

INTERNET PRIVACY

Published on: June 24th,2020

Submitted By : Avanish Anand

Internet privacy is defined as the security level and privacy of personal data published via the Internet. It is also commonly referred to as online privacy. Internet privacy comes under the laws of data privacy and thus, is a fundamental human right. In simpler words, internet privacy is the protection consumers are entitled to when they are involved uploading, downloading and storage of their data through online mode. The idea of internet privacy is vast, and employs various technologies, factors and techniques to safeguard sensitive data and private communication and preferences over the internet.

Although the risks posed to the users are vast, mentioned below are some the of common internet privacy risks :

1. Malware – A malware is an application which illegally damages online and offline computer data using various viruses and Trojans.
2. Phishing – Phishing is an online hacking activity used for secure user data theft, which includes username, password, bank account number, credit card details etc.
3. Pharming – Pharming involves use of illegal hacking procedure to redirect an online website visitor (user/consumer) to a different IP address.
4. Spyware – Spyware is an application which works offline to obtain data without a user's consent. As soon as the system goes back online, the previously illegally acquired data is sent to source of the spyware.

With knowledge of the common ways the consumers may be duped online, it's also a necessity to acquaint oneself of the various steps we can take to prevent that from happening, some of which are as follows :

1. Don't use public storages for personal data : While many of us do tend to overshare on social media, it's not limited upto there. We must refrain from sharing or storing private data on online services that are not meant for the same. An example of such would be to use Google Docs or any cloud based service for the storage of personal passwords.
2. Using messaging apps that employ end to end encryption : Most of the commonly used messaging apps do employ encryption, but for namesakes, i.e., encryption in transit, in which the messages we send are decrypted at the provider's base, and stored on their servers, hence defeating the purpose of privacy. Contrary to this, an end to end encryption (used in WhatsApp Messenger among the popular messaging apps) does not store the data anywhere and the sender and the receiver are the only two parties involved.
3. Using secure passwords : This one might seem like a piece of cake, but this also is where most of the users falter. We should prefer using long passwords everywhere, generally containing more than 12 digits or characters or a combination of both. We should also use separate passwords for separate services.
4. Staying private on Wi-Fi networks – The majority if us rush to establish a connection when we see a free public Wi-Fi in order to save some of our paid data charges, but these are very risky. Public Wi-Fi networks are known not the encrypt traffic, which means that anyone connected on the same network may use it to illegally access your sensitive data. We must avoid transmitting any such sensitive data such as credit card data, logins, passwords etc. on a public Wi-Fi. Using a paid VPN service is also a good measure to protect our information from prying eyes.

[All Articles](#)

[Home](#)[article](#)[events](#)[supcoming](#)[about](#)[join](#)

Navigated to INTERNET PRIVACY