DIGITAL ONLINE SECURITY BY JAOC

Why Do This?

Taking the time to manage your personal data is one of the most effective ways to protect yourself online. The benefits are significant, and the specific reasons may vary depending on your situation. Strong data hygiene helps reduce risks such as:

• Doxxing

"Doxxing" refers to someone gathering personal information about you—such as your home address, email accounts, or phone numbers—and releasing it publicly with the intention of causing harm. This can lead to coordinated harassment, both online and offline, and can escalate into serious safety concerns.

• Phishing and Spearphishing

Phishing attempts try to trick you into clicking a link, opening a file, or revealing login details so attackers can take control of your device, steal information, or monitor your activity. Some scams are broad and generic (fake parking fines, toll payments, job offers, or social-media purchases), while "spearphishing" targets specific individuals. Attackers often gather the details they need—addresses, family names, device types—simply by searching online.

• Stalking

The sheer amount of publicly available information today makes it far easier for someone to track down personal details such as addresses, phone numbers, or information about family members. Reducing your digital footprint helps limit these risks.

• Identity Theft and Fraud

The more information available about you, the easier it is for scammers to impersonate you. Details from social media—like the name of your first pet or your school mascot—can be used to guess security questions or forge documents. Minimising what's publicly accessible reduces these opportunities.

How to Protect Yourself

The best time to secure your information is **before** anything goes wrong. Once your data is in the hands of malicious actors, your options become limited. The goal is to make your information difficult to find in the first place. Here are practical steps to get started.

1. Establish a Strong Personal Security Baseline

Your broader privacy efforts won't be effective if your core accounts aren't secure. If someone gains access to your email or social media, they may obtain the very information you're trying to protect.

Start by strengthening your foundation:

- Use **unique, strong passwords** for every account (a password manager makes this easier).
- Enable **two-factor authentication (2FA)** wherever possible.
- Consider using a **tracker-blocking tool** to limit the data collected about your browsing habits.
- Remove or reset the **advertising ID** on your phone to reduce mobile tracking.

These steps reduce the amount of data available for purchase or profiling and help prevent companies from monetising your online activity.

2. Doxx Yourself

To understand what others can find about you, start by searching for yourself:

- Enter your name, nickname, username, handle, or avatar into a search engine.
- Search your address, phone number, and email addresses as well.
- Use a private browsing window or a separate browser to avoid personalised results.
- Use advanced search operators to uncover deeper or older information.

Tools like the **OSINT Framework** can help you explore usernames, email addresses, and social networks more thoroughly.

It’s normal to feel overwhelmed by what you discover. The important thing is that you’re now aware of it and can begin reducing your exposure. Make notes of anything sensitive or high-priority.

You can also do this exercise with trusted friends or family—others may spot things you’ve overlooked.

---

3. Minimise Your Publicly Available Data

You may find your information listed on “people search” websites that publish addresses, phone numbers, and other personal details. These sites gather data from:

- Public records
- Online trackers
- Commercial transactions

Data brokers compile this information into detailed profiles that can be purchased by anyone, including those with malicious intent.

You can request removal from these sites, but the process is often slow and must be repeated periodically because data is frequently repopulated.

Options include:

- **Manual removal** using opt-out instructions (such as journalist Yael Grauer’s data broker opt-out list).
- **Paid services** like EasyOptOuts or Optery, which automate the process. These services can help, but they require ongoing subscriptions and cannot guarantee full coverage.

A combined approach—handling the most sensitive entries yourself and using a service for the rest—works well for many people.

4. Audit Your Social Media Accounts

Create a list of every social media or forum account you've used. A password manager can help you identify old accounts you may have forgotten.

Then:

- Review each account's privacy settings.
- Decide who you want to be visible to.
- Consider making personal accounts private, especially those containing photos or family information.
- Keep professional accounts (like LinkedIn) public only if needed.

Many organisations publish helpful privacy checklists for major platforms to guide you through the settings.

---

5. Remove Yourself from Google Results

Google offers tools to help you monitor and manage what appears about you in search results:

- Use the **"Results about you"** feature to receive alerts when new personal information appears.
- Request removal of search results that display sensitive data such as your phone number or address.

Note: Removing a result from Google Search does **not** delete the information from the original website, and it may still appear on other search engines. However, reducing visibility on Google is still valuable given its widespread use.