9 Free Online Privacy and Security Tools Worth Considering

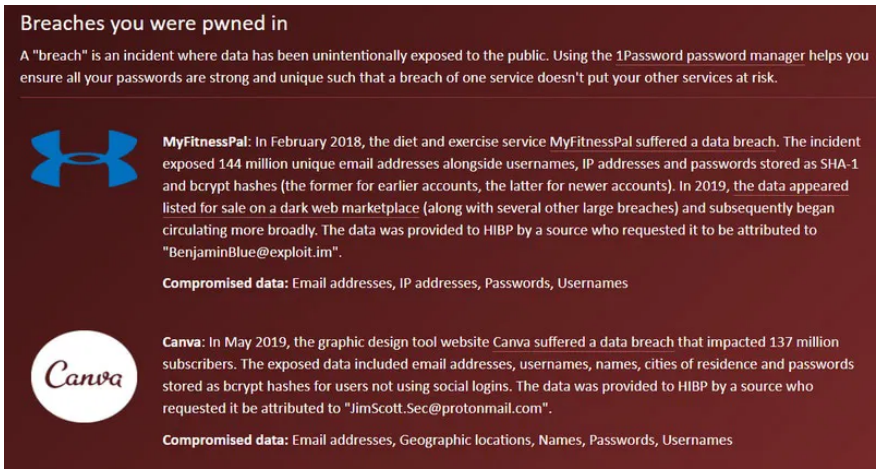
There are many online security tools that can provide on-demand security and enhanced privacy, no matter what device you're using.

There are many online security tools that can provide on-demand security and enhanced privacy, no matter what device you're using. Whether it's securing your device, online accounts, or browser, there's a tool designed for every need. This list includes the best online security and privacy tools for every purpose.

1. Have I Been Pwned?

Was your email or password exposed in a breach? Have I Been Pwned will check your email for data breaches, telling you the exact names of the companies that have suffered data breaches and what type of data was exposed. If your email has been exposed in a breach, you should change your password, beef up your email security, and maybe even switch to a secure email service.

Enter your email address in the search bar and click the **pwned?** button . If the email has been the subject of a data breach, it will show you how many breaches there have been and when they occurred. You can also click **Notify me** at the top and provide your email address to be alerted to future breaches.

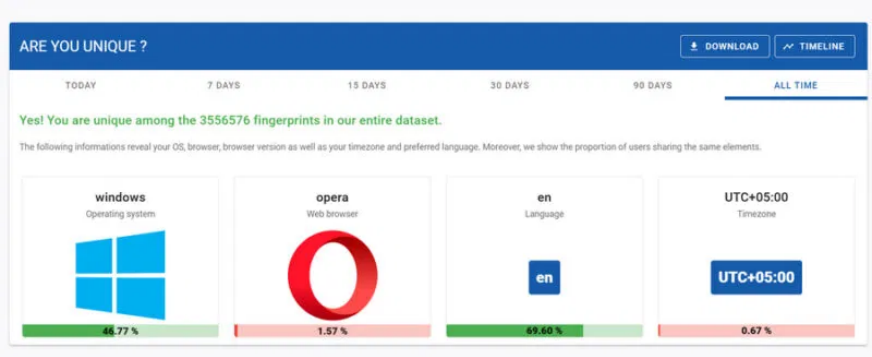


It also has a **Passwords** section where you can enter your passwords to see if they have been exposed in a breach. Don't worry, it uses k-anonymity to check passwords, so the full password is never revealed to the tool.

2. Am I Unique?

Browser Fingerprinting is a common but little-known online security tool that companies use to identify users and collect data. If your browser has unique characteristics, companies can identify you even if you hide information from them — like cookies . Am I Unique? scans your browser for 57 types of attributes to see if your characteristics are unique.

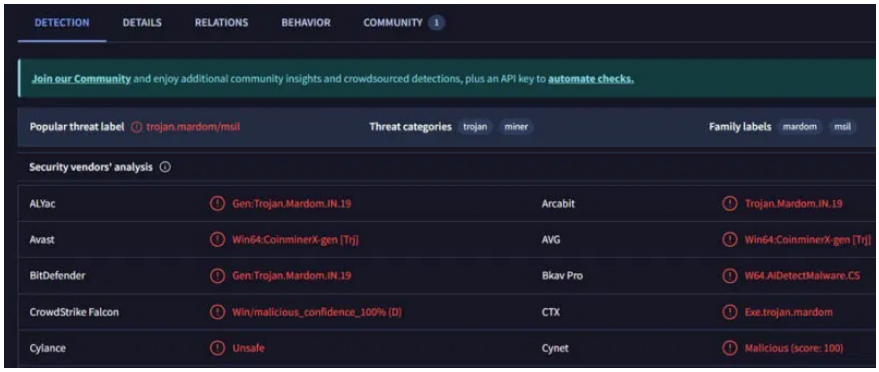
Select the **See My Fingerprint** button on the website and the tool will scan and tell you everything. At the top it shows the overall unique score for your browser fingerprinting and below it the results of all the individual attributes.



Uniqueness is distinguished by green, yellow, and red. If there are too many red properties, adjust those properties in the browser to reduce your own footprint.

3. VirusTotal

There's no need to risk running an infected file when you can simply check it with VirusTotal. This online security tool scans your files and URLs for malware and compares them to results from over 70 URL scanners and antivirus software. When you upload a file, it shows you the analysis from all the security vendors and how they classify the file.



It also includes a great community section where members can comment and share additional information about the file if available. Also, try Hybrid Analysis . It works similarly but has a dedicated sandbox tool that checks the file's behavior to detect malicious files instead of relying solely on AV scanning.

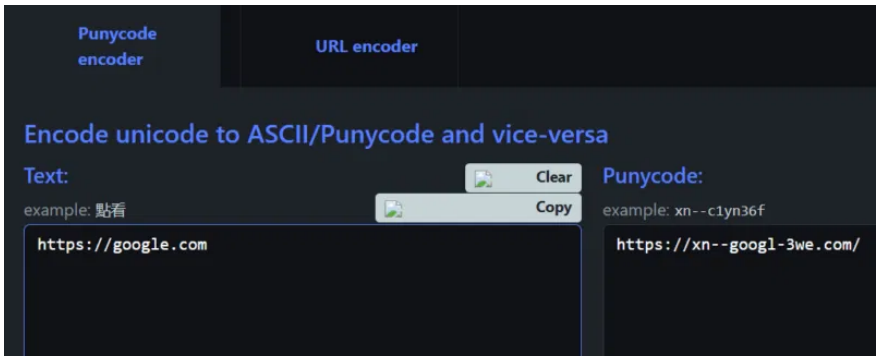
4. FaceCheck

In addition to being one of the better online security tools for detecting fake profiles, FaceCheck also helps detect identity theft and doxing attempts by finding photos that match your face. Provide a clear photo of your face and the tool will find publicly available photos that match your face.

The best matches will appear at the top with a score based on how likely they are to be a match. You will also see the name of the site where the photo was uploaded. If you find photos of yourself that you did not upload, it means someone is trying to steal your identity or upload your photos without your consent.

5. Punycoder

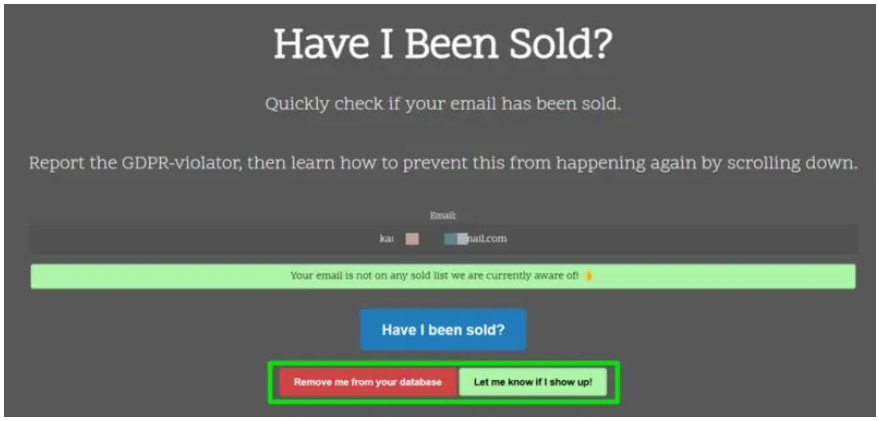
Homophone attacks are common, whether it's sophisticated phishing or account impersonation. Punycoder makes it easier to detect homophone attacks by converting letters from different scripts into Punycode.



If you think a valid URL or name is being spoofed with letters from different scripting languages, just enter it into the Punycoder's **Text** field . If the URL or name contains non-ASCII characters, the conversion command in the right panel will start with **xn--** .

6. Have I Been Sold

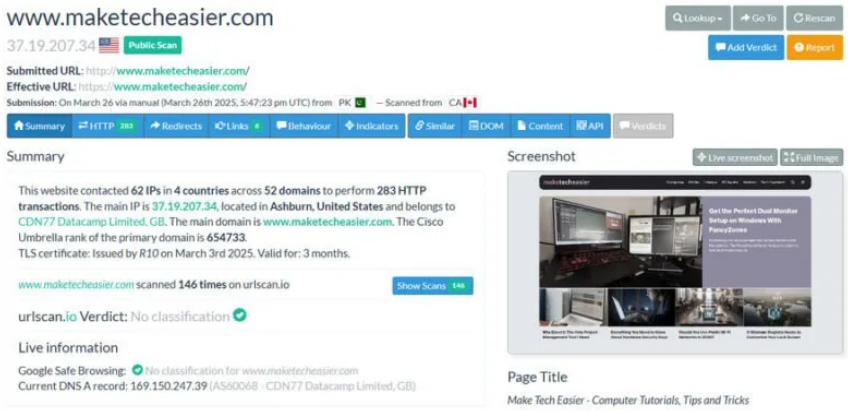
This online privacy tool is inspired by Have I Been Pwned but focuses on emails that have been sold. Have I Been Sold maintains detailed profiles of business email lists that are often sold B2B. Enter your email and it will show you if your email has been sold on any such lists.



Since selling emails without consent is a violation of GDPR, you can report the company that sold your email. The tool also allows you to set up notifications about future appearances on such lists. Click the **Let me know if I show Up!** button to opt in to these notifications. You can click the **Remove me from your database** button to turn off notifications.

7. URLScan

If you come across a shady link but still want to know where it leads, try URLScan. This online tool loads the website in a sandbox environment and provides detailed security information. The details it provides include a screenshot of the main page, contacted IP, contacted domain, main IP, technology used, direct links on the page, loaded JavaScript, cookie information, and more.



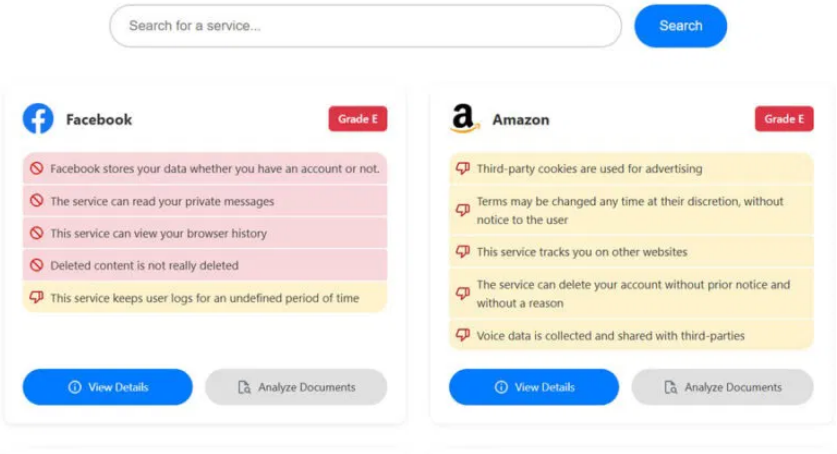
While all of this information has many uses, you can use it to determine whether a results page is safe. For example, screenshots will tell you what you'll see or whether links connect to the correct source.

The free version has some limitations – like 5,000 public scans per day – but it's enough for most users unless you scan too much.

8. ToS;DR

People often don't read the terms of service pages of websites and services before clicking agree because they are often long and complicated. ToS;DR makes it easy to understand what's inside a website's ToS pages by summarizing and categorizing them.

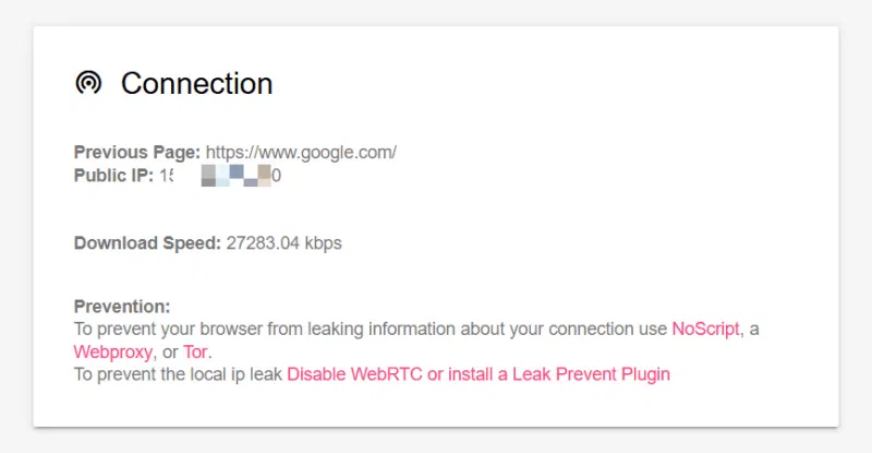
When you enter a website's URL, it will tell you how bad or invasive the site's terms of service page is. For larger sites like Facebook, Reddit, Amazon, CNN, etc., the tool will give you a score from A to E to rate how much the terms will affect you. In quick scores, the tool will tell you what the service can do with your account and information.



Even if it doesn't rank the site, it will still show summary points of that site's ToS page – or at least provide direct links to the ToS and other legal pages. You can click on each point to get a link to the terms written in the ToS.

9. Webkay

Webkay is one of the simpler online privacy tools. It shows you all the information that websites and services can see about you without your permission. Its main purpose is to show you how much of your information is revealed to the websites you connect to. The information includes your approximate location, operating system, browser name and version, browser plugins, hardware specifications, connection speed and IP, and gyroscope information.



For each piece of information, it also tells you exactly what you need to do to hide it, which mostly involves using the NoScript extension to block scripts. It also has additional features like scanning images for metadata and revealing details about your local network.

Keep these online security tools in your arsenal and check them regularly. You never know when a new threat will emerge or an inadvertent change will impact your setup. Just make sure you combine them with good security habits for maximum protection.