INTERNXT

Take Control of Your Online Privacy:

A Guide to a More Private Online Experience, For Everyone

Table of contents

Introduction

Welcome to Take Control of Your Online Privacy: A Guide to a More Private Online Experience, a comprehensive ebook designed to help you take control of your privacy.

By downloading this book, you are on your way to a more secure, private internet experience. We will discover the potential risks to your data or sensitive information when browsing the internet, signing in to online accounts, or using your email.

We will also offer expert tips and strategies on how to avoid data hacks, stolen passwords, privacy-focused tools, and applications to help you transition to a digital lifestyle centered around online privacy.

If you are ready to start your journey towards online privacy and identify, protect, and remove your private information from exploitative websites, then let's get started.

Learn more about cybersecurity, online privacy, and tech basics at our blog.

Why is online privacy important?

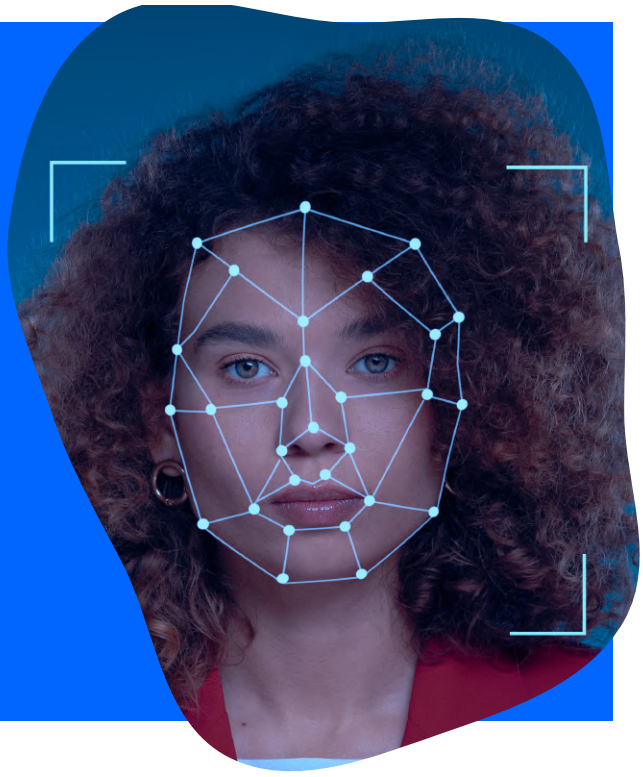
Online privacy is important because it limits the power you give to external parties, governments, companies, your social media following, or hackers and protects you and your data from being misused, sold, manipulated, or exposed without your consent.

Companies invade your privacy for their benefit

As companies grow and become more efficient, they capitalize and double down on actions that have helped them achieve huge profits. It is this corporate greed for growth that has led to the internet's current thirst for customer data to outshine the competition.

For example, the data that companies collect include, but are not limited to:

- Birthdates
- Browsing history
- Email
- Location
- User behaviour
- Cookies and website tracking



One such example of a company using collecting and selling your data is Google.

Google: a nightmare for online privacy

It's almost impossible to talk about online privacy without dealing with Google's collection of personal data. Google continues to be the subject of many privacy violations, and rather than change its ways, it would rather pay fines of $391 million and continue on its way.

It's no secret that Google collects personal information and tracks its users through Chrome, Google Search, Google Play apps, Google Maps, YouTube, and more. Prevent Google from accessing your data by adjusting your Google controls and settings.

When you search on Google, they collect all the following data:

- Personal information: Your name, phone number, gender, date of birth
- Your email addresses
- Where you live
- Where you work
- Your interests
- Things you search for
- Websites you visit
- Videos you watch
- Ads you click on or tap
- Your location
- Places you've visited around the world
- Device information
- IP address and cookie data
- Your YouTube search history and recently watched videos
- What you've said to the Google Assistant, including via smart speakers

For an in-depth guide on adjusting your privacy settings in Google, check our What Google Knows resource dedicated to users who want to use Google without compromising their privacy.

Why do Google and other companies collect your data?

In short, it's a form of exploitation. Google's motivation is to target ads and 'personalize' your experience with their services.

By surrendering your data, you enable hundreds of thousands of advertisers to bid on your information and deliver targeted advertisements based on your sensitive personal data, all through Google's data collection efforts.

Everyone involved benefits from your information except for you. You are the product.

Keep your data safe with privacy-focused browsers

Your internet browser is the interface you use to access the internet. As such, it knows and handles a lot of your data. Unfortunately, this makes web browsers the perfect data collection tools for advertisers and marketers.

Here are some alternative browsers to Chrome that you can switch to for a more private browsing experience.

Brave

Supported platforms: Windows, macOS, Linux, Android, iOS.

Brave is on the **open-source*** Chromium web core and proprietary code. It is free to use. However, you'll have to pay for added features such as Brave's Firewall and Virtual Private Network, (**VPN***), powered by Guardian (which currently supports only Android and iOS).

Brave supports almost 160 languages for global use. Brave Shield blocks privacy-invasive ads, cookies, scripts, browser fingerprinting, and trackers and disallows third-party data storage. As such, you enjoy faster speeds. Brave claims their pages load three to six times faster than Chrome and Firefox.

Mozilla Firefox

Supported platforms: Windows, macOS, Linux, Android, iOS.

Mozilla Firefox is a privacy-centric browser, as reflected in their Personal Data Promise - Take less. Keep it safe. No secrets. Your online activities and data are yours alone to know, not others.

Firefox blocks third-party tracking cookies, autoplay, ad trackers, and social trackers, among others. The Enhanced Tracking Protection (ETP) stops third-party trackers from collecting and selling your information.

While they store some data on you, it is minimal, and they do so for your benefit. However, some of you may feel uncomfortable knowing this. Not to worry, though, it's not the only option you have available.

Tor Browser

Supported platforms: Windows, macOS, Linux, Android.

Another open-source tool, Tor Browser is known to be a genuinely anonymous browser. Tor has earned 'the onion router' due to wrapping your information in multiple layers of encryption like an onion.

Tor Browser emphasizes protecting you against tracking, surveillance, and censorship. Your communications route via multiple servers (owned by unknown volunteers) when you connect to the Tor network. Traffic is encrypted and sent through these entries, transit, and exit nodes (servers) until it reaches its destination.

Hence, Tor Browser affords a high degree of anonymity for users. The Tor browser means business, as it also blocks browser plugins such as Flash, RealPlayer, QuickTime, and others (these have vulnerabilities that can reveal your **IP address***).

Vivaldi

Supported platforms: Windows, macOS, Linux, Android.

Vivaldi claims not to track or profile you and does not collect your information and sell it to third parties. Vivaldi comes with a built-in ad blocker that you can use to block intrusive ads. Also, Vivaldi does not store cookies or temporary files, helping to increase page loading speeds.

Vivaldi does not encourage using third-party apps and extensions due to possible additional vulnerabilities. Instead, they enable you to use their secure built-in apps that don't take up too much of your resources, e.g. (mail client, translator, ad blocker, pop-up blocker, private calendar, and more).

The Vivaldi browser makes it hard for websites to fingerprint you, meaning your data is kept private.

Iridium

Supported platforms: Windows, macOS, OpenSUSE, Fedora, RHEL / CentOS.

Another open-source tool, Tor Browser is known to be a genuinely anonymous browser. Tor has earned 'the onion router' due to wrapping your information in multiple layers of encryption like an onion.

Tor Browser emphasizes protecting you against tracking, surveillance, and censorship. Your communications route via multiple servers (owned by unknown volunteers) when you connect to the Tor network. Traffic is encrypted and sent through these entries, transit, and exit nodes (servers) until it reaches its destination.

Hence, Tor Browser affords a high degree of anonymity for users. The Tor browser means business, as it also blocks browser plugins such as Flash, RealPlayer, QuickTime, and others (these have vulnerabilities that can reveal your **IP address***).

Apps and services for increased privacy

People use various apps and services to conveniently chat, collaborate and organize with others. However, there are growing concerns about data privacy for at least 8 in 10 adult consumers worldwide.

These people are more likely to be the target of online scams or privacy breaches because companies, such as Google, sell their data to third parties. That being said, here are the most popular apps and services you can switch to today to increase your online privacy.

Alternative to “Googling”

Google holds a commanding position in the search engine industry, with an average market share of 86-96% worldwide. However, more privacy alternatives are available when searching the web.

DuckDuckGo has earned significant popularity as a privacy-oriented search engine because it saves your search history in a non-identifiable manner. It doesn’t store tracking cookies and personal identifiers like IP addresses, nor does it share personal information with third parties, ensuring a more private browsing experience.

Alternative to Google Maps

If you want to travel around the world and explore new areas without Google joining you for the ride, OSMAnd is an open-source map and navigation app.

One of OsmAnd’s key features is its ability to function entirely offline. It has voice guidance, traffic warnings, re-routing options, and more. Additionally, it includes footpaths, hiking trails, and biking paths, catering to the needs of outdoor enthusiasts.

Alternative to Gmail

As email is one of the most widely used forms of communication on the internet, a secure email provider is essential. If you already have a Gmail account and don't fancy migrating the hassle of changing platforms, at the very least, you should implement some Gmail account security tips.

Aside from that, if you are interested in a website's service but don't want to sign up with your actual email and be bombarded with spam, a temporary email is a great solution to avoid giving a company your personal information.

Finally, if you are looking for an encrypted email provider, some encrypted email companies people use include:

StartMail: A privacy-focused email service allowing users to create different, anonymous email aliases.

Tuta: An encrypted, open-source email provider that offers 2FA, custom domains, login protection, and more features in the future.

Mailfence: A secure, affordable, and encrypted email provider that uses digital signatures to guarantee you are exchanging information with the right party.

For the complete list, check our blog post for more alternative email providers.

Alternative to YouTube

YouTube may dominate the video hosting world, but Vimeo is an alternative for people looking to move away from Google's products, with a popular option being Vimeo.

Vimeo differs from YouTube by adopting a more stringent approach regarding its privacy policy and data security. While Vimeo does collect specific data, it refrains from sharing it with third parties. Users can control their content's privacy settings on the platform.

Alternative to Google Drive

Finally, any information you create, share, or store online necessitates a secure storage platform, and the most common and popular way is via cloud storage.

Internxt offers an alternative to Google or other cloud storage providers because of our vision for a more secure, private internet.

Internxt implements end-to-end encryption* and zero-knowledge policies* to keep your files safe at rest and in transit, ensuring that you are the only one who controls who has access to your files; not even Internxt can see your files, passwords, or personal information.

There are also many additional features to enjoy with Internxt, such as Drive, Photos, and Send, to suit your needs. It also boasts a simple and user-friendly interface and affordable monthly, annual, and lifetime plans.

Easing the transition to online privacy

Embarking on the journey of online privacy life involves several key steps, and the time it takes may differ depending on your current apps and usage. Begin by assessing how Google tracks you and choose how you would like to reduce Google usage by identifying areas where you heavily rely on their services.

Once you have a clear picture, you can choose from any alternative services that align with your needs and privacy preferences to gradually reduce your reliance on Google while enhancing your privacy and data security.

Extra Methods to Achieve Online Privacy

Achieving online privacy requires many different practices, and while switching from Google entirely is a valid choice, it is easier said than done for many people. With that in mind, here are some other tips for increasing your online privacy.

Social media privacy settings

Log into your social media accounts and check your privacy restrictions. You need complete control over what you share publicly and who can see this information, so it's best to turn your accounts private or select the individuals you wish to share the information.

Choose platforms with encryption

You should only use messaging, data-sharing apps, or cloud storage providers using with end-to-end encryption. This way, if a third party gains access to the data, it will be unreadable.

Secure your passwords

Reusing passwords across multiple accounts or using weak passwords is one of the major causes of data breaches. Once a password is stolen, it can lead to identity theft or your information being sold on the dark web, leading to more attacks of online fraud or financial crimes.

Each password you use for your different accounts should be:

- **Long:** minimum 10 characters.
- **Unique:** only used for one account.
- C**omplex:** a mixture of random symbols, e.g. (·%*^_ª=).

A way to secure your passwords and accounts is a combination of a password generator and a password manager from a reputable company.

Regularly update your software

Updates for your software remove vulnerabilities that were present in older versions. Regular updates are particularly important because they not only fix known vulnerabilities but also help prevent new ones from emerging.

When software vendors discover and patch vulnerabilities, they strengthen your defense against potential **zero-day vulnerabilities***. Nowadays, most operating systems enable automatic updates to help secure your devices. Check your settings regularly for when a new update is scheduled and back up your files accordingly.

Additionally, regularly updated software may also include new functions and design features that improve the stability and overall experience, so it's a win win situation!

More privacy resources

Check out these free resources to help you manage your cloud storage, secure your accounts, and keep your information secure and private on the web.

Byte Converter

Find out how many GB in a TB or how much cloud, phone, or drive storage you really have left with Internxt's free Byte Converter.

Temporary Email

Receive emails anonymously with our free, private, and secure temporary email address generator.

Password Checker

Find out how secure your passwords are for your accounts with our password checker.

File Virus Scanner

Scan any document, image, PDF, or other file types to detect malware or other dangerous files.

Password Generator

Instantly generates highly secure passwords.

Glossary

Understanding these key terms will help you protect yourself and your children online.

Open source

Open-source software is software built with the source code made freely available to the public. The source code can be inspected, modified, and fixed by professionals to reduce security vulnerabilities. Internxt's source code can be viewed on GitHub.

VPN

Stands for Virtual Private Network, a technology that allows users to create a secure and private connection by encrypting your connection over the internet, making it difficult for others to access or view your data.

IP Address

An internet protocol address is a unique numerical label assigned to each device connected to a computer network. People often use a VPN or browser to change their IP and hide their geographical location.

RSA Encryption Key

An RSA (Rivest-Shamir-Adleman) key is part of a cryptographic system that keeps data safe. A public key locks (encrypts) the data, and the private key unlocks (decrypts) it. An RSA encryption key is a widely used system for secure communication and transactions over the Internet.

End-to-end encryption

End-to-end encryption encrypts data on a sender's system or device, securing it during transmission, such as messaging. Only the intended recipient can decrypt the data, keeping the information private from the service provider.

Zero-knowledge policies

A company with a zero-knowledge policy does not have access to any user data or encryption keys - giving the user complete control over who can access or view their information.

Zero-Day vulnerability

A zero-day vulnerability is a security flaw in software or hardware that's unknown to the vendor or developer. The name "zero-day" is because there are zero days of protection once the security flaw is discovered.

INTERNXT

Stand for privacy, switch to Internxt

Try Internxt for free