BE LIBRARY SMART: PROTECTING YOUR PRIVACY

BROWSERS AND SEARCH ENGINES

duckduckgo.com This search engine doesn't track your activity, and their mobile app that assigns grades based on sites' privacy offers more secure mobile browsing.

startpage.com This search engine uses Google's results but does not track your IP address or use cookies.

brave.com Brave is a browser that blocks trackers and ads and automatically upgrades to https when available. Their mobile app features the same protections.

torproject.org The Tor browser routes users' activity through proxies all over the world to help provide anonymity.

ADD-ONS/EXTENSIONS

disconnect.me This browser extension blocks third-party trackers. Available for Chrome, Firefox, and Opera, with laptop/desktop and mobile versions.

noscript.net This browser extension disables JavaScript, Flash, and other elements of websites that can be used to track or infect a computer. Available for Firefox and Chrome.

HTTPS Everywhere If a secure version of a website exists, this extension will automatically connect to it over the insecure default version. Available for Firefox, Chrome, and Opera. eff.org/https-everywhere

Privacy Badger This add-on prevents websites from using invisible trackers. It learns from trackers' behavior to block tracking across multiple sites. Available for Firefox, Chrome, and Opera. eff.org/privacybadger

uBlock Origin This add-on blocks ads, trackers, and malware. Available for Firefox, Chrome, Microsoft Edge, and Safari. github.com/gorhill/uBlock

Brought to you by the Maryland Library Association's Intellectual Freedom Panel and the Ruth Enlow Library.

BE LIBRARY SMART: PROTECTING YOUR PRIVACY

APPS AND SERVICES

VPN Short for Virtual Private Network, this will route your internet connection through different IP addresses to better protect your privacy. VPNs are especially useful when using public or free wifi connections. They vary in price, features, and reliability, so do your research.

Password Managers Generate and store complex passwords to keep your accounts safer. Popular providers include LastPass, 1Password, DashLane, and KeePass. Paid and free versions available.

Two-Factor Authentication: Enabling two-factor authentication makes your accounts more secure by requiring a second form of identity verification when logging in. Check whether 2FA is available for your accounts at twofactorauth.org.

Looking for more? Visit PrivacyHaus [privacy.haus], a curated collection of apps and services that prioritize privacy.

TIPS & TRICKS

- Don't reuse passwords for multiple accounts.
- Don't save information like usernames or passwords in web forms, especially on public or shared computers.
- Look at the URL of websites you visit. Websites that start with "http" are not secure. Don't enter personal information or account numbers on sites that don't start with "https".
- Be cautious with flash drives: using one you're not familiar with can infect your computer with malware. Only use a flash drive if you know where it has been, or scan it with security software before use.
- Enable automatic updates for your browser, security software, and operating system to make sure you have the latest security patches and protection against threats.