Tread Lightly Online: How to Check and Manage Your Digital Footprint

While you can't use the internet completely undetected, you can manage your digital footprint and protect your data privacy. Every click, post, and account sign-up leaves a trace online, along with almost everything else you do on the web. These small bits of information can be used to learn more about you than you realize, especially when added together. We call this your "digital footprint" – the trail of data you leave behind as you navigate the internet.

There isn't really a "leave no trace" way to use the internet these days – even if you use Incognito mode on your web browser, you will still need to have online accounts like email or shopping. You can still take control of your data, though. Managing your digital footprint helps to protect your data and boosts your cybersecurity.

The goal isn't to disappear from the internet entirely. But we can be intentional about what data we share and where. Just as you would be mindful with the personal information you'd share with a stranger, you can (and should!) be mindful about what info you share online.

1. Ask "Why?" before sharing

Every time a website or app asks you to share personal details or any data, take a moment. Ask yourself a few questions:

- Why is the service asking for this?
- Does the app or website really need this data to work?
- What do I get in return?

For example, your GPS app needs your location to give accurate real-time directions. But a store's coupon app doesn't need constant location access. Does your third-favorite social media platform need access to every photo on your phone? The less data you give, the less you expose.

2. Google yourself

Occasionally, search your name on major search engines to see what others can find about you online. If you regularly use AI platforms like ChatGPT or Google Gemini, it might also be worth checking out your name there, too. It can be surprising – and sometimes a little alarming.

Additionally, plug your email address into Have I Been Pwned to check if it's been involved in a data breach. If an account pops up:

- Change the password for the account immediately.
- If you've used the same password for other accounts, change them (and stop reusing passwords!)

3. Use a password manager to review your online accounts

A password manager helps you generate strong, unique passwords for every account, and we love them! They also provide other benefits, like displaying just how many accounts you've created over time.

Use your password manager to:

- Identify old or unused accounts.
- Delete accounts you don't need.
- Update weak or reused passwords.

4. Avoid creating unnecessary new accounts

Almost all websites these days push users to create accounts – even for one-time purchases. This is because your data is so valuable! But every new account increases your exposure to spam, trackers, and potential data breaches.

If you don't think you need an account when purchasing from a website, use guest checkout!

Fewer accounts mean a smaller digital footprint and less for you to manage and protect.

5. Adjust your privacy settings

Today, some accounts, like Google, Facebook, Apple, and Microsoft, are hard to avoid. However, you can limit how much data they collect.

- Review and adjust privacy settings regularly (we think once every three months is good).
- Limit what information is public, like who can see your social media posts.
- Restrict what data platforms can access, track, or store.

6. Know your privacy rights

Data privacy is a right, and in many places, you have legal rights when it comes to collecting and storing your data. Look into how the law impacts your privacy. Some examples include:

- California's CCPA enhances how Californians see and delete personal data companies collect.
- The E.U.'s GDPR offers strong privacy rights for people in Europe
- Stay informed about privacy! New laws could give you more power over your digital footprint.

7. Browse and post with care

The adage about an ounce of prevention being worth a pound of cure is still true in the digital age. It's easier to prevent privacy issues than to clean up after them. Here are a few habits to adopt:

- Use private or "Incognito" browsing to avoid saving history and cookies.
- Limit what you post on social media. Know that even private posts and DMs can leak.
- Don't post private, identifiable information like birth dates, travel plans, and addresses.

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.