



What is SiteAdvisor software?

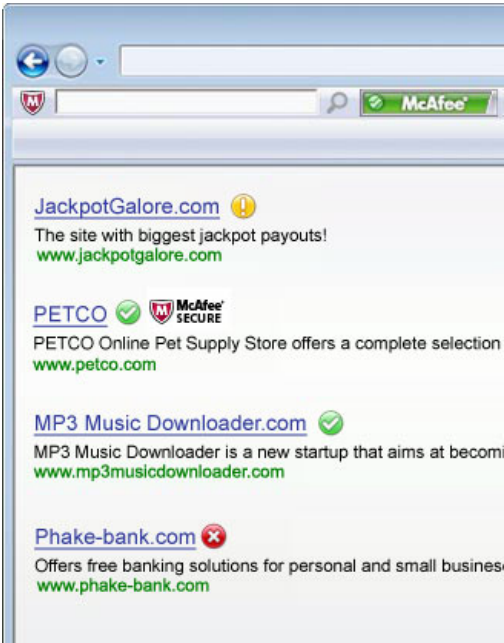
SiteAdvisor software is an award-winning, free browser plug-in that gives safety advice about Websites before you click on a risky site.

How It Works


With SiteAdvisor software installed, your browser will look a little different than before. We add small site rating icons to your search results as well as a browser button and optional search box. Together, these alert you to potentially risky sites and help you find safer alternatives.

These site ratings are based on tests conducted by McAfee using an army of computers that look for all kinds of threats (detailed below). The result is a guide to Web safety.


The SiteAdvisor technology is free, easy to install and even easier to use. And it doesn't collect any personally identifiable information.




Rating Icons




McAfee SECURE: Tested daily for hacker vulnerabilities.




SAFE: Very low or no risk issues.



CAUTION: Minor risk issues.




WARNING: Serious risk issues.




UNKNOWN: Not yet rated. Use caution.

Secure Search Icons



SECURE SEARCH BOX: Worry free searching.



BROWSER BUTTON: Validates site rating.

• [Learn more](#)

How Site Ratings Are Determined

Each day, thousands of times a day, McAfee visits Websites and tests them for a comprehensive set of security threats. From annoying pop-ups to back door Trojans that can steal your identity, we find the danger zones before you stumble on them. Here's what our test computers look for.

[Downloads](#)

[E-mail Practices](#)

[Browser Exploits](#)

Downloads

Downloadable files like screensavers, toolbars and file sharing programs can be-or may be bundled with -- [adware](#), [spyware](#), [viruses](#) and other malicious computer code. Sometimes, the malware is added without your knowledge. Sometimes, you click "yes" or "I agree"

[Phishing Sites](#)[Web Reputation](#)[E-Commerce Vulnerabilities](#)[Website Annoyances](#)[Links \(Online affiliations\)](#)

without reading the fine print. The end result is often the same – a PC that slows to a crawl, a hidden password sniffer that is used to steal your identity, or valuable personal files destroyed or scrambled.

We download and install each file we find – we even open zip files. We then scan our test computer to see what changes have been made. If a program is determined to be a virus, Trojan, or certain other types of malware, that program will earn a red rating.

E-mail Practices

[E-mail](#) is one of the most enduring vehicles the bad guys use to get their hooks into unsuspecting consumers. "Free" product lures, cheap overseas pharmacies, phishing URLs masquerading as real bank sites, and ever present adult material tax your time, your inbox and sometimes even your wallet. The worst of them can lead to [identity theft](#).

Our test computers click on these links and register our e-mail at each sign-up we find. We use each test e-mail address once and only once so we know exactly what registration led us to receive a given set of e-mails. Depending upon the type and number of e-mails we receive, we may assign a yellow or even red rating for that site's e-mail handling practices.

Browser Exploits

A browser exploit is a rare but especially nasty piece of computer code that installs itself on unprotected computers, often without a consumer's knowledge. Exploits, sometimes called drive-by-downloads, are one of the key tools scammers use to install keystroke loggers (which can steal your passwords) and Trojan programs (which can turn your computer into a 'bot or slave machine'). We test each site we visit for exploit code using an unprotected computer. If we find an exploit, it always earns a red rating. By letting the bad guys do their worst to us, we prevent them from doing their worst to you.

Phishing Sites

One of the most popular weapons scammers have to steal our sensitive personal information – especially our financial information – is the [phishing](#) site. These imposters are pixel perfect copies of real sites – typically bank, e-commerce and auction sites – that trick even the savviest users into submitting detailed information like bank passwords or credit card numbers. Once that information gets sold on the black market, consumers can suffer complete identity theft.

We automatically rate phishing sites red and whenever you try to browse to one, we automatically re-direct you to a warning page.

Web Reputation

SiteAdvisor ratings now incorporate web reputation analysis from the McAfee TrustedSource™ system. This system collects security data from tens of millions of sensors located in more than 120 countries. McAfee's proprietary technology analyzes traffic and linking patterns, website behavior, content analysis, site registration and hosting, to develop an overall reputation rating for the website. TrustedSource data complements SiteAdvisor software by adding quick response to new threats. When TrustedSource sensors - whether individual computers or corporate servers - discover a risky website, the entire system is updated with this new information.

E-Commerce Vulnerabilities

E-commerce sites are especially attractive to hackers because successful break-ins can lead to a treasure trove of detailed consumer financial data. Hackers then sell that information to scammers who use your identity to buy stuff for themselves!

Thousands of the most popular e-commerce sites have signed on with McAfee to conduct daily tests for hacker vulnerabilities. Sites that pass are known as McAfee SECURE sites, which means they are safe from more than 10,000 known hacker vulnerabilities. And that means consumers are less likely to fall victim to identity theft.

Website Annoyances

Pop-ups and cookies are a fact of life on the Internet. We test each website we visit for both. Sites with excessive pop-ups or traps that spawn new pop-ups when you try to close or leave the site are rated red. We report our findings about each site's cookies on its site profile page, but do not penalize a site for their presence.

Links (Online affiliations)

As Web users get smarter about Web security, the scammers have had to get sneakier about trying

to snare you. One trick they use is to set up lots of websites that by themselves are not malicious, but exist just to funnel visitors to an infected download, a spam trap or a drive-by-download site. Using our incredibly detailed database of Website safety, we rate sites red or yellow if we think too many of their links go to other risky sites.