**How to protect your privacy online?**

We are living in an age where maintaining online privacy is an everyday challenge. As you type, browse and talk online every day, your activity is constantly monitored, analyzed and even sold to companies for commercial purposes. No matter how safe you think your information is, as you fill out forms or make online purchases, your name, education, address, employment, hobbies, and even financial data is used by marketing companies and data brokers to get financial gains. Mass surveillance is now a reality, and has never been easier as it is today. What’s even worse, considering the [data privacy laws](https://dataprotection.blog/data-protection-and-privacy-laws-across-the-world/), we are forced to allow access to our private information before using applications, because we are given no other choice but to trade-off between digital convenience of enjoying benefits of online world and privacy. However, it’s still not impossible to protect your online privacy, as with easy surveillance, it has also become easier to apply end-to-end encryption, stay aware and take small actions that can actually make a big impact.

By taking some basic steps and changing the way you interact online, it is possible to take back control of your online privacy. You don’t need to be tech-savvy or invest a lot either. Rather, a little time and effort along with abundantly available free tools can get you started.

Here are some important actions that can help you protect your privacy online.

**Use End-to-End Encryption Applications for Secure Messaging**

Use messaging apps that provide end-to-end encryption to stay safe from prying eyes. Examples include WhatsApp, Signal and Telegram.

In many email communications as well, messages are still transmitted without encryption in cleartext. This makes it very easy for an outsider to eavesdrop on your email messages. Gmail and Outlook provide encryption, but only if both sender and receiver are using their service. Look for other alternatives that provide encryption regardless of the service being used by the other party.

Also turn on encryption on other services and devices, as some of them offer encryption but don’t have it enabled by default. Always manually turn on encryption on all such devices.

**Use Strong Passwords and Protect Accounts with a Password Manager**

This may seem like a basic security measure, but is often overlooked and underestimated. Weak passwords are one of the common reasons of security breaches. Never use default passwords, easy-to-guess passwords or those related to your personal information. If someone is able to guess your password, they can instantly access all your data. It is also recommended to keep different passwords for all accounts so if one account gets compromised, others remain safe.

However, with so many accounts and so many passwords to juggle, it gets very hard to remember them all. The best way to manage your passwords is by using a password manager which makes it easy to generate strong passwords, track them and retrieve them when required – all at one place.

**Use VPNs over Public WiFis**

Always use a Virtual Private Network (VPN) when connecting to an unprotected or public WiFi network. Public WiFi networks at airports, coffee shops or other places that offer free WiFi can be used for identity thefts. Most of the online traffic over public WiFis is transmitted in plain text which makes it easy for cyber criminals to intercept your browsing activity and get all details. In some instances, hackers deliberately set up fake public access points to install malware on all connected devices.

A VPN protects your private information by sending it over the network in encrypted form with the help of a virtual tunnel which makes it almost impossible for hackers to track your activity based on IP address.

**Keep Your Systems and Applications Updated**

Every other day, security vulnerabilities are discovered in applications and patched with new updates. It is always advised to regularly update your devices, applications and services to secure yourself from the threats of previously discovered vulnerabilities.

**Use an Ad Blocker to Block Ads and Trackers**

Though it may seem like adware only brings personalized ads to you, it mostly tracks you over the web, collects your location data and browser history to refine your digital profile. There are chances that there are countless trackers that follow your online activity. However, there are many free tools available for blocking such intrusive ads. Ad blockers also come with the added advantage of decreasing battery usage and speeding page load time.

**Use Private Search Engine to Search the Web Anonymously**

Though Google owns the largest share of the search market, it is notorious for tracking user search activity for targeted advertising that majorly contributes to its business. However, the good news is that there are many private search engines available that keep privacy as a priority. DuckDuckGo and SearchEncrypt are two such examples. These search engines encrypt your search using the Secure Sockets Layer and expire your search results after some time. They also offer extensions for well-known browsers.

**Turn on Two-Factor Authentication (2FA)**

Two factor authentication adds an extra layer of privacy over the usual password protection such as in [banks](https://www.endpointprotector.com/blog/5-ways-banks-secure-data/) that use key fobs to ensure a [secure payment system](Link%20to:%20http:/www.cardzgroup.com/BankCards.html). In 2FA, even after entering the password, you are required to enter another detail such as a code sent to you via email or SMS, or a google authenticator key.

**Update your Social Media Privacy Settings**

We share our everyday lives on social media which makes us more susceptible to privacy invasion. It’s important to regularly review and update your privacy settings on all social media accounts and ensure that only people added with you on your social networks can see your regular updates. Always review your sharing settings, remove your connected apps, delete location history and control who can see your information.

**Be Cautious of Smart Devices**

Smart devices have brought a new meaning to the digital era with their convenience and value. But they also pose serious threats to your online privacy and security. Never install suspicious apps seeking information access permission in your [smartphones](https://darkcubed.com/blog/2020/6/10/smartphone-security-tips). Also, for IoT devices, most of them do not come with software updates and are highly vulnerable to a large number of attacks. This is why cybercriminals find them easy targets to fetch personal information of users or to invade their privacy. Almost all kinds of gadget and electronic device now comes with internet connectivity including televisions, thermostats, security cameras and more; with rarely any patches available. To avoid being a victim of privacy invasion through a smart device, never connect cheap, random device to your WiFi networks. If you really need to, set up a guest account over your WiFi for such devices; use WPA2 encryption, change default passwords and update router regularly. Also consider turning off the devices that are always listening, such as Google Home Assistant or Alexa, when not in use.

**Protect your Identity when doing Financial Transactions**

When using your credit or debit cards online during a transaction, never save your financial details. You may be prompted to do so and while it may save you the trouble of entering your details next time, saving details is not a good idea due to security reasons. If you find out that your card details have been compromised, freeze it at once. Freezing your payment cards prevents cybercriminals from opening new accounts in your name.

**Conclusion**

With all these security measures in place, the best way to maintain and protect your privacy online is to stay vigilant and on the lookout for malicious activity. Never click on suspicious links and watch out for potential scams. Do not share your personal information with anyone that you don’t recognize personally. Only a little knowledge and the right attitude can go a long way in helping you protect your privacy online.