Use Apps and Software to Protect Your Data

Our data is constantly collected and shared, and we often don't even know all the types of data being gathered. Keeping your information private is a challenge, and in many cases, you might not have a choice. But there are tech tools now available that are in your corner. From private browsers to data removal tools and all-in-one privacy suites, these programs let you take back some control of your digital footprint.

Just a note: the NCA is a non-profit organization and we do not endorse products. We recommend checking out trusted review sources like PC Mag, Tom's Guide, Consumer Reports, and Wirecutter. We've listed some popular examples of each product type, but the NCA does not recommend any companies over the others.

PRIVATE BROWSERS

"Private browsers" are browsers that prioritize privacy by minimizing data collection and online tracking. Unlike the most common browsers, which store browsing history, cookies, and other data, private browsers are built to block these tracking mechanisms.

They may include features like default ad-blocking, protection against fingerprinting (a method of identifying users based on unique device traits), and minimal data retention. People often use private browsers to avoid targeted advertising, enhance online privacy, and reduce the amount of personal information companies collect.

These browsers are especially useful for those concerned about maintaining anonymity or protecting sensitive data online. Some popular privacy browsers include:

- Brave
- Opera
- DuckDuckGo

DATA REMOVAL SERVICES

Data brokers are companies that have a business model based around collecting, storing, and selling your data. Data removal services are a way to take on data brokers. These services are designed to help you protect their privacy by managing and reducing the amount of personal information available online.

These services search for data collected by data brokers, public databases, and other third-party entities, then request or facilitate its removal. They can also automate the opt-out process for data collection, making it easier for users to maintain control over their digital footprint.

People use data removal services to minimize risks like identity theft, targeted advertising, and online tracking, ensuring that their personal information remains private and secure. Some popular data removal services include:

- Permission Slip
- Optery
- DeleteMe

PRIVACY EMAILS

Your email inbox is a treasure trove of data. In fact, many popular email clients use anonymized data from your inbox to target ads to you. Consider switching to a private email provider, which prioritizes your privacy and security.

These email clients offer strong protection compared to mainstream email platforms. A quality privacy email uses end-to-end encryption, ensuring that only the sender and recipient can read the contents of emails, even if intercepted. They also avoid scanning emails for advertising purposes and limit data collection.

Additional features might include allowing to sign up for newsletters anonymously, encrypted storage, and data minimization practices. Opt for a private email provider to safeguard sensitive communication, maintain privacy, and take greater control over your personal information. Some popular privacy email clients include:

- ProtonMail
- StartMail
- Mailbox.org
- Tuta

VPNS

Each of your devices has an IP address, a string of characters that identifies where you go on the web. Virtual private networks (VPNs) are a tool to protect your sensitive data better and maintain anonymity. A VPN prevents your internet service provider (i.e., the company that sells you internet access) from tracking your specific journey on the internet, although they can still gather some data, like the fact that you're connected to a VPN. Using a VPN is great from a privacy perspective because ISPs have a history of selling your data to others.

Fortunately, most of the websites you use are probably encrypted -- you can tell because the web address uses an HTTPS connection as its first four letters. But a VPN is still useful if you ever connect to a public Wi-Fi network, but you must still be careful.

Always do your research regarding VPNs – a shady VPN is worse than no VPN at all. Some popular options include:

- ExpressVPN
- NordVPN
- Mullvad
- ProtonVPN
- SurfShark

COMPREHENSIVE DATA PRIVACY SERVICES

Though a bit expensive, privacy protection suites are all-in-one tools that offer comprehensive digital security and privacy management. These services combine multiple features, including identity theft protection, antivirus software, data breach monitoring, password management, and VPNs. These services usually charge a monthly or annual fee.

Data privacy suites aim to provide users with a convenient, comprehensive solution for protecting personal information. Privacy protection suites are popular with people who want a more robust defense against online tracking and identity theft. These services allow you to stay vigilant about their privacy without needing multiple separate tools.

Because of the investment, you want to make sure to research multiple options before selecting a suite. Some popular offerings include:

- Norton LifeLock
- Aura
- IdentityForce

USE TECH TO STAY PRIVATE

We firmly believe that protecting your personal data is essential. More and more, there are a variety of tools available to help you take control of your privacy. Whether you're looking to browse anonymously, secure your communications, or remove your information from data brokers, these solutions are a massive help. You can actually use technology to reduce your digital footprint. With the right tools and a proactive attitude, you can take your privacy into your own hands.