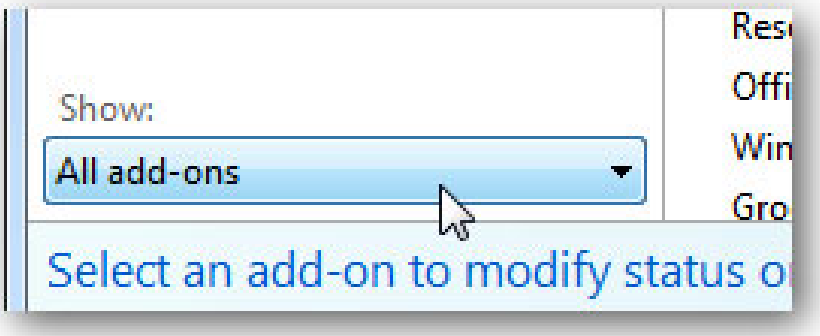
The undesirable side effect is that you will be prompted more when accessing sites that use ActiveX Controls. Microsoft encourages you to add sites that you really trust to your Trusted Sites list . and make sure to clear the 'Require https' checkbox at the bottom.

To add a site to the Trusted Sites, click the **Trusted Sites** icon shown in the image above, then click the **Sites** button, type the website **URL** , and then click the **Add** button.

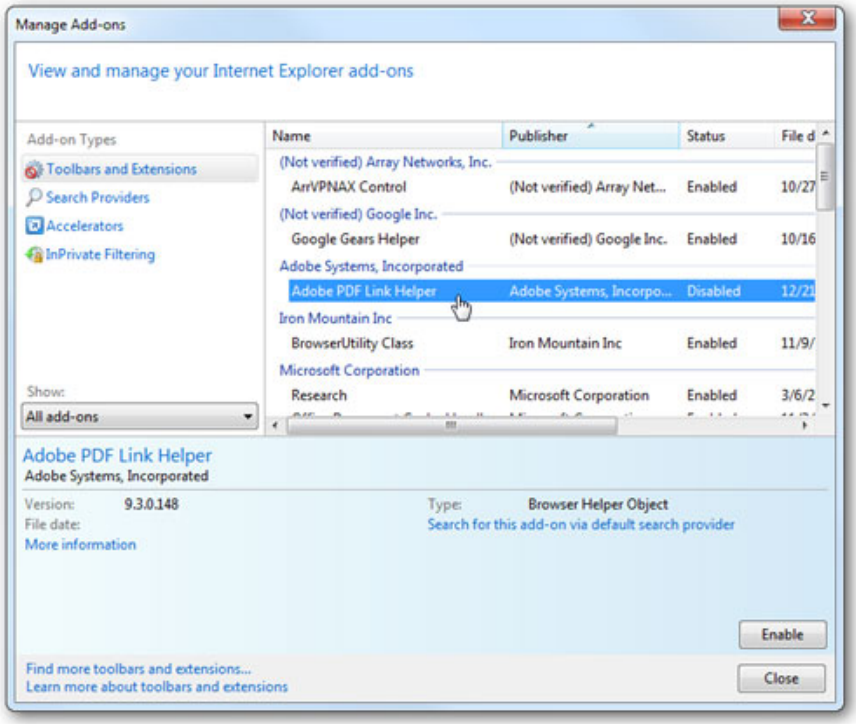


Disable unnecessary plugins

Open **Tools** -> **Manage Add-ons** from the IE menu, then change in the drop-down menu under ' **Show** ' to ' **All add-ons** '. You will then see a list of all the add-ons that are currently enabled, so we can begin to disable unnecessary add-ons.



Here, you will have a fairly large list of add-ons and can start disabling them by clicking on them, then clicking **Disable** . Important note here: Adobe Reader seems to have another security vulnerability and if you don't really need Java support, you can disable it.

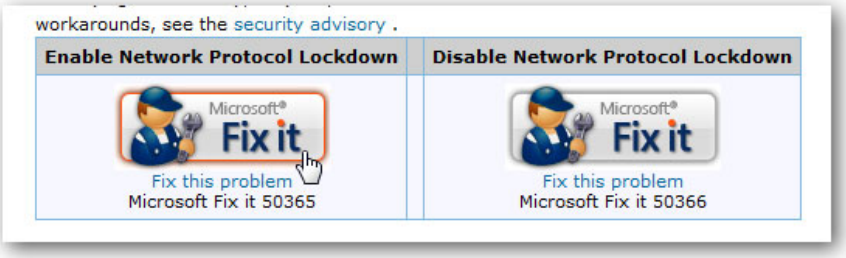


My general principle is to disable what is not needed, or can disable all then re-enable add-ons that you feel really need. Disabling add-ons is the fastest way to make IE run faster.

Use Microsoft FixIt to fix the problem

One of the best things is that Microsoft has recently provided the 'Fix it' feature on their support site - with some problems, you can launch the Microsoft utility and let it solve the problem yourself. yours.

However, in this case, you can use Internet Fix to activate Network Protocol Lockdown. You can click on the image below to access the Microsoft site:



You finished reading the article "**Protect yourself against IE security holes**" 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.