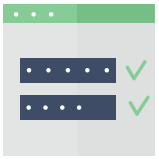
ONLINE PRIVACY GUIDELINES

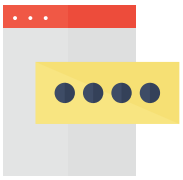
Use these steps to keep your online information profile more secure. Questions? Please contact the library at **askus@wnpl.info**.

ACTIONS TO TAKE



Have a unique password for each account. Do not reuse passwords. If you keep a paper list of passwords, keep them in a locked safe or another secure location.

Change passwords frequently, at least once every three months.

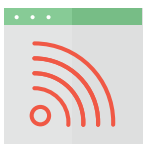


Use two-step authentication, particularly with financial accounts. Two step authentication adds a second step to the login process by requiring a phone call, text, or email with a security code, sent to your registered contact information.

Use antivirus software on your devices, like McAfee or Kaspersky.

Install all updates for your computer or device - updates give your technology the most current protection.

Use an email search tool to see if your email address has been compromised in a data breach. Tools like 'Have I Been Pwned?' and "What Is My IP Address?" will search for email addresses associated with data breaches.
https://haveibeenpwned.com/
https://whatismyipaddress.com/breach-check



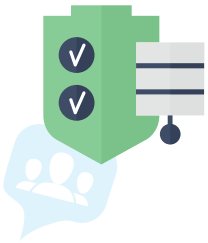
Be cautious when using free, unsecured WiFi - since anyone can use these networks, it makes users more vulnerable to hacking. Avoid signing into financial accounts on a public WiFi system.

Do not open suspicious email or text messages. These messages can contain links to damaging scripts or programs.

Shop at online stores that provide secure connections - look for websites that begin with https:// and have a lock symbol next to the web address.

Warren-Newport Public Library
224 N. O'Plaine Road, Gurnee, IL 60031
847-244-5150 • www.wnpl.info

ONLINE PRIVACY GUIDELINES



Guard your social media privacy - be mindful that what you post on social media can potentially be seen by anyone (even people with harmful objectives), and do not make your profile public. Set your privacy settings to the highest possible option, and review them frequently (look for the settings icon in the app or website menu - it will say settings or have a gear symbol next to it - then look for privacy settings).

Back up important data and files. If you save tax returns or bank statements to your PC, keep a copy of those files on a flash drive.

Cover your webcams! Use a piece of masking tape to cover the camera on your computer or phone when not in use. Turn off your microphone when not in use.

Use 'incognito' mode on your browser. Incognito mode allows users to search the web while rejecting or avoiding standard data collection practices.

Utilize ad blocking and popup blocking options in your browser - click the settings link in the top right corner of your browser screen and review your blocking options (in Chrome, the settings can be reached from the menu dots -- three vertical dots on the upper right side of the browser).

Consider using a browser specially designed to protect your privacy online - DuckDuckGo is a free Internet browser that does not track user info or activity.

Be skeptical online. People and organizations can be dishonest about who they are and what their intentions are, so do your due diligence. Look for reviews of websites and verify that you have the correct web address. If you receive an email, text, or phone call from a government agency, your bank, or a retailer that you do business with, and they ask for account information, do not give it to them. Call the agency or organization directly to verify that they have reached out to you.

The following articles outline the privacy options listed above, and much more. If you have additional questions, please contact the library via email at **askus@wnpl.info**.

https://internetsafety101.org/StepsToPrivacy

https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online

https://staysafeonline.org/stay-safe-online/