

**EXCLUSIVE REPORT**

# **SAFE ONLINE BROWSING**



**Protect Your Web Browsing  
Experience From Cyber Threats**

# Safe Online Browsing

---

## How can we be sure we are safe online?

We are surrounded by Information Technology and its various forms and implications. But, this every day connection makes us dependent and open to threats from outside.

We are prepared to use our operating systems at home, at work and somewhere between these two, a space we usually dedicate to our passions and hobbies.

Even more, we connect and synchronize our mobile phones to our systems, so that we may always be on alert with all the “important” news out there.

But our continuous strive to stay up to date and connect from everywhere doesn’t make us vulnerable?

## So, how do you stay safe?

It is quite “simple”, you start buying and installing:

- “well-known” antivirus against online threats
- “good” security product against spyware
- “reliable” pop-up blocker
- “specialized” security product against online criminals
- “strong” back-up product to make sure you are covered in case of disaster
- “useful” utility program to clean unwanted files (temporary Internet files or cookies) and orphan Windows registry files.

The bigger question at hand here is... **is it enough?**

## **Are you now protected? Or is there anything else you should pay attention to?**

We are not saying that installing various security products won't improve your online security and that you won't be as safe as possible. But before you start investing time, energy and money in so many security tools, why don't you start by improving the main free tool you use to reach the online world: your BROWSER.

Today, some of the most popular web browsers, like Internet Explorer, Mozilla Firefox and Google Chrome are installed on most Windows operating systems. And it is easy to notice the increasing threat coming from online criminals that try to take advantage of web browsers and their vulnerabilities.

Using these open gates, they compromise legitimate websites or they place malicious content on legitimate websites so that an user may be easily deceived in clicking and downloading data or financial stealing malware.

Securing our browser is the first step we need to take in order to assure our online protection and it is a mandatory step, since a number of factors and causes arise and complicate our task:

- inexperienced users click on links without analyzing the risks they expose themselves to.
- websites that are disguised as legitimate sites or web locations that contain malicious content.
- web browsers that promise fast connection and download speeds without keeping a high security level.
- browser (or application) vendors which are late in discovering and patching security vulnerabilities. We have already covered this issue regarding the applications' slow patching process in this article.

- drive-by downloads, which imply that some downloaded software packages are bundled with another application or program which may prove dangerous for system's security and stability.
- programs and applications downloaded and installed on the system without having the possibility of receiving security patches.
- questionable websites that ask the user to install and enable additional features so that malicious content may be downloaded on the system.
- users that lack the necessary knowledge to configure and secure their web browsers.
- web browsers' vulnerabilities, which become a favorite means for online criminals to exploit and compromise operating systems.

## Browser Features And The Risks They Pose

We rely on our browsers to access various web pages and locations and to have a complete online experience, our browsers use and employ various elements, such as Java, ActiveX and cookies to generate content for the required web pages.

Before we can configure our browser and increase our online security, we must understand a few terms since we have to deal with them again and again in our attempts to protect our sensitive data.

These features are usually enabled by default in our browsers to improve our online sessions, but at the same time these options pose a big security risk for our operating systems and databases. The recent years have revealed that online criminals use available vulnerabilities in our browser and in its additional features to control operating systems, retrieve private data, damage important system files or install data stealing software.

The features presented below are important for your browser's operation and for your online security, therefore we must acknowledge their role before we can decide if we need to disable them or not.

- **ActiveX** is a software component or an add-on of Windows operating systems and it comes already installed on our computers if we have Internet Explorer. ActiveX is required by some websites to view certain elements or take actions, improving the general browsing experience, so when you access an online website, you may be requested to install it. At the same time, we must acknowledge that online criminals may use ActiveX in creating and adding malicious ActiveX software to web pages in order to damage computers. If you don't need ActiveX in your computer activity, do not install it, especially if you don't trust the publisher or the website.

- **Java** is a programming language developed to create applications on our computers or active content on a website. Java has two parts: the Java application that runs on our computers and the browser plug-in, which we recommend you to disable unless you really use it.
- The Java browser plug-in opens up a great number of security holes allowing hackers to access your personal data, such as your credit card information or your banking account credentials. For more information about this threat, read this [article](#).
- **JavaScript** is a programming language that makes web pages interactive and is used mainly for displaying dynamic content, improving your online experience. The problem with JavaScript is that many viruses are script based and a great number of scripts can be dangerous being used to delete system files or perform a number of malicious tasks.
- **Cookies are files which are stored on your browser** and hold some amount of data about your browsing history. They are used by many websites, since there would be a lot of information to burden the website's server machine. They can be accessed by a website in order to improve your browsing session, though this behavior has given rise to privacy concerns and security issues.
- **Extensions or add-ons** are pieces of software that add or modify a feature or a functionality in your web browser. Some of them allow you to block ads, watch online videos or they are closely integrated in social media websites improving your online session. For example, Adobe Flash is an add-on which allows your web browser to watch movies or play online games. The possible issues which may appear from extensions is that some of them can be used to inject ads into the sites you visit or track your entire browsing activity, being therefore used for malicious purposes.

## Tips & Advice For A Secure Browsing Experience

We covered the main steps we can take in Internet Explorer, Mozilla Firefox and Google Chrome to secure our browsing sessions. But, we also need to display some general recommendations we can follow to improve our online safety, no matter what type of browser we are using:

- **Keep the browser up-to-date with the latest patches.** Your browser, as well as other software you have installed on the system, even the operating system, must have the latest patches installed as soon as they become available. It is important for your online security, because they are released in order to fix product vulnerabilities. If you don't do this simple step, you expose your system security to online criminals' attacks.
- **Use a good antivirus program** from a big company, as your virus defense. It is important to have a reliable security software on your system, one which should include a real-time scanning engine. Having a real-time scanning engine means that files you download from online locations are analyzed as soon as they are on your computer. Find the best solution by checking the test results run by important names in the security industry, such as AV Comparatives, PC Magazine, AV-TEST or Virus Bulletin and select the best antivirus solution.
- **Stay away from phishing attacks.** This malicious attempt to retrieve personal information from a user is usually done using the e-mail. Typically, you receive an e-mail message which seems to be coming from a banking website or from an online shop. The problem is with the links from these e-mail messages. Though they seem to be authentic, if you click one of them, you will be directed to a fake version of the website.
- **Don't use the same password for all your online accounts.** If you use the same password in multiple locations, you better change it as soon as possible. Just

imagine what happens if a hacker gets access to one of your online accounts: in just a few moments, he will get access to all your accounts. Even if you are hacked, having different passwords for each account will help you limit a potential loss.

- **Use secure websites for your sensitive online operations.** You should be very careful when running financial transactions on any web location. To visit a secure website, make sure the web address starts with “https://”. The “s” comes from “secure socket layer” and it indicates you are connected to a website where data, which is sent and received, is encrypted.
- **Monitor your bank account with Online Banking Alerts.** You can set up alerts for any change in your banking account, such as when you receive money or when money are taken from your account. Normally, you will be informed when your salary is received or when an automatic payment has been done. But it is useful also in case someone tries to remove unauthorized money from the account.
- **Be careful when connecting to public and free wireless networks.** One of the favorite methods used by online criminals to retrieve your credentials is by using wireless sniffers to access data sent over unprotected networks. One way to increase your security is by using a “private browsing” session, this way you make sure your credentials won’t be stored locally. Nevertheless, this won’t stop the Internet Service Provider or anyone else “listening” out there to catch your private communication.



## Conclusion

In this fight for online protection, keeping your main tool – the BROWSER – secure is a vital step.

That is why our operating system defense should contain multiple layers of protection, from security products to manually customizing our browsers, since our web browser is actually the central tool we use to access our social media accounts, our e-mail addresses and our online banking websites.

Simply said, our browser has become the essential connection tool we use to reach the Internet.

But, as we previously said, there is an ongoing fight and challenge for online security and we have to be open and accept alternative means to protect our private data.