5 Browser Security Myths That Need Busting

SYDNEY BUTLER, howtogeek.com, @gendowasright, JUN 14, 2023

Misinformation or outdated advice about online security can make you and your personal data vulnerable. So let's look at five common browser security myths so you can keep your understanding of browser security and the browser itself up to date together.

Incognito Mode Makes You Completely Anonymous

The myth that incognito or private browsing mode makes you completely anonymous is a common misconception. Incognito mode provides privacy by not storing your search history, cookies, or form data. However, this only applies to your particular device and browser.

Your internet service provider (ISP), network administrator, and the websites you visit can still track your activities while in this mode. Also, if malware lurks on your device, incognito mode won't hide your activities from it. For more robust privacy, you might consider using a VPN or a privacy-focused browser like Tor, though these tools also have limitations that we will discuss later.

A Secure Website (HTTPS) Means It's Safe to Browse

Most internet users have been taught to trust websites that use HTTPS, indicated by a padlock symbol in the browser's address bar. It's true that HTTPS encrypts your communication with the website, which prevents snoopers from reading the data in transit. However, this does not guarantee that the website itself is safe.

HTTPS only ensures secure transmission of data; it does not ensure the integrity of the site's content. Cybercriminals can also use HTTPS on their malicious sites, tricking visitors into thinking these sites are safe. Always ensure the website you're visiting is genuine and reputable, regardless of whether it uses HTTPS.

Downloading Files Is the Only Way to Get Malware

Many people believe that they can only get malware by downloading and running suspicious files. While this is one way to get infected, it's not the only way. Drive-by downloads and malicious advertisements can infect your computer without requiring you to download and run a file manually.

You can also get infected by simply visiting a compromised website, even without clicking on anything. Always keep your browser and its plugins updated to the latest version to guard against known vulnerabilities, and consider using a reputable ad blocker to minimize risks.

All Browser Extensions Are Safe

While browser extensions can add useful functionality to your browser, not all extensions are safe. Some extensions may contain malicious code, while others might track your browsing activities for marketing purposes. Even extensions that were initially safe can become harmful if they're bought and repurposed by less scrupulous developers. Which is why we've called browser extensions a privacy nightmare, and you'll often see news about popular extensions hiding malware.

Therefore, always be cautious about the extensions you install. Only install extensions from trusted developers, and check the permissions an extension asks for during installation. A weather forecast extension, for example, shouldn't need access to your entire browsing history—and you may want to consider if you even need a weather forecast extension in the first place.

Using a VPN Makes Your Browsing Completely Secure

VPNs are a great tool for privacy and security, but they're not a silver bullet. A VPN encrypts internet traffic and masks your IP address, making it more difficult for others to track your online activities. However, it does not make your browsing completely secure.

The websites you visit, and any malware on your device, can still potentially track your activities. Moreover, the VPN provider itself can see your internet traffic unless it employs a strict no-logs policy. And it's important to set up your VPN correctly and avoid common mistakes.

Therefore, while a VPN is a good tool for online privacy, it should be used in combination with other security measures, like secure browsing practices, updated software, and strong, unique passwords for each of your online accounts.