Staying safe online: How to browse the web securely

DUBAI, UNITED ARAB EMIRATES, August 17, 2022 /EINPresswire.com/ -- Phil Muncaster, guest writer at ESET explains how to spot some of the threats that you can face while browsing online, and the best tips to stay safe on the web.

Web browsers are our gateway to the digital world. We spend hours on them each day, which makes them not only a vital tool for legitimate users, but a valuable target for threat actors. Over the years they've become a repository of credentials, cookies, web searches, and other juicy information that could be targeted by cybercriminals. They may even use attacks to control your computer remotely and access the network it's connected to.

Threats go beyond malicious third parties. Many users may also feel slightly queasy at the thought of third-party advertisers and others accessing and tracking their personal information via the browser. Fortunately, there's plenty you can do to manage these risks.

Top browser threats
There are plenty of threats out there: some targeting browsers more directly than others. Here are a few of the top ones:

Exploitation of vulnerabilities in browsers or any plugins/extensions you may have installed. This tactic could be used to steal sensitive data or download additional malware. Attacks often start with a phishing email/message, or by visiting a site that has been compromised or is controlled by the attacker (drive-by-download).

Malicious plug-ins: There are thousands of plugins on the market, which users can download to enhance the browsing experience. However, many have privileged browser access. That means malicious plugins spoofed to appear legitimate could be used to steal data, download additional malware and much more.

DNS poisoning: DNS is the address book of the internet, converting the domain names we type into IP addresses, so that our browsers display the sites we want to visit. However, attacks on the DNS entries stored by your computer, or on DNS servers themselves, could allow attackers to redirect browsers to malicious domains like phishing sites.

Session hijacking: Session IDs are issued by websites and app servers when users log in. But if attackers manage to brute force these IDs or intercept them (if they aren't encrypted), then they could log in to the same sites/apps masquerading as the user. From there, it's a short hop to stealing sensitive data and potentially financial details.

Man in the middle/browser attack: If the attackers manage to insert themselves between your browser and the websites you're viewing, they might be able to modify traffic – for example, redirecting you to a phishing page, delivering ransomware, or stealing logins. This is especially true when using public Wi-Fi networks.

Web app exploitation: Attacks like cross-site scripting can still target apps on your machine rather than the browser, but the latter is used to deliver or execute the malicious payload.

The privacy angle
These scenarios all involve malicious third parties. But let's not forget the large amounts of data that internet providers, websites, and advertisers collect on visitors every day as they browse the web.

Cookies are small bits of code generated by web servers and stored by your browser for a certain amount of time. On the one hand, they save information that can help to make the browsing experience more personalized—for example, showing relevant ads or ensuring you don't have to log in multiple times to the same site. But on the other hand, they represent a privacy concern and a potential security risk, if hackers get hold of them to access user sessions.

In the EU and some US states, the use of these is regulated. However, when presented with a pop-up of options, many users simply click to accept the default cookie settings.

How to browse the web more securely
There's plenty that users can do to mitigate security and privacy risks when browsing the web. Some involve the browser directly; others are best practices that can have a positive knock-on impact. Here are some key best practices:

Keep your browser and plugins updated, to mitigate the risk of vulnerability exploitation. Uninstall any out-of-date plugins to reduce the attack surface further

Only visit HTTPS sites (ones with a padlock in the browser address bar), meaning hackers can't

snoop on traffic between your browser and the web server

Be “phishing aware” to reduce the risk of browser threats that travel via email and online messages. Never reply to or click through on an unsolicited email without checking the sender’s details. And don’t hand over any sensitive information

Think before downloading any apps or files. Always go through official sites

Use a multi-factor authentication (MFA) app to reduce the impact of credential theft

Use a VPN from a reputable provider, and not a free version. This will create an encrypted tunnel for your internet traffic to keep it safe and hide it from third-party trackers

Invest in multi-layered security software from a reputable vendor

Enable automatic updates on your OS and device/machine software

Update browser settings to prevent tracking and block third-party cookies and pop-ups

Switch off password auto-save in the browser, although this will impact the user experience when logging in

Many of the above tips are optional and will depend on how strong your privacy concerns are. Some users are prepared to accept a certain amount of tracking in return for a smoother browsing experience. However, the security tips (like HTTPS, automatic updates, security software) are essential to reduce your exposure to cyberthreats Happy browsing.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
