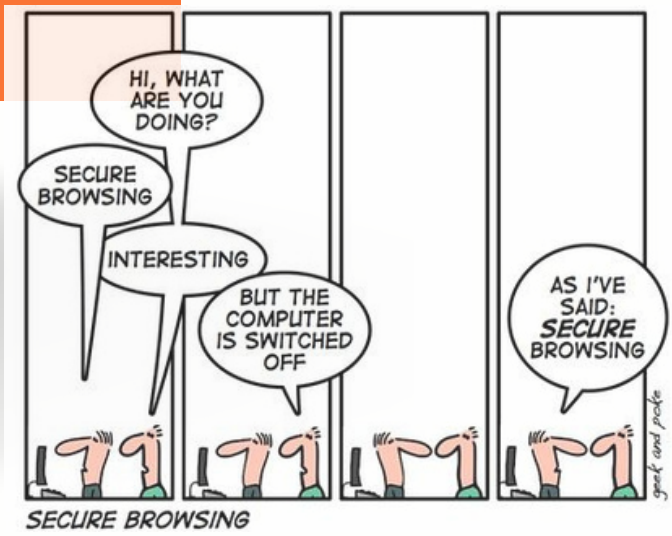
Security Matters

NEWSLETTER



BROWSE BETTER, BROWSE SAFER: TIPS FOR ONLINE SAFETY

In today's interconnected world, the internet serves as our digital playground, our virtual marketplace, and our source of information with just a few clicks. However, this convenience also exposes us to potential risks, from cyberattacks to data breaches. As we delve into the realms of online security, we'll explore the threats that lurk in the digital shadows, from phishing scams to malicious websites.

Web browsers have become flooded with ad-sponsored content, making browsers a key battleground for end-user privacy. Data is one of today's key ingredients for generating revenue. Online advertising companies can use web browsing histories to fingerprint individual browsers over time, creating shadow user profiles to reveal information including a user's interests, product searches, and more.

Before any browsing activity, choose your browser wisely. Below are some best practices when choosing and using a browser securely.

Firefox

- ☑ Recommend using **Firefox** as the **default browser.**
- ☑ Turn on "**HTTPS-only mode**".
- ☑ Install and enable browser extension:
  - **Privacy Badger** (block invisible trackers)
  - **uBlock Origin** (content and ad blocker)
- ☑ Recommend using **DuckDuckGo** as the **default search engine.**
  Firefox > Settings (the three horizontal lines at the top right of the browser bar) > Search > Default Search Engine > Drop-down menu to select DuckDuckGo.
- ☑ Firefox will configured to "Always use private browsing mode".
- ☑ Enable **two-step authentication**. Download software tokens beforehand. E.g. Authy, Google Authenticator.

Google Chrome

- Turn on "**Always use secure connections**".
- Install and enable browser extension:
  - **Privacy Badger** (block invisible trackers)
  - **uBlock Origin** (content and ad blocker)
- Recommend using **DuckDuckGo** as the **default search engine.**
  Google Chrome > Settings (the three vertical dots at the top right of browser bar) > Search engine > Manage search engine > Click the vertical dots next to DuckDuckGo > Make default
- Google Chrome will configured to "Clear cookies and site data when you close all windows".
- Enable **two-step verification**. Download software tokens beforehand.
  E.g. Google Authenticator, Authy.
- Review and remove third-party apps & services with account access.
- Manage location history and devices with account access.

Tor Browser

- Designed for private and anonymous web browsing by routing your internet traffic through the Tor network.
- Your activity bounces around the network until it reaches its destination.
- Provides anonymity online, making it difficult for anyone to track your internet activity.
- Protect yourself against tracking, surveillance, and censorship.
- Can be slow at times.

Some other best practices for online safety:

1. Always check for a URL beginning with "**HTTPS**" or a **padlock** icon in the browser bar.
2. Beware of short URLs.
3. Disable the "remember/saved password" option.
4. Clear your browsing history, cookies and cache regularly.
5. Keep your digital arsenal up-to-date, including the operating system, browsers, apps, anti-virus, and anti-malware software.
6. Think before you click on links and attachments.
7. Never give away your credentials.
8. Change your password regularly. Enable two-factor authentication (2FA).
9. Use a Virtual Private Network (VPN) to keep your online activity private.
   E.g. Proton VPN, TunnelBear, Express VPN

Related News

Fake version of two Android apps need to be uninstalled now before your bank account info is stolen

Fake Signal and Telegram apps have been distributed through the Google Play Store and Samsung Galaxy Store. The apps, which are called Signal Plus Messenger and FlyGram, are designed to steal user data, including contact lists, call logs, and device information. The apps were initially targeted at users in China, but have since expanded to other countries.
Read more: https://bit.ly/45CoQM4

Update your iPhone: Apple just pushed out a significant security update

Apple released a significant security update for iPhones and iPads Sept 7 to patch newly discovered security vulnerabilities in the devices' system software. The issue was discovered by researchers at the University of Toronto's Citizen Lab, who said the software flaw was being "actively exploited" to deliver commercial spyware called Pegasus developed and sold by the Israeli company NSO Group.
Read more: https://bit.ly/3NRg991

Millions infected by Spyware hidden in fake Telegram apps on Google Play

Spyware masquerading as modified versions of Telegram have been spotted in the Google Play Store that's designed to harvest sensitive information from compromised Android devices. The activity has been codenamed Evil Telegram by the Russian cybersecurity company. The apps have been collectively downloaded millions of times before they were taken down by Google.
Read more: https://bit.ly/45aF9iW

Beware of fake browser updates that install malware on systems

Hackers have been stealing millions of dollars in cryptocurrency, seemingly after the LastPass (password manager) breach. The LastPass data breach of 2022 saw criminals accessing entire password vaults, leading to a series of increasingly implausible denials from the company.
Read more: https://bit.ly/47BjGB8

If you didn't change your passwords after the LassPass data breach..Do it now!

Hackers have been stealing millions of dollars in cryptocurrency, seemingly after the LastPass (password manager) breach. The LastPass data breach of 2022 saw criminals accessing entire password vaults, leading to a series of increasingly implausible denials from the company.
Read more: https://bit.ly/44Gq2gO

Google Chrome teases full tracking protection tool to keep users protected

Google Chrome plans to introduce a “Tracking Protection” section in settings for its Windows, macOS, and Android versions. This section will consolidate various features to prevent tracking while users surf the web. The “Tracking Protection” page will have options for users to choose their desired level of protection.
Read more: https://bit.ly/45CoQM4

How to delete private browsing history and protect your privacy

Most people use the incognito browsing mode when they want to keep their browsing history private, but simply using Incognito or Private Mode isn't enough. Your Internet Service Provider (ISP) and other third-party entities may still be able to track your online activity, even during private browsing. Not only that but if you share your device with others, even they can find out what you visited in incognito mode.
Read more: https://bit.ly/3PIr9aU

Update everything: This critical WebP vulnerability affects major browsers and apps

A major vulnerability in the WebP Codec CVE-2023-4863, has been discovered, forcing major browsers to fast-track security updates. A heap buffer overload occurs when a program writes more data to a memory buffer than it's designed to hold. When this happens, it can potentially overwrite adjacent memory and corrupt data. Worse still, hackers can exploit heap buffer overflows to take over systems and devices remotely.
Read more: https://bit.ly/45aF9iW

This devious phishing scam makes it look like dodgy emails are actually safe

Hackers are using the dreaded “zero font” tactic in phishing emails, instilling a false sense of legitimacy in otherwise malicious threats. Hackers use the size 0 for a font, making certain text invisible to the human eye. Threat actors leverage this fact to confuse email security solutions and have otherwise malicious emails end up in the inbox, instead of the spam folder.
Read more: https://bit.ly/47BjGB8