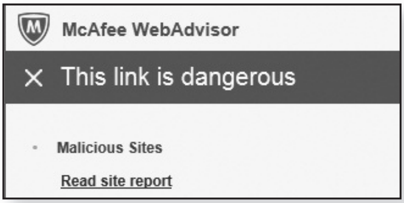
Identifying Safe Websites

Check Whether a Website is Potentially Dangerous Before You Open It

This article shows you how to:

- Install an early-warning system for risky websites
- Get rid of possibly-dangerous ads on web pages
- Recognise and avoid suspect web addresses

There are billions upon billions of web pages out there. The vast majority are safe and trustworthy, but a small percentage are dangerous, aiming to infect your PC with malicious software ('malware'). Needless to say, even a small percentage of those billions adds up to a huge number, and you might easily stumble upon one of them.



McAfee WebAdvisor

This link is dangerous

Malicious Sites

Read site report

The solution is to remove whatever dangers you can and to be forewarned of any others before you visit a website. The 4 safeguards in this article will help you do exactly that.

Contents:

What Could Be 'Dangerous' about a Website?

Any website is potentially harmful

You might be tempted to think of a website in much the same way as a newspaper: you open it, read it for a while and then close it, and it couldn't possibly do any harm. Sadly, that couldn't be further from the truth.

While the vast majority of websites are safe to visit, there's a sizeable number which certainly are not:

Immediate malware infections

- Some websites are 'actively dangerous': they try to infect your PC with malicious software the moment you arrive, or they try to fool you into installing extra software on the pretence that the website won't work properly without it.

Tempting, but dangerous, software

- Some are 'passively dangerous': they look respectable on the surface, but they offer software (or other items) to download which are dangerous.

Cloned 'phishing' sites

- Some are 'phishing' sites: they're designed to look just like a well-known bank, online store or travel agent, but they were created by scammers with the intention that you'll be fooled into entering your private sign-in details.

> Along similar lines, often around Christmas time, fake online stores appear which are designed to look exactly like (for example) the real Debenhams or John Lewis stores, with the intention that you'll be tricked into buying goods there. You won't receive those goods, of course, and since you entered your payment details to buy them, it could be an expensive shopping spree!

Infected advertisements

- Even well-known, trusted websites can be a threat. Many websites display advertising from third parties, and they don't always check those ads as carefully as they should. Even on a respectable website, a maliciously-crafted ad could attempt to install malware on your computer.

Unfortunately, there's no magical solution that can guarantee to keep your PC safe from harmful websites: in the online world, common sense and some natural scepticism go an awfully long way! However, the four safeguards I'll present on the following pages will help to keep you safe on the inevitable occasions when even common sense can't help you.

Safeguard 1: Install an Early Warning System for Dangerous Websites

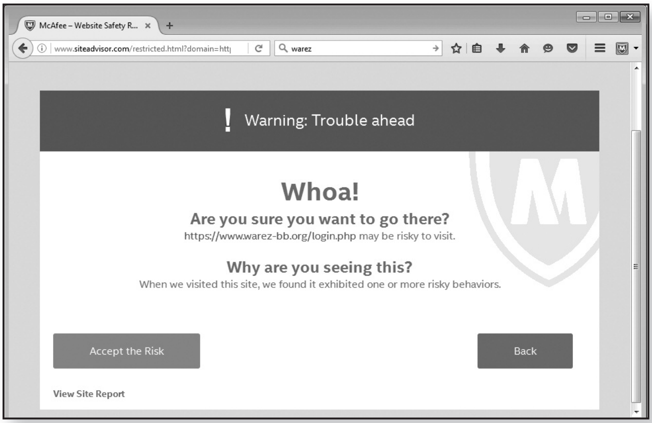
A useful add-on for your web browser

My first recommendation is to install a free program named McAfee WebAdvisor. This isn't a traditional program of the sort you'd find on your Start menu: instead, it's an 'add-on' (or 'extension') for your web browser. It works with Windows 10, 8.1 and 7, and the three popular web browsers Internet Explorer, Mozilla Firefox and Google Chrome.

McAfee WebAdvisor works in two very useful ways:

Avoid risky websites

- First, if you arrive at a website that's known (or suspected) to be dangerous, it whips you away from it immediately, before it can do any harm:


McAfee – Website Safety R...
www.siteadvisor.com/restricted.html?domain=htt
warez
Accept the Risk
Back
View Site Report

! Warning: Trouble ahead

Whoa!

Are you sure you want to go there?

https://www.warez-bb.org/login.php may be risky to visit.

Why are you seeing this?

When we visited this site, we found it exhibited one or more risky behaviors.

Link checking at search engines

- Second, it includes a ‘Secure Search’ feature which checks the links presented whenever you search the Web (at Google, for instance) and adds a little icon beside each to tell you whether each website is safe to visit.

> It’s worth noting that McAfee WebAdvisor’s advice is based solely on whether a website is known for attempting to infect your PC in some way. A ‘safe’ site in this respect isn’t necessarily one with good, honest business practices too!

To install McAfee WebAdvisor, follow these steps:

1. Start your favourite web browser and then visit the following address:

   home.mcafee.com/root/
   landingpage.aspx?lpname=get-it-now

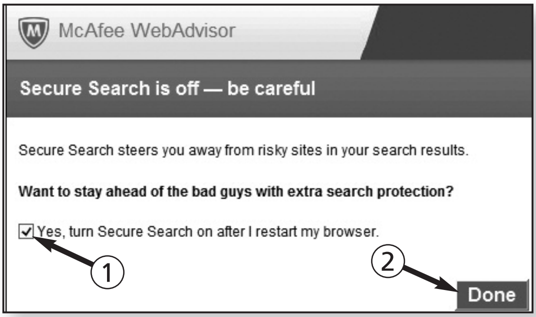
2. When you arrive at the page, click the red **FREE DOWNLOAD** button.

Start the installation

3. When the file has finished downloading, open it to begin installing McAfee WebAdvisor: you can do this by pressing **Ctrl+J** to display a list of downloaded files. This one should be right at the top of that list, named **saSetup.exe**: click it to open it, and click the **Yes** or **Continue** button in the ‘User Account Control’ security prompt that appears.
4. Tick the box to accept the licence agreement and then click the **Install** button. After a few seconds, the installation will be complete: leave a tick in the box beside **Open my browser** and click **Done**.
5. Your web browser will open another window and take you to a page on McAfee’s website. Here you can click a **Learn more** button to read a little more about WebAdvisor: feel free to do that.

6. Near the bottom of your screen, you'll also see a box that invites you to turn on 'Secure Search': make sure there's a tick in the box ① and then click **Done** ②.

Turn on ***Secure Search***



McAfee WebAdvisor

Secure Search is off — be careful

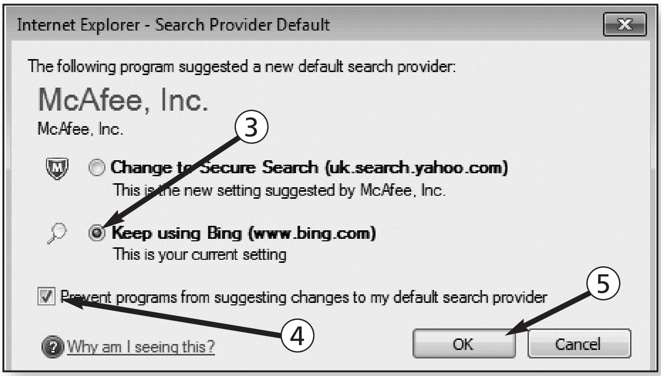
Secure Search steers you away from risky sites in your search results.

Want to stay ahead of the bad guys with extra search protection?

☑ Yes, turn Secure Search on after I restart my browser.

7. At this point, you may also see a dialog asking if you want to change your 'search provider'. I'm sure you're quite content with the website you use for searching the Web (probably Google or Bing), so select the **Keep using** option ③ to keep your settings unchanged. I also suggest ticking the box beside **Prevent programs from suggesting changes to my default search provider** ④. Having done that, click **OK** ⑤.

There's no need to change your search provider



Internet Explorer - Search Provider Default

The following program suggested a new default search provider:

McAfee, Inc.
McAfee, Inc.

○ **Change to Secure Search (uk.search.yahoo.com)**
This is the new setting suggested by McAfee, Inc.

● **Keep using Bing (www.bing.com)**
This is your current setting

☑ Prevent programs from suggesting changes to my default search provider

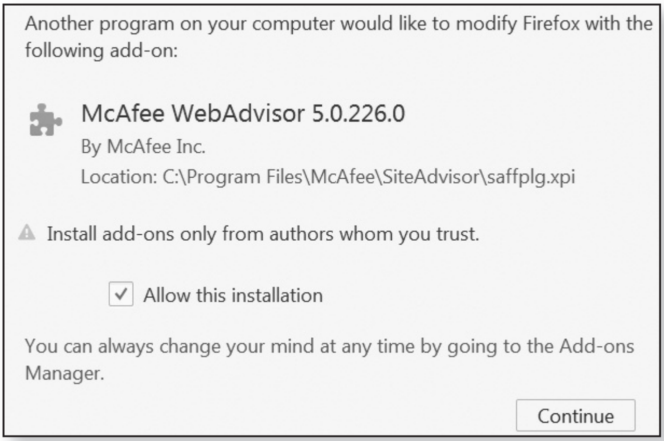
8. Now close your web browser: you quite likely have two browser windows open at this point – the one

Close your browser

you opened initially, and the one that opened in step 5 and took you to the McAfee website – so close both of them.

Allow the add-on to be installed

9. Wait a few seconds and then open your web browser again. As soon as it starts this time, your web browser will probably show a page explaining that the McAfee WebAdvisor add-on wants to be installed in your browser. The exact wording will vary according to which browser you're using (the screenshot below shows how Mozilla Firefox asks this question), but you must allow this add-on to be installed and enabled, so be sure to choose the Yes/Allow/Enable option.



Another program on your computer would like to modify Firefox with the following add-on:

McAfee WebAdvisor 5.0.226.0

By McAfee Inc.

Location: C:\Program Files\McAfee\SiteAdvisor\saffplg.xpi

Install add-ons only from authors whom you trust.

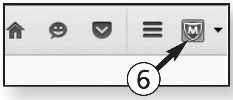
☑ Allow this installation

You can always change your mind at any time by going to the Add-ons Manager.

10. Having done this, you'll probably be prompted to restart your web browser one last time: do that, and you're all set!

One final setup step

11. Well, almost. There's one extra little change we'll make. On your browser's toolbar, you'll see that an icon for McAfee WebAdvisor has been added ⑥, with a little arrow to its right. Click that little arrow and choose **Options** from the menu that



appears beneath it. In the window that opens, scroll down a little way to find the 'Search results' heading and select the option that reads **Tell me if a search result is safe in any search engine**. Now click the grey **x** in the top-right corner of this window to close it.

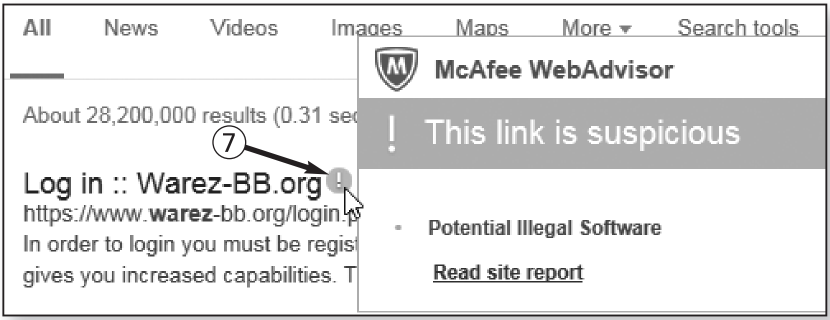
How WebAdvisor makes you safer

Now you're definitely all set and ready to continue with your web surfing as usual, but with some helpful added protection from McAfee WebAdvisor. So, here's what it does:

- First, as I mentioned on page 3, if you happen to land on a potentially-risky web page, you'll be whisked away from it to McAfee's special warning page. Here you can click on **Accept the Risk** if you really do want to visit the page, but an obviously-safer option is to click **Back** and go back to where you came from instead.

Check icons beside your search results

- Second, when you visit a search engine to search for websites, you'll see little colour-coded circular icons beside the links in your search results ⑦: a green tick means the link is safe; a yellow exclamation mark means its suspicious; a red cross means the link is dangerous. If you place your mouse pointer over one of these icons, you'll see a little pop-up panel confirming the diagnosis and containing one or two bullet-points explaining McAfee's findings. Any link that doesn't have a green tick is definitely best avoided!



About 28,200,000 results (0.31 sec

Log in :: Warez-BB.org

https://www.warez-bb.org/login.p

In order to login you must be regist

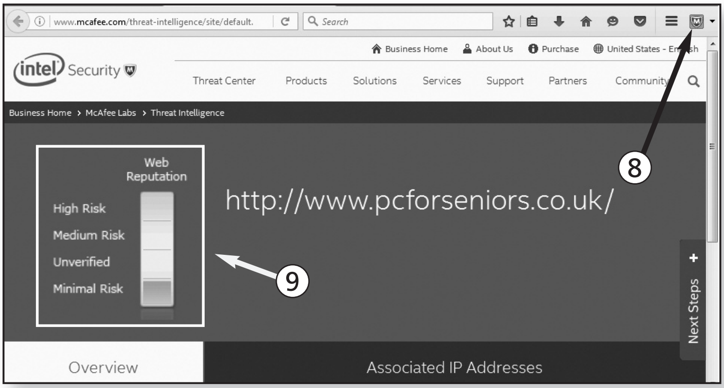
gives you increased capabilities. T

! This link is suspicious

- Potential Illegal Software

Reports of websites' safety reputations

- Third, WebAdvisor can give you a more detailed report on any website. If it's a site you've come across in a search, as explained above, you can click **Read site report** in the pop-up panel to read more about it before visiting. If you've already arrived at the site, click the McAfee icon on your toolbar ⑧. In both cases, the report opens in a new browser tab. The main point to check here is the 'Web Reputation' meter ⑨: if it shows a 'Minimal Risk', the site is safe to visit; if the meter shows either 'Medium Risk or 'High Risk', it's advisable to leave the site (or not visit it), and certainly not to download anything from it or provide any personal information. I would also suggest treating 'Unverified' websites in the same way: after all, there are plenty of known-safe websites out there!



Safeguard 2: Protect Yourself from Dangerous Ads

Malicious ads on hacked websites

Over the course of a week in mid-2015, several million visitors to over 50 websites (including the search engine Yahoo! and the photo service Flickr) had their PCs infected by malware embedded into Flash-based advertisements on those websites. Online criminals had managed to hack into those websites and place those infected ads on their web pages. Other well-known sites including Amazon and YouTube have also unwittingly found themselves serving up malicious ads to their visitors.

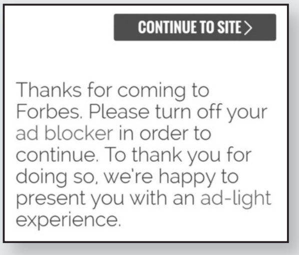
Clearly, then, simply keeping away from websites that are known to be risky isn't enough. In theory, any website can be hacked in a similar way, and it goes without saying that the hackers would want to target the most popular and frequently-visited sites.

Solution: install Adblock Plus

Therefore, by far the best safeguard is to install a so-called 'ad blocker', and the one I recommend (which I've used myself for years) is the free Adblock Plus.

The great thing about Adblock Plus is that you just 'install it and forget it'. At every web page you visit, it automatically removes the majority of advertising, leaving only the small, inoffensive (and harmless!) text-based ads. Crucially, this means that all ads using the potentially-risky Adobe Flash will be blocked, therefore making your surfing a great deal safer, not to mention much less annoying.

There's just one drawback to using an ad blocker. A few websites now detect that you have something like Adblock Plus installed and won't allow you to use the site unless you turn it off (or adjust its settings to add an 'exception' for that website which allows its ads to be displayed). This is on the basis that the site relies on its advertising revenue to continue. However, my advice is to keep the ad blocker enabled and, if you have no other choice, just leave the site.



Thanks for coming to Forbes. Please turn off your ad blocker in order to continue. To thank you for doing so, we're happy to present you with an ad-light experience.

Adblock Plus works with all four popular browsers: Internet Explorer, Mozilla Firefox, Google Chrome and the new Microsoft Edge (in Windows 10). To install it, follow these steps:

1. Start your favourite web browser and visit the address below:

   www.adblockplus.org

2. When you arrive, you'll see a large green button with the words **Install for Internet Explorer** or **Install for Firefox** (and so on, depending which web browser you're using). Click that button.

Follow the steps for your web browser

3. From here, the steps will vary from one browser to another:
   - In Internet Explorer, click the **Run** button on the panel at the bottom of the window, and choose **Yes** when prompted to close the browser. Follow the straightforward steps to install Adblock Plus and then start Internet Explorer again. When it starts, click the **Enable** button to allow Adblock Plus to start working.
   - In Mozilla Firefox, click **Allow** in the little pop-up message at the top of the browser window, then click **Install**.
   - In Google Chrome, click **Add extension** in the little pop-up box that opens, and the rest happens automatically within a few seconds.
   - In Microsoft Edge, you'll be taken to the Adblock Plus page in Windows 10's Store app. Click the **Free** button near the top of the page, and then wait while Adblock Plus is downloaded and installed. When this is done, close the Store window to return to Edge where you'll see a note saying 'You have a new extension'. Click **Turn it on** and you've finished.

Safer (and less annoying) surfing!

With Adblock Plus now installed, just carry on surfing as you normally do: it doesn't need any additional setting-up and it won't ever display warnings or ask questions. It silently blocks the risky and annoying ads from all the web pages you visit. Not only does that make your surfing much safer and less infuriating, but you'll also find that your web browser loads pages more quickly without the weight of all those extra ads!

Safeguard 3: Avoid Potentially Dangerous Web Addresses

Always tread carefully

Although tools like McAfee WebAdvisor and Adblock Plus can do a certain amount to help you avoid the dangers of the Web, it pays to keep your wits about you when surfing and look out for anything that doesn't seem quite right.

Understand and check web addresses

An important way in which you can do this is by keeping an eye on the addresses of the websites you're visiting and, better still, the addresses you're about to visit by clicking links to them: when you hold the mouse over a link in your browser before clicking it, you'll see the address that it leads to in a little box at the bottom of the window.

Here are the 3 key points to check in web addresses:

Is the domain name spelt correctly?

Intentional typos in the domain name

The 'domain name' is the part of the address that appears immediately before the first single-slash. Taking **http://www.microsotf.com/windows** as an example, the domain name is **microsotf.com.** But would you visit that site?

Hopefully not: it looks like a misspelling of 'microsoft'. That address has quite likely been registered by a scammer who hopes people won't notice that spelling mistake and will visit the site in the belief that it's the Microsoft website. I mentioned earlier that scammers set up clones of popular online stores, and they use the same trick: they can't register the **debenhams.com** domain name (because it's already owned by Debenhams), so they'll register a misspelling such as 'debnhams.com' or 'debenhms.com' and set up their cloned site there. Always check the spelling to avoid ending up at one of these risky websites!

Is the Top Level Domain correct?

Is the TLD unexpected?

The Top Level Domain (or TLD) is the last part of the domain name: **.com** in the examples above, or **.co.uk** in **www.pcforseniors.co.uk**. Most website owners try to buy a domain name ending in **.com** or **.net**, or in the TLD for their own country (**.co.uk** for the UK, **.fr** for France, **.de** for Germany, and so on).

The trick here is to watch out for unusual TLDs – those that don't match what you know about the company. For instance, **debenhams.co.nz** – the spelling is correct, but would Debenhams really have set up a New Zealand ('nz') website or is it more likely to be a scam? Likewise, **www.barclays.co** may look correct at first glance, but where's the **.uk**? Here, the TLD is just **.co**, denoting Colombia – not where you'd expect to find the real Barclays Bank website!

Are you looking at the name of a folder?

Is it the domain name…

You're led to believe that the link you're about to click would take you to the HSBC bank's website, whose domain name is hsbc.co.uk. However, that link looks something like this:

http://www.notables.ru/hsbc.co.uk/secure-login

… or just the name of a folder?

Do you trust it? You shouldn't! The domain name (before the first single-slash, remember) in this link is

notables.ru – a Russian domain name and certainly not one you'd associate with HSBC! Anything that appears **after** the single-slash is either the name of a folder or the name of a file, and anyone setting up a website can name their folders and files in any way they like (just as you can on your own PC).

In the example shown above, the scammer has named a folder 'hsbc.co.uk' in the hope that you'll trust this link simply because it contains the familiar HSBC domain name. Remember: check what comes before that very first single-slash. Anything that comes after it is irrelevant!

Safeguard 4: Follow These 4 Rules of Web Security

Continuing the theme of self-protection, I'll finish with 4 golden rules to keep in mind, which, between them, should help you steer clear of risky websites.

Rule 1: Avoid links in email messages

Be sure you end up at the site you expect!

In most email programs, just as in web browsers, you can move your mouse pointer over a link in an email message and you'll see where it really leads. By doing that, you can check the address against the three key points I covered above. But a safer option is simply not to click the link. If the message seems to have come from a company you know – your bank, an online store you use, a government organisation – a safer option is to start your web browser and type the address you know to be correct (or select it from your Favourites/Bookmarks list). That way, you can be sure of ending up at the right website. (And if the message didn't come from a company you know, are you sure you trust it? All the more reason not to click the link it contains!)

Rule 2: Did you type the address correctly?

Check for spelling mistakes

I've mentioned that scammers set up sites with names based on spelling mistakes or typos – microsfot.com, amazon.-co.uk and so on. They do that because they know we'll occasionally type an address wrongly into our web browser and end up at the scam site rather than the real one. After typing an address, always double-check its spelling before you press **Enter** to visit it.

Rule 3: Never install software you weren't actively looking for

Don't be fooled into installing software

Some websites (or the ads they display) show messages saying things like: You must install this codec to watch this video; You must install this software to use our site; Your PC is at risk, you must install this virus scanner. Never, ever do it – and ideally leave any site that tries to force unsolicited software on you straight away. The only software you should ever install is that which you've carefully selected based on trusted reviews or recommendations. And then only while keeping Rule 4 in mind…

Rule 4: Only download from trusted websites

Look for software on its maker's own website

You've decided that a particular program is worth having. However, if you simply search for it by name at Google or somewhere similar, you'll probably find it available at all sorts of sites. Do you trust them all? Can you be sure the copy they're offering hasn't been tampered with? Don't take any chances: find the website of the company which makes that software and download it directly from their own site!

Don't trust a bargain!

Likewise, if you know it's a program that should cost money, be very wary of any websites which claim to be offering it free, or surprisingly cheaply. Don't be tempted. There's always a catch, and that catch may turn out to be very expensive indeed!