How to Improve Your Data Privacy

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/how-to-improve-your-data-privacy/

By Vipin PG | Published July 19, 2025 | Updated January 4, 2026 | Format: Guide | 5 min read

Quick answer

In the modern era, billions of people around the world rely on an Internet connection. We might connect in order to work, or to shop, or to play.

In the modern era, billions of people around the world rely on an Internet connection. We might connect in order to work, or to shop, or to play. The opportunities thrown up by the technology are considerable, but there are risks associated with spending time online, too.

Not least of these risks is the possibility that valuable data might be compromised. For this reason, everyone who deals with the internet should learn about the various data-protection measures available.

Use Strong, Unique Passwords for Every Account

When you use a weak password that can be easily guessed, you make it easy for a malicious actor to gain access to the account associated with that password. If you have many accounts that share the same password, then the hacker only has to guess it once.

The modern era provides a fantastic antidote to this problem: the password manager. This is a piece of software that will generate secure passwords on your behalf. All you need to remember is the password for the manager itself, which can be secured using multi-factor authentication.

This approach not only improves your digital hygiene but also saves time and reduces mental clutter. With the rise in password breaches and credential stuffing attacks, password managers are now considered essential tools, even for everyday users. Applications like Bitwarden, 1Password, and Dashlane offer free and premium versions to help users store hundreds of unique, complex passwords safely. Multi-factor authentication (MFA), such as OTPs sent to your mobile device or biometric verification, adds an extra layer of protection in case your master password is ever compromised.

Adjust Privacy Settings on Apps and Devices

Many modern applications collect more data than their users realize. In many cases, there are privacy options available which allow users to control the way that their data is collected and used. However, if the organization behind the application is opaque, then you might not feel justified in trusting it. You might look for open-source alternatives, whose code can be scrutinized by an online community. Or, you might abandon your use of the app or platform altogether.

To strengthen your digital privacy, it’s important to take time to manually review the permissions that apps request. For example, if a flashlight app wants access to your location or contact list, that’s a red flag. On both iOS and Android devices, you can usually disable unnecessary permissions such as microphone, camera, and location access. Web browsers like Firefox and Brave also allow you to disable third-party cookies and fingerprinting trackers, making it harder for advertisers and data brokers to follow your online behavior.

Furthermore, some operating systems now offer built-in privacy dashboards where users can see which apps have accessed sensitive information and revoke access if needed. Making this a regular habit, just like updating your software, will go a long way in keeping your data private.

Store Your Data, Photos, and Backups in a Safe Place

If you have lots of data that you'd like to keep secure, then the best option might be a remote server. This will allow you to avoid the cost and inconvenience of a physical storage drive. You'll be able to access your personal photos and work-related assets from wherever you are in the world, and backup regularly to prevent data loss.

Free cloud storage is widely available from a number of specialist providers. Consider your options!

Some of the most popular services include Google Drive, Dropbox, OneDrive, and iCloud, each of which offers a limited amount of free storage and premium plans for more extensive needs. When choosing a provider, pay attention to encryption protocols and data handling policies. End-to-end encryption ensures that even the service provider cannot view your data.

However, while cloud storage is convenient, it's wise not to rely solely on it. A good backup strategy follows the 3-2-1 rule: keep three copies of your data, on two different media types, with one copy stored offsite. For example, use an external hard drive for local backups and a cloud provider for offsite redundancy. Tools like Synology NAS or Time Machine for Mac users make automated backups effortless.

Be Aware of Phishing Scams and Public Wi-Fi Risks

Sometimes, it's user error that creates a security vulnerability. You might put your trust in an email or direct message you've received, or click on the wrong kind of link. Be extra cautious when inputting your personal data into a web form, especially if you haven't navigated to the page in question yourself.

If you're using public Wi-Fi, then you might benefit from the use of a Virtual Private Network. This is an intermediary that will encrypt all of your activity, meaning that your data can't be intercepted by a malicious actor on the same network.

Phishing scams are becoming more sophisticated, often mimicking well-known brands and using social engineering techniques to lure users into revealing sensitive information. Always double-check the sender's email address, avoid clicking suspicious links, and never download attachments from unknown sources. Many modern email clients, such as Gmail and Outlook, have built-in phishing detection, but it's ultimately up to the user to stay alert.

When it comes to public Wi-Fi, treat all networks-whether at a cafØ, airport, or hotel-as untrusted. Avoid logging into sensitive accounts like banking or email unless you're connected through a VPN. Modern VPN services like ProtonVPN, Mullvad, or NordVPN not only protect your traffic but can also mask your IP address, making your online activity more private.

Additional Tips to Stay Safe Online

In addition to the steps above, here are a few more practices to adopt for robust digital security:

- Update software regularly: Outdated apps and operating systems are more vulnerable to attacks. Always install the latest updates, which often include security patches.
- Use antivirus and anti-malware tools: Reliable security software can detect and block threats before they do damage. Make sure your definitions are updated.

- Avoid oversharing on social media: Sharing too much personal information, such as birthdays, locations, or travel plans, can make you a target for identity theft or physical threats.
- Enable account recovery options: Set up backup email addresses, security questions, and phone numbers for account recovery in case you lose access.

Conclusion

By following these data protection measures, individuals can dramatically reduce their risk of falling victim to cyber threats. While the internet offers vast opportunities for learning, work, and entertainment, it also demands a proactive approach to privacy and security. In today's digital age, safeguarding your personal data isn't just smart-it's essential.

References

1. staysafeonline.org - articles / best-practices-for-security-and-privacy-settings - https://www.staysafeonline.org/articles/best-practices-for-security-and-privacy-settings
2. proton.me - drive - https://proton.me/drive
3. techradar.com - vpn / us-vpn-usa - https://www.techradar.com/vpn/us-vpn-usa