Knowledgebase > Security > Browsers and Search Engines > Browse More Safely with an Ad Blocker

Browse More Safely with an Ad Blocker

patricia falcon - 2023-09-29 - Comments (0) - Browsers and Search Engines

Ads while browsing aren’t only annoying but can also be dangerous. **According to the FBI**, cyber criminals are using search engine advertisement services to impersonate brands. Clicking on one of these fake ads will direct the person to malicious sites that host ransomware and steal login credentials and other financial information.

To protect yourself, take a few simple precautions when on the web:

- Type a business’s URL into a browser’s address bar to access the official website directly, rather than search for a business or financial institution.
- Before clicking on an advertisement, check the URL to make sure the site is authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.
- Use an ad blocking extension on your browser when performing internet searches. Most browsers allow a user to add extensions, including extensions that block advertisements, and many are free. These ad blockers can be turned on and off within a browser to permit advertisements on certain websites while blocking advertisements on others.

For suggestions on which ad blocker(s) to install (you can use more than one such as combining a privacy tool like Privacy Badger along with a specific ad blocker) read PC Magazine's **The Best Ad Blockers for 2023** or Wirecutter's **Our Favorite Ad Blockers and Browser Extensions to Protect Privacy**, or **Tom's Guide**, which breaks them out by browser type (i.e., Chrome, Edge, Firefox, Opera, Safari, Android, iOS).

To add your choice(s), search for that name in your browser’s app store, usually accessed through its Extensions/Add-ons/Plug-in function, and select it to add the extension. You may need to “pin” it to your browser to have it displayed with the other extensions. Clicking on it allows you to view its options and update any settings.

If you believe you've become a victim, report it:

Let the OIT Information Security Group (isg@brown.edu) know if you have encountered one of these malicious ads. And if you believe you’ve been a victim of fraud or malware based on brand impersonation from search engine advertisements, you should report the incident to your local FBI field office at **www.fbi.gov/contact-us/fieldoffices**. The FBI also encourages victims to report fraudulent or suspicious activities to the FBI Internet Crime Complaint Center at **www.ic3.gov**.

Related resources:

- Block or Allow Pop-ups
- Keep your browser up to date
- Use private search engines