ULTIMATE PRIVACY GUIDE 2019

POWERED BY BESTVPN.CO

Introduction 2
Privacy Threats 3
Privacy Tools 11
Tools for Securing Your Online Payments 12
Secure Search Engines That Don't Track 16
Email Encryption Tools 17
Tools to Secure VoIP Conversations 18
Tools for Securing Instant Messages 18
Data Encryption 19
Protocols 23
Which Protocol (and Encryption) Should You Use? 24
How to Secure Your Browsing 25
How to Secure Your E-Mails 28
How to Secure Your Conversations 32
How to Secure Your Cloud Storage 34
Countries That Violate Your Privacy 39
Enhance The Use Of Antivirus, Firewall and Anti-Malware 43
Tips and Tricks For Online Privacy 46
How to Generate Strong Passwords 54

Introduction

When it comes to surfing the internet, browsing an online store, updating a status or sharing something on social media, and making online financial transactions, we all have one basic human right and that is of internet privacy.

The small bits of information that zoom across the internet are like pieces to a puzzle, which can reveal a wealth of information about anyone when put together. This personal information can be very damaging if compiled together and used for specific purposes.

Thanks to the revelations unveiled by Edward Snowden about the NSA's and the government's surveillance on citizens, this right to privacy is being violated. To make matters worse, there are numerous countries around the world that conduct unwanted surveillance on their citizens and monitor all their internet/phone activities.

Many of these countries have introduced legal regulations and legislation that require telecom companies and internet service providers to record their users' metadata. What this means is that every time you visit a website; make a purchase online; send/receive an email; make a phone call (over VoIP); or send a text message; all these activities are recorded and used by the government for surveillance purposes.

This is where you need to understand the numerous threats that are present over the web; how they can affect your privacy; the tools and software that are available for defending against each of these threats; and how you can use them to protect your privacy and become anonymous.

Privacy Threats

Desktop & Laptop Threats

Mac and Windows users need to be worried about certain desktop threats that originate from the internet and can breach your privacy. Here are some of the most common threats you can expect to encounter as a Mac/Windows user:

- **Botnets:** they are a collection of software 'bots', remotely controlled by their creator and built to infect your computer with malicious entities (virus, malware, etc.).
- **Hacking:** this is the process through which cyber criminals break into your system and gain unauthorized access to your personal data.
- **Malware:** it is malicious software that infiltrates your system and damages your computer. Malware can also contain viruses, Trojans, adware, etc.
- **Phishing:** Phishing is a process through which cybercriminals try to retrieve personal and financial information about users. They use fake emails, websites, text messages, and other methods to gain personal and exploitable information about you.
- **Pharming:** when you are redirected to illegal and malicious websites, this process is known as pharming. Cyber-goons use this process to commit fraud and obtain personal information about users.
- **Spam:** it is the mass distribution of commercials, emails, messages, advertisements, pornographic material, and other unwanted content, to unsuspecting users. Spammers usually obtain email addresses of targeted users from blogs, websites, and social media profiles.
- **Spoofing:** this technique is used by cybercriminals, usually in combination with phishing, to steal your personal information. These criminals use websites or email addresses to obtain such information from you and try to make it as legitimate as possible.
- **Spyware & Adware:** these are software that infiltrates your system and collect personal information about you. Such software are mainly attached with free to download content over the internet. Many of these software can also contain viruses.
- **Viruses:** these are the most common sources of attack on your computer. Viruses are malicious programs that infect your computer and all other systems you come in contact with.
- **Trojan Horses:** these are executable files that are hidden or embedded within legitimate software. Their main purpose is also to hack into your system, delete your files, or log your keystrokes.
- **Worms:** these are widely used programs that are propagated over the internet. These programs get stored onto your hard drive and cause unwanted interruptions when you use the internet by shutting down parts of the internet.

- **DNS & IP Leaks:** these threats originate when you are using anonymity software and your secure traffic leaks outside the anonymity network. Any entity that is monitoring your traffic can log your activities through DNS or IP leaks.

Web Browser Threats

There are numerous threats that propagate from your web browser and damage your online privacy and security. It is important to note that many popular web browsers, such as Google Chrome, Mozilla Firefox, Internet Explorer (now Microsoft Edge), Safari, and Opera have various security vulnerabilities.

We will focus on Google Chrome, Mozilla Firefox, and Internet Explorer for now in our guide and add details about other browsers very soon.

Google Chrome

Have you ever noticed that your Google Chrome requires you to sign-in with your Gmail ID? This is because Google Chrome saves a file on your computer where it stores all your email addresses, names, passwords, account numbers, phone numbers, social security numbers, credit card details, mailing address, and other auto-fill information.

According to Insider Finder, the data that Google Chrome saves leaves your private information susceptible to data theft. This is because Google makes copies of this data and stores it on History Provider Cache, Web Data, and other SQLite Databases.

These stored files are unprotected and if anyone has unrestricted access to your system or breaches these databases, they can easily retrieve your private information. If you are using Google Chrome on Windows PC, you can find these files here:

"%localappdata%\Google\Chrome\User Data\Default\"

Mozilla Firefox

When it comes to selecting a web browser, Mozilla Firefox is one of the lightest browsers to use. With that being said, it's not the most user-friendly browser in the industry. Compared to Google Chrome or Internet Explorer, Firefox can be difficult to manage.

In addition to this, there are certain security vulnerabilities in Mozilla Firefox that will leave your privacy breached. Some of these security threats pertain to unexpected crashes, memory safety hazards, and data security threats.

Mozilla Firefox has been known to crash when multiple plug-ins are working in the background. It provides poor data safety measures and low encryption levels. This leaves your personal information, and browsing history exposed to numerous cyber threats.

Internet Explorer

Internet Explorer might have lost its charm and gone back to square one in terms of web browser options, but it is important to highlight its security vulnerabilities. This is because some services still require you to use IE to access their online features.

Some of the security threats include malware attacks to bypass IE security features, DDoS attacks, exploiting the weak configuration of Windows and Internet Explorer, code attacks (JavaScript), and exposure of confidential data through malicious websites. All these threats will leave your private and confidential data on IE exposed to unwanted threats.

Another important factor you need to consider is that as of January 12th, 2016, Microsoft no longer supports all previous versions of Internet Explorer except for the latest Internet Explorer 11. It is even promoting you to upgrade to the latest Windows 10 and use its new browser called Edge, clearly indicating the IE is no longer a secure browser. Also, in the long run, you won't be receiving any security upgrades and bug fixes for IE, which puts at risk from various cyber threats.

Mobile Browsing Threats

With the increasing use of smartphones and tablets, internet security and privacy risks have increased considerably. This is due to the unsecure internet connection (Wi-Fi Hotspots) to which these devices connect. There are numerous cyber-criminals lurking around on these unsecure internet connections, waiting to pounce on your personal information and take advantage of your data.

This threat is magnified due to the diverse nature of these handheld devices and their ability to sync all your accounts, social media profiles, pictures and other data all in one place. According to Kaspersky Lab, the most targeted mobile operating system is Android. In 2012, more than 35,000 malicious Android programs were used to attack users.

The malicious programs were included in apps, Google Play Store, the Amazon app store, and certain third party app stores. Kaspersky categorized these Android threats into three categories:

- Advertising Modules
- SMS Trojan Viruses

- Exploits (to gain access to your personal information stored on the device)

This shows that mobile browsing is even riskier than normal web browsing. Like web browsers, mobile browsers are weaker when it comes to protecting your online privacy. The security measures and protocols used in web browsers are not strong enough to protect your personal information.

Online Banking & Payment Threats

The increasing use of e-commerce, online payment methods, online banking, and mobile banking has put your financial information is at high risk. With cyber criminals looking to exploit personal information about you, your bank account details and financial transactions are among the prime targets.

Symantec highlighted that there are two sources through which attacks on your online banking and payment transactions occur. These include local attacks and remote attacks. In local attacks, malicious cyber goons directly attack your local computer. In remote attacks, users are redirected to remote websites where their financial information is exploited.

These online banking and payment threats are increased if you use mobile banking. Various banks have found numerous security vulnerabilities in their mobile banking apps. In 2009, CitiGroup identified that their mobile banking app stored sensitive user data on smart phones in hidden files. So if you are using any of these apps or making online transactions on your PC, beware of all these threats.

Governmental Surveillances

If cyber criminals and malicious software's are not enough, there are numerous governmental organizations that are hell-bent upon spying on you. The first signs of governmental surveillance were revealed by Edward Snowden with the PRISM program in 2007. This program provided NSA the liberty to collect user's internet communication information for major US internet companies.

What's known as 'metadata', these governmental intelligence agencies can see all your internet activities, tap your phone lines, record all your communications, emails, text messages, VoIP conversations, and filter foreign traffic that passes through their boundaries.

NSA & Other Spy Collaborators

NSA might be seen as the pinnacle of all spying agencies but other intelligence agencies around the world have collaborated with NSA and share user's metadata with each other. A prime example of such collaboration is

the Five Eye nations (US, UK, Canada, Australia and New Zealand). Originally founded in World War II, Five Eyes are not used for War on Terror.

Legal Rules & Regulations

When it comes to legalizing governmental surveillance, there are numerous laws and legislation passed by the government. The US Patriot Act, FISA Amendment Act (FAA), and CISA are some of the examples passed in United States.

Similarly, other nations have also implemented laws that exempt intelligence agencies from prosecuted for breaching the personal privacy of their citizens. In Britain, the Serious Crime Bill allows such immunity to intelligence agencies like GCHQ, police and other surveillance agencies.

Data Retention Laws

Then there are laws that require telecom companies, ISPs, and tech companies to record metadata of their users legally. Such laws have been legally implemented in various countries. Some of these include Australia, European Union countries (UK, Italy, Germany, Czech Republic, etc.) and various other regions.

While these nations have laws that require storing of personal information of users, other nation's intelligence agencies continue to record sensitive data of users without any legal proceedings (like NSA in USA).

Social Media Threats

The increasing use of social media, physical boundaries have become nonexistent when it comes to connecting with other people. Sharing pictures, videos, latest trends, posting updates, and even buying stuff online have made the use of social media that much more important in our lives.

With that being said, social media has opened an outlet for numerous cyber threats that can bring harm to your online privacy. We all have been asked by someone unknown to add them on Facebook or follow them on Twitter and Instagram; these personal use social media for all kinds of heinous crimes. Here are some of the social media threats that can severely hamper your privacy and security:

Identity Thefts

Cyber criminals use your personal information (name, date of birth, photos, surname, etc.) and use this information to their advantage. From the creation of fake profiles to accessing illegal content, identity thieves can also try to exploit your financial transactions that are left behind on social media websites.

Spamming

There are numerous advertising companies that use social media websites like Facebook and Twitter as a platform for advertising their products and services. In the midst of these advertising companies are spammers. They promote malicious websites to users on social media and send ads in bulk, appearing user's newsfeeds. For instance, in November 2011, Facebook users were victims of a campaign that showed pornographic spam on their Facebook walls.

Sexual Harassers

Over the years, there have been numerous cases of victims being murdered, raped, and molested by sexual predators via social media. They prey on victims by using their personal details obtained from social media profiles. These sexual predators also use social media for harassment and making unwanted advances to random people.

Mainly teenagers are the biggest victims of sexual crimes through social media. One of the most popular cases relating to sexual crime via social media was of Peter Chapman, convicted murderer who used his fake Facebook profile to prey on young women.

Surveillance by Government

Social media provides an open access to all your private information and activities over the internet. Facebook, Twitter, LinkedIn, Instagram, and other social media websites are a prime target for governmental surveillance. These agencies can access such private information or use legal action into obtaining such data from these social media services.

Social Engineering

Social Engineering refers to the psychological manipulation of people and tricking them into revealing private and confidential information. The social media threats that we mentioned above, like identity theft and spamming, can be used in a much broader sense and be a part of a more complex fraud.

An attacker performing social engineering could use your social media profiles to gather information about your home (address), your contact details, your friends, your date and place of birth, your banking details and other financial information, your interests, and various other confidential data. This information can then be used by the attacker to perform all kinds of cybercrimes.

Organizations are usually a prime target of social engineering attacks as the attackers look to retrieve confidential business data and use it for their own advantage. Some of the common methods used for such attacks include baiting, phishing, pretexting (fabricated scenarios), quid pro quo (a promise in exchange for inform

Email & Text Messaging Threats

In the world filled with online scams and various cyber criminals, you are vulnerable to such threats from emails and text messages as well. There are many threats can hamper your privacy using emails and text messages:

- Botnets
- Hackers
- Malwares
- Viruses
- Spyware
- Phishes
- Scams
- Identity Theft
- Trojan Horses
- Adware

They would attach links in emails and make it look legitimate as possible, inducing users into opening them and getting infected. This way your privacy gets breached and the cyber goons gain access to all your sensitive data. Some cybercriminals can hack into your email account by cracking your password and gain access to all your confidential data.

Apart from spyware, viruses, phishing scams, and other threats you are prone to from emails, don't forget texting services. Web texting services, like WhatsApp, provide another avenue for cyber goons to seize control of your private information.

Some of these threats originate from web malware sent via text messages in different languages, crash messages intended to stop someone's web texting service, and the use of spying software to monitor status changes, pictures, messages, calls, and browsing.

Voice over Internet Protocol (VoIP) Threats

If you thought emails and text messaging services were unsafe, VoIP services can also lead to potential privacy breaches. With the increasing use of VoIP services like Skype, Vonage, Ring Central Office, and Ooma Telo, the number of privacy threats have increased considerably.

Cyber criminals look to eavesdrop on your conversations over VoIP services, hijack your registration, disrupt your conversations, make fraud calls and subscriptions, use our contact details, and use your credit card details.

Similarly, Denial of Service (DoS) attacks are also used to make your VoIP services slow or almost unusable. All these threats can severely damage your privacy and leave all your sensitive data in the wrong hands.

Cloud Storage Threats

Now if you are someone that storages their data on Google Drive, OneDrive, Shutterfly and other cloud storage devices, you should beware of privacy attacks in such services. Remember the hacking of iCloud and the leaked images of various celebrities in 2014.

If the hackers can break into Apple's iCloud, they can also break into other cloud storage services. According to a report by Gartner, 36% of US consumers will store their content on the cloud. This stat beckons the rising of numerous privacy attacks in the coming future and shows that lethal damage they can do.

Another privacy threat that you need to consider when using cloud storage is that they can be seized by law enforcement agencies. Governments can obtain legal warrants or legal notices to retrieve data of users from these cloud storage companies.

Privacy Tools

To protect against the numerous privacy threats that arise from various sources, you need certain tools for protecting against them. Here we have listed all the possible software, browser extensions, and other tools that you can use to safeguard your privacy against all the threats.

Virtual Private Network (VPN)

A Virtual Private Network or VPN is a software/application that creates a secure tunnel between you and a remote server. It is the ultimate tool for becoming anonymous over the internet and hiding your true identity. If you are concerned about maintaining your anonymity over the internet, consider investing in a premium VPN service.

A VPN has several servers located in different countries around the world. When you connect to these servers, secure tunnels are created. While doing so, your original IP address is masked and replaced with the IP address of the server you are connected too. It is the best defense against government surveillance as spy agencies cannot see your true location.

If you are concerned about your internet activities being tracked by your ISP or anyone else, a cheap VPN allows you to secure your data from such entities. When you create these secure tunnels, all your internet traffic is encrypted and hidden away by protocols in the process; not allowing your ISP, government or any other third party to eavesdrop on what you do over the internet.

Here are some factors you should look for in a VPN that would protect your privacy:

- Zero log policy (does not keep activity logs)
- Provides at least AES 256 bit encryption levels
- Offers OpenVPN protocol
- Offers shared IP’s
- Has servers spread across the world
- Anonymous payment options available
- VPN service is based in internet friendly location

Tor (The Onion Router)

Tor is a free to use software that is designed to encrypt your internet traffic and keep you anonymous over the internet. Originally known as The Onion Router, Tor became its acronym and is now known by this name throughout the world.

Tor allows you to connect to a series of randomly selected nodes on its network of servers (operated voluntarily) and encrypts all your internet traffic each time it passes through a node. Although each node knows who is connected to it and who it connects to, no one knows the entire circuit (route).

Since Tor is free, it provides an immediate solution to preserving your privacy against online surveillance and becoming anonymous. However, one of the major drawbacks of Tor is in its final link in the circuit (exit node). As nodes are operated by volunteers, those running the exit nodes come under scrutiny if anything illegal passes through their node (like pirated content).

This leads to the problem of finding public exit nodes on Tor as they are available in a limited amount. Also, governments of various nations, such as China's, has used these exit nodes to monitor users and blocked these nodes. Similarly, Tor should not be used for P2P file sharing or using torrents. So if you value your privacy and can be patient with finding exit nodes, then Tor is your best tool for preserving your privacy.

Free Open Source Software (FOSS)

The use of free open source software (FOSS) comes on the back of increasing influence of NSA over tech companies and forcing them to create backdoors for their software and programs. FOSS allows everyone to see the secure codes and examine them; allowing programmers to create open source software that are difficult to tamper with.

Free open source software minimizes the risk of governmental intelligence agencies from interfering in the software and weakening its defenses. Over the years, NSA has been reported to fiddle with online security software and hamper their security in order to gain access to the program.

This is precisely the reason why you should avoid software made in US or UK, as the developers can be easily influenced by NSA and alike. It is recommended that you use FOSS more often and if you combine it with open source operating systems, like Linux, you can secure your privacy and minimize any risk of governmental agencies from tampering with the programs.

Tools for Securing Your Online Payments

Now if you are someone that shops online often then you should know that the majority of the cyber attacks are made in an attempt to gain access to your financial information. According to a report by McAfee, the total financial loss to the global economy in 2014 was estimated to reach $575 billion.

Based on this statistic, you should secure your online privacy, especially when making online payments and transactions. Here are some tools that you can use for securing your online payments.

- Use anonymous payment methods (like BitCoin)
- Use Prepaid Credit Cards
- Use Crypto – Currencies
- Buy with cash for local purchases

BitCoin

BitCoin isa revolutionary payment system that allows you to make anonymous payments. Developed in 2008 and released as an open source software in 2009 by Satoshi Nakamoto, what makes BitCoin so secure is that it does not require a middleman or controlling organization (like a central bank) to work.

BitCoin is perhaps one of the most popular crypto currencies currently in use today. Many e-commerce websites, VPN providers, and other services accept payment through BitCoin. The basic mechanism behind BitCoin is similar to peer to peer technologies such as BitTorrent.

To ensure complete anonymity while paying with BitCoin, follow these steps:

- Create a pseudo, disposable account (email address, name, etc.) that does not reveal your true identity.
- Always use new BitCoin address (wallet) when making a purchase. This will ensure that the financial transactions cannot be traced back to you.
- When filling out BitCoin details, never reveal your real name, phone number, address, and other personal information.
- If you buy BitCoin from automated exchanges (like CoinBase), they may require you to reveal real world identity. However, with mixer services (such as Shared Coin), you can ensure complete anonymity by laundering your BitCoin purchases. Although, this method is not free but mixer services anonymizes your BitCoin by swapping it with other users; making it difficult to be traced back to you.

Prepaid Credit Cards

Another method of securing your online payments is through the use of prepaid credit cards. Although this method may be location dependant, you can use it to buy gift cards over-the-counter and then use a pseudo email address to purchase crypto currencies like BitCoin. This method ensures complete anonymity while making the purchase and also guarantees secure online transaction.

Crypto Currencies

Today, there are over 660 different crypto currencies that are available for trading in the online market. BitCoin is undoubtedly the most used of them all and the most popular as well. However, besides BitCoin, you

can use other crypto currencies make your online payments. Some of these include Auroracoin, DigitalNote, Dash, Nxt, Emercoin, and many more.

Virtual Machines

You can boost your online security by accessing the internet or streamlining certain tasks on the internet using virtual machines. In the world of computing, virtual machines are programs or software that emulates a particular computer system.

This is achieved by emulating a hard disk onto which an operating system is installed while your normal OS runs in the background, effectively emulating a computer system. So in short, it's like running a whole new OS on top of your standard OS. Some popular virtual machines include the likes of VMWare Player, VirtualBox, Parallels, QEMU, and Windows Virtual PC.

This makes virtual machines an excellent tool for protecting your privacy over the internet. The malicious threats caught by virtual machines protect the host computer from being infected or infiltrated. However, virtual machines can make your system slow as more processing power would be required for running an OS on top of another OS.

DNS & IP Leak Tests

Now if you are using privacy tools to hide your IP address like a VPN, there are still chances that your IP address and DNS can be leaked. To find out of your DNS traffic or IP is leaking, you can use free tools such DNSLeakTest.com, Whatsmyip.org, and DNSleak.com.

If the results of the test show the DNS and IP of your privacy software (VPN) then you have no leaks. However, if you are being shown the DNS and IP address of your ISP then you have a leak. This means that anyone monitoring your traffic can trace it back to you due to these DNS and IP leaks.

To fix this problem, DNSLeakTest.com has outlined the following steps:

- Before connecting to your privacy software (VPN), set your static IP address properties if using DHCP.
- Once you are connected, remove all the DNS settings.
- Once you are disconnected, switch back to original static DNS server or DHCP.

These are some basic steps that can help you fix DNS leaks. There are programs available that can initiate these steps automatically and fix DNS leaks. Otherwise, you can manually clear the DNS settings and fix the problem of DNS leaks.

Web Browser Extensions

In order to protect your online privacy that arises from web browsers, there are various browser extensions and tools available at your disposal. These tools range from cookie blocking extensions, VPN extensions, HTTPS, to programs that will help you secure your browsing history.

VPN Extensions

There are a handful of VPN providers that offer their own web browser extension. From the likes of Hola, Zenmate, and TunnelBear, these providers allow you to secure your web browsing by encrypting it and tunneling it through their own servers using these extensions. Majority of these extensions are free to use but some of them have a cap on the amount of data you can use in a given time period.

Ghostery

A free web browser extension available on Google Chrome, Mozilla Firefox, Safari, and Opera, Ghostery allows you to see all the hidden tracking technologies are working in the background. With Ghostery, you can block cookies, tags, beacons, web publishers, pixels, and other web tracking tools.

AdBlock Plus

This is a must have browser extension as AdBlock Plus blocks all kinds of ads (paid & free). AdBlock will stop any ad that pops up while you browse various websites, block ads on YouTube, Facebook, and other social media channels, and disable third-party cookies and scripts. Although AdBlock may allow some ads to pass through but can change its filter preferences to stop any ads being allowed through.

Privacy Badger

Privacy Badger is another browser extension designed to stop tracking technologies that are running the background. It stops spying ads, cookies, fingerprinting technologies, blocks malware, and various other web tracking technologies.

HTTPS Everywhere

The HTTPS Everywhere is also a free web browser extension and is a must-have. Compatible with Firefox, Chrome, and Opera, what HTTPS Everywhere does is that it ensures that you always connect to a website through HTTPS connection. This protects your web browsing privacy as your web traffic passes through encrypted connections.

Disconnect

Disconnect is an excellent little tool that works similar to Ghostery. It will allow you to block all web tracking technologies, blocks malware, and keeps your web searches private. The premium version of Disconnect also offers a VPN service, multi-device compatibility (3 devices simultaneously), and works on desktop and mobile.

NoScript

There are many scripts that are running in the background on your web browsers (mainly javascript). These scripts can leak identifiable information about you. NoScript is a powerful tool that can give you control over which scripts run on your web browser. However, NoScript is not for anyone who is not tech-savvy. It requires technical knowledge and understanding of the risks involved in stopping certain scripts.

BetterPrivacy

Apart from normal cookies, some websites run LSO (Local Shared Objects) for tracking your activity. LSOs are commonly known as 'Flash Cookies'. You can configure Flash and block all the LSOs. However, that would mean breaking Flash content – which could be problematic. This is where using BetterPrivacy extension is helpful as it blocks these Flash Cookies and allows you to manage the LSOs.

Secure Search Engines That Don't Track

Among the many web browsing threats, the last thing you need to worry about is different search engines storing all your search information. Popular search engines, Google and Yahoo, store information such as your IP address, search term query, date and time of the search (query), and trace the search back to your computer using Cookie ID.

Most search engines also combine your past search queries and the posts that you 'Like' on social media in order to bring you the best search results as possible. This is what's known as 'filter bubble' where search engines profile you and bring up results closer to your interests; in turn lowering results that might have an alternate point of views and opinions.

This is where you should use search engines that do not track you and provide you with unbiased search results. Following are some of these secure search engines:

DuckDuckGo

One of the best alternate search engines currently out there. With DuckDuckGo, your search queries are anonymous and are not tracked. However, DuckDuckGo does state that it has to comply with court orders and share user data if asked. But since it does not track your search queries, there isn't anything potentially dangerous that can be given away.

YaCy

If you do not trust the search engines maintaining your privacy then you can use YaCy which relies on peer-to-peer technology. YaCy does not store your search terms or use Cookie IDs, instead of using a global peer network it provides the best results from indexed web pages.

StartPage

This is another secure search engine that promises not to store information about your searches, use Cookie IDs, or send your personal information to third parties.

Gibiru

What Gibiru does is use Google search results but keeps your IP address (identity) anonymous by separating the search term using proxy servers. It also removes all records within a few seconds of performing the search

Email Encryption Tools

The increasing infiltration of governments and the implementation of data retention laws have made our emails susceptible to privacy breaches. Most email services have incorporated SSL encryption to their email services. However, SSL is of no use if these email providers (Google & Microsoft) are sending your information to governmental agencies (NSA).

The answer to securing your privacy over emails lies in end-to-end email encryption. There are various tools that you can use to secure your emails. Here are some of the best and easy to use email encryption tools.

Do note that these encryption tools do not hide every aspect of your email. The email address of the sender and receiver, subject line, and the date & time of the email are still visible. The only contents that are encrypted are the body of the message and its attachments.

- GNU Privacy Guard
- Pretty Good Privacy (PGP)
- Infoencrypt
- GPGTools

- GPG4Win
- HP SecureMail
- Proofpoint
- EdgeWave
- Cryptzone
- Mailvelope
- DataMotion
- Sendinc
- Enlocked

Tools to Secure VoIP Conversations

In light of various cyber attacks, you are vulnerable to privacy breaches via VoIP services. To safeguard your privacy against the VoIP threats, that we highlighted earlier, you should use VoIP services with end-to-end encryption. Some of these tools include:

- **RedPhone:** It is open source software available in Android devices and is free to use. RedPhone offers end-to-end encryption over VoIP services, allowing you to encrypt all your calls.
- **Signal:** it is free and open source software but designed for iOS devices. Signal is developed by the same makers that made RedPhone. It allows you to encrypt your voice calls and text messages as well.
- **Jitsi:** you can easily substitute Skype with Jitsi as it allows all the functionalities such as calls, video conferences, file transfers, and Chat. However, Jitsi encrypts all your conversations and VoIP activities with ZRTP.
- **Tox:** this is another free to use software to secure your VoIP conversations. Just like Skype, Tox allows you to make free calls, send messages, transfer files, and host video conferences. However, calls on Tox are for Tox – to – Tox.
- **Silent Circle:** this is a complete suit where you can encrypt all forms of conversations. Within this suit is the feature called Silent Phone. This helps to protect your voice and text based conversations on iOS and Android devices. Previously, it also provided Silent Eyes (a VoIP services on Windows) feature but now the service has been discontinued.

Tools for Securing Instant Messages

The tools that we have mentioned above for securing your VoIP conversations also provide protection for your instant messages. Apart from these tools, there are some dedicated apps and programs designed to safeguard your privacy over instant messages. Some of these include:

- **Pidgin + OTR Plugin:** it is a open source IM client that can be used with Google Talk, Yahoo, MSN, and many other chat services. OTR plugin is an add-on and allows end-to-end encryption with forward secrecy. This secures all your messages and encrypts all your conversations.
- **Gliph:** one of the best tools for safeguarding your messages, Gliph allows you to change your identity to a pseudo name and then switch it back again. Another feature that sets apart Gliph is its ‘Real Delete’ option, were you can delete your message from sender’s and receiver’s devices as well as from Gliph’s servers.
- **Adium + OTR Plugin:** Adium is also a free and open source IM client but exclusively for iOS devices. The OTR plugin comes built-in with Adium allows you to encrypt your instant messages.

- **Chatsecure:** it is compatible on all major platforms and works with almost all IM services. Chatsecure has OTR built-in and protects your messages from any privacy breaches.
- **Telegram:** it is compatible on Android, iOS and Windows devices. Telegram provides end-to-end encryption, securing all your messages. Telegram does not store your messages on its servers and has a feature where it can delete the message from sender's and receiver's device simultaneously; leaving no trace of your conversation.
- **TextSecure:** designed for Android specifically, TextSecure replaces the default text app in your Android device and encrypts all your messages. This is an excellent tool as your messages will remain encrypted even if your phone gets stolen.

Data Encryption

In light of all the privacy threats and increasing interference from various governments, it is data encryption that allows you to safeguard your private information. Many of the tools that we have listed above use encryption to hide your data from landing into the hands of privacy invaders.

What is Encryption?

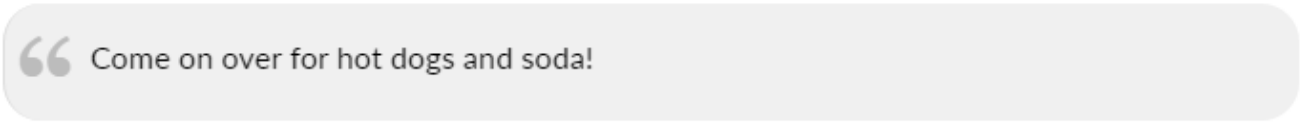
You will find multiple definitions of 'encryption' over the internet. Some have defined it as a way of translating the data into secret codes, while others have put it as the conversion of data into ciphertext that cannot be read by anyone except for the authorized parties.

However, to simply put it, encryption is a way by which your messages, files, and other information are scrambled, not allowing anyone to see the contents of the information unless they have the correct encryption key to unscramble the data.

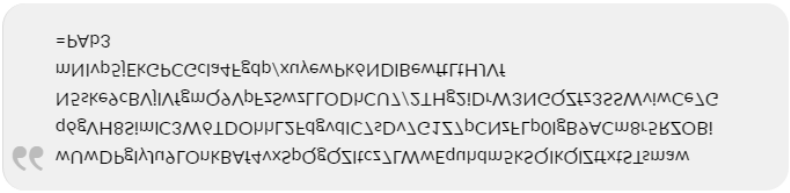
How Does Encryption Work?

Like the definition puts it, data encryption scrambles your data and using encryption algorithms, it translates plaintext into ciphertexts. The encrypted data cannot be understood or read by anyone unless they have the encryption keys to decrypt the data.

To demonstrate what it looks like to encrypt a message, we used PGP software to encrypt an email containing the following message:



When it was encrypted by PGP, this is what anyone will see if they intercepted our message:



Different Types of Encryption Algorithms

When you dig a little deeper into encryption, what goes in the background is that there are different algorithms that are working to encrypt your data. Over the years there have been various encryption algorithms, each with their particular encryption key length, level of protection, and other features.

- **Triple DES:** Data Encryption Standard (DES) algorithm was perhaps the first ever encryption algorithm made public. This was relatively weak and easy for hackers to crack. To replace DES, Triple DES was introduced which used three individual keys of 56 bit. Now slowly replaced by other encryption algorithms, Triple DES was highly used by financial services.
- **Blowfish:** it is one of the most flexible encryption algorithms out there and was also introduced to replace DES. Using 64-bit ciphers, Blowfish is known to provide great speeds and is mainly found in protecting your password while you shop online or make payments.
- **Twofish:** it is the successor to the Blowfish algorithm and was also known to provide fast speeds. Twofish used encryption keys up to 256 bit and its free open source nature meant that it is found in popular encryption software such as TrueCrypt, GPG, and PhotoEncrypt.
- **RSA:** unlike Triple DES, Blowfish and Twofish, RSA uses an asymmetric algorithm. What this meant is that RSA used 2 keys, one for encryption and the other for decryption. This made RSA more secure than the other encryption algorithms and is found in popular software such as PGP and GPG.

- **AES:** Advanced Encryption Standard (AES) is considered the strongest encryption algorithm in today's time and is trusted by the US government and other authorities. Using encryption keys from 128 bit, 192 bit and 256 bit, AES can stop all kinds of attacks from hackers. Although brute force attacks can still crack AES encryption, it would require a massive amount of computer power and time to achieve this.

Encryption Key Lengths

We have talked about encryption, how it works and some of the popular encryption algorithms you will find in various encryption tools, but how long does it take to break the cipher. The easiest or crudest way of finding that out is by looking at the encryption key lengths.

These are the total number of zeros and ones or the raw numbers involved in an encryption key. Depending on these key lengths, security experts determine the total amount of time it would take to break each encryption. To give an idea, consider this:

- AES 128 bit encryptions would require 3.4×10^{38} operations to successfully break it.
- The fastest and most powerful computer on earth, Tianhe-2 (located in China), would take roughly 1/3 of a billion years to break AES 128 bit encryption by force.
- Since AES 256 bit is more powerful than 128 bit, it would require 2^{128} times more computer power to break it by brute force. More precisely, 3.31×10^{65}

Looking at these numbers, it would massive amounts of computer power, resources, and time just to break AES 128 bit encryption. While it takes this much time to break 128 bit, cracking AES 256 bit encryption would make the world stop. That is why, perhaps, it has not been broken yet and considered the strongest encryption level so far.

Ciphers

However, don't think that encryption key lengths are the only thing that determines encryptions strength. The mathematical algorithms that encrypt your data in the background, called ciphers, are the real strength of any encryption.

These are the main reason or source through which encryption is broken. Any weakness or shortcomings in the algorithm can be exploited by hackers and used to break the encryptions. We have already discussed some common ciphers above such as Blowfish, RSA, and AES.

End-to-End Encryption

In order to guarantee complete privacy and security, you should opt for services that offer end-to-end encryption. What end-to-end encryption does is that it encrypts all your data at your end (PC, laptop, router, phone, tablet, gaming console, etc.) and then decrypted at the intended destination.

The best thing about end-to-end encryption is that there are no middlemen or any third party that can access your data during the entire process. No entity can access your unsecured data in end-to-end encryption without permission. This is what makes end-to-end encryption an absolute must for protecting against various cyber threats.

Perfect Forward Secrecy

Perfect Forward Secrecy is a system that ensures your encryption remains safe from being breached. It works by creating new and unique private encryption keys for each session. This way Perfect Forward Secrecy prevents your data from being compromised in case there is a leakage of an encryption key; protecting other session keys in effect.

Can Governments Compromise Data Encryption?

Since we have talked about encryption in detail, the real question beckons, can governmental agencies compromise data encryption? According to the facts revealed by Edward Snowden, this is very much true. The underlying reason for this is because of NIST (National Institute of Standards and Technology).

NIST develops and certifies almost all of the data encryptions that are currently in use today. Some of these include AES, RSA, SHA-1, and SHA-2. However, the problem with NIST is that it works very closely with NSA for developing different encryption ciphers. NSA has been known to tamper with software and create backdoors; leaving us to question the integrity of NIST.

GCHQ & NSA Can Break RSA Encryption Key

One example of encryption being compromised by governments came out of the information provided by Edward Snowden. Based on his reports, a codenamed program called ‘Cheesy Name’ was used to single out certificates and could be cracked by GCHQ supercomputers.

What this meant is that any form of encryption that relies on certificates can be cracked by governmental intelligence agencies. Based on this notion, SSL, TLS, and 1028 bit RSA encryption key could be easily compromised by NSA and GCHQ. This is why you will find 2048 bit and 4096 bit RSA encryption in most of the software (primarily VPNs).

Protocols

Secure protocols are the other piece of the puzzle that helps to secure your privacy and safeguard your data against numerous threats. They work in combination with different data encryption levels; forming protective barriers that won't allow different threats from breaching your privacy and security.

Different Types of Protocols

There are various protocols that you will see while using different encryption software. Some software automatically selects the best-suited protocols while others allow you to choose (like in a most VPN services). Here are the most commonly seen protocols you will see:

PPTP

Point-to-Point Tunneling (PPTP) is considered one of the fastest and easiest protocols to use today. However, there are many security vulnerabilities in PPTP. It is not the most secure protocol and can be easily breached by hackers, governmental surveillance agencies, and others alike. This is why PPTP is mostly referred for bypass geo restrictions and streaming online, not for securing your privacy.

L2TP/IPSec

L2TP/IPSec provides better security and is considered more secure compared to PPTP. Since L2TP itself doesn't encrypt your data, you will see it with IPSec suit. However, L2TP/IPSec is much slower in performance; different firewall also make it difficult for setting it up, and according to Edward Snowden L2TP was deliberately compromised by NSA at the time of its development.

OpenVPN

OpenVPN is open source software and is considered the most secure protocol that you can use today. It supports all major encryption algorithms (Blowfish, AES, etc.) and high security with fast speeds. The open source nature of OpenVPN means that it was not compromised by NSA. Having said that, OpenVPN requires third-party software for setup on some devices and can be tricky to set up.

SSTP

You will find SSTP protocol primarily on Windows platform. Originally developed by Microsoft, it was first seen in Windows Vista SP1. SSTP provides similar security as OpenVPN but given the long history between NSA and Microsoft, there are chances that it could be compromised.

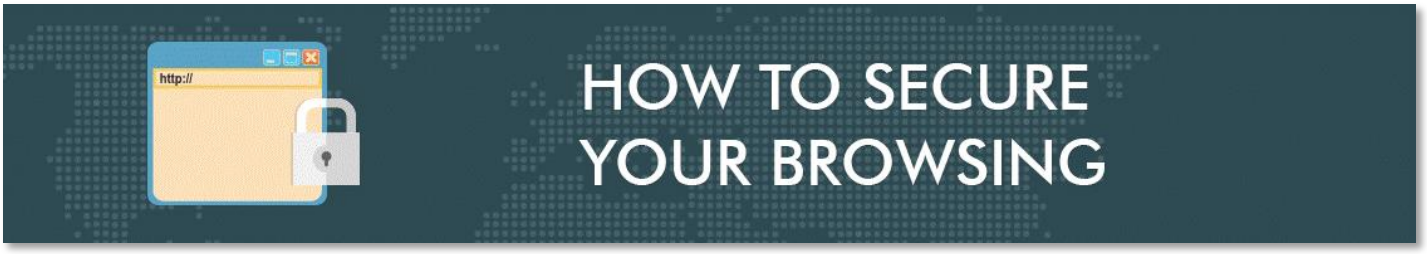
IKEv2

IKEv2 provides good overall security and uses the same basis as the IPSec protocol. IKEv2 is considered by faster than PPTP, SSTP, and L2TP/IPSec and is mainly found in various mobile operating systems (such as BlackBerry). However, not all devices support IKEv2 and its configuration can be complex. Since it was jointly developed by Microsoft and Cisco, IKEv2 is not immune to NSA tampering.

Which Protocol (and Encryption) Should You Use?

When you take the pros and cons of each of these protocols into consideration, finding the right balance for online privacy can be tricky. For ultimate online security and anonymity, OpenVPN protocol with 256 bit AES encryption should be your first and obvious choice.

The open source nature of OpenVPN and immense power needed to break AES 256 bit encryption means it's the strongest you can use today. On the other hand, you can use L2TP/IPSec protocol if the OpenVPN protocol cannot be used for any reason. L2TP/IPSec provides secure connections and is supported by a wide variety of devices.



How to Secure Your Browsing

Now that you know about various threats that can breach your online privacy, the different tools that you can use to stop your privacy being invaded, and which encryption and protocols you should use, here is a quick guide on how to secure your web browsing.

Clear Cookies

Cookies are the real reason why different websites know what you are up to on the web. They get stored onto your PC and send small pieces of information back to the website. So the next time you visit the same website, a cookie sent to the website's server containing all your previous activities.

These cookies can store important information about you such as passwords, credit card details, addresses, and other personal information. This is where using browser extensions such as AdBlock Plus, Privacy Badger, and Ghostery come to your aid. They help in identifying and blocking various types of cookies. Similarly, BetterPrivacy browser extension is highly useful for blocking Flash Cookies and managing LSOs.

Many popular browsers now have the option to stop storing regular cookies but Flash cookies are still a menace. However, you can use the following application to clear Flash cookies:

- **CCleaner** (available on Windows and Mac OS): CCleaner helps to protect your privacy by clearing out flash cookies. It also aids in making your system faster and clears your system's registry, which can be cluttered with errors and broken settings

Use Browser Extensions to Strengthen your Privacy

In addition to cookies, your online privacy can be compromised by online surveillance, hackers, spammers, and other malicious cyber-goons. This is where using a VPN browser extension allows you to safely access the websites and surf the web without leaving any tracks. VPN browser extensions come in handy when you are short on time but want to access online banking or want to make online purchases.

Similarly, AdBlock Plus stops pesky ads from being spammed onto your browser screen. It is a great tool for preventing third-party ads from retrieving personal information about you or leads you to fraudulent websites.

Web Tracking Technologies

Web tracking technologies work in the background and monitor your every move. If you want to identify these tracking technologies then browser extensions such as Ghostery, Privacy Badger, Disconnect, and NoScript can very useful. They block various tracking tools such as tags, malware, cookies, beacons, pixels, web publishers, and other similar technologies.

Here are different web tracking technologies you should consider:

- **Browser Fingerprinting:** as we mentioned above under 'Web Brower Threats', many latest browsers collect information about you in various ways so that you can be uniquely identified. The process through which this is achieved is called browser fingerprinting and you can stop this by using the Privacy Badger add-on.
- **HTML Web Storage:** there is a web storage that is built into different web browsers. It works just like cookies but has more storage and you cannot monitor it or selectively remove it from your browser. In Firefox and Internet Explorer, you can turn HTML Web Storage off, but using Click&Clean and BetterPrivacy extension to remove content from this web storage.
- **ETags:** Entity Tags or ETags are a part of HTTP protocols and are used for validating your browser's cache. When ETags are validated, you create a fingerprint when you visit a website and these ETags can be used to track you.
- **History Stealing:** there are various notorious websites that can retrieve your previous browsing history. The process employed by these websites is to exploit how the Web works. The most damaging part about History Stealing is that it is virtually impossible to stop. However, you can stop it from tracking your original identity by using a VPN or Tor.

Use Search Engines That Don't Track You

Many popular search engines such as Google and Yahoo store precious information about you which can be traced and could lead to privacy breaches. This is where you need to use search engines that don't track you, in order to secure your browsing.

We have mentioned some of these search engines in detail under 'Privacy Tools'. Search engines such as DuckDuckGo, StartPage, YaCy, and Gibiru do not store information such as your IP address, search term queries, and other information.

Make Your Mobile Browsing Secure

As we plunge into the world of handheld devices and increasing use of internet on Smartphones, it is important to secure your privacy on mobile browsing. The browser extensions that we have mentioned so far focus primarily on desktops but some of them will work on your mobile platforms as well.

Amongst them is the popular AdBlock Plus which will help you to stop pesky ads, tracking technologies, and other malicious background tools. If you have Firefox installed onto your mobile device, then you can also use extensions such as Ghostery.

Similarly, there are various apps that you can use for advanced cookie management and blocking various web tracking technologies. Private Browsing and Do Not Track options are now being made available on various mobile operating systems, which is a step in the positive direction.

Protect Your Social Media Profiles

While we are on the subject of securing your privacy while browsing, it is important to mention the steps for securing your social media profiles as well. Here are some of the steps you can take to ensure the safety of your social media profiles:

- **Check the Privacy Settings of Social Media Profiles:** different social media networks like Facebook and LinkedIn provide various privacy settings and allow you to control and manage posts on your profile. Use these settings to preserve your online privacy.
- **Setup Two Factor Authentication:** you can set up two-factor authentication on social media profiles to protect against hackers and other forced break-ins. Some social media networks such as Facebook and Twitter already offer this feature. Use it to ensure no one access your account without your approval.
- **Create Strong Passwords or Use Password Manager:** in addition to two-factor authentication, you should create strong passwords or use a password manager to manage password security of different social media profiles.
- **Don’t Reveal or Post Too Much Personal Information:** as you might have seen, people list down every little detail of themselves on social media profiles. We would advise you against this and would recommend that you put up a little detail of yourself as possible.
- **Manage Your Friends Circle:** social media allows you to connect with numerous people but not everyone needs to know every aspect of your life. Manage your friends' list and put limitations on personal information visible to different individuals.

- **Think Twice before Posting:** once you post something online on social media, make sure that it is something that won't compromise your privacy.
- **Use Remove, Block, & Report Features:** different social media networks allow you to report, block and remove malicious activities on your profile. Use these features when you feel someone is harassing you or trying to breach your privacy.

How to Secure Your E-Mails

The on-going surveillance conducted by governmental agencies, the implementation of mandatory data retention laws, and the continuous threats posed by cyber criminals, your emails are at great risk. Over the years, many users have lost private and confidential data when their emails were hacked or intercepted.

We mentioned earlier the threats that you can encounter through emails. From email spoofing to defamatory emails, frauds, and malicious content sent over the emails, it is of great importance that you secure your emails.

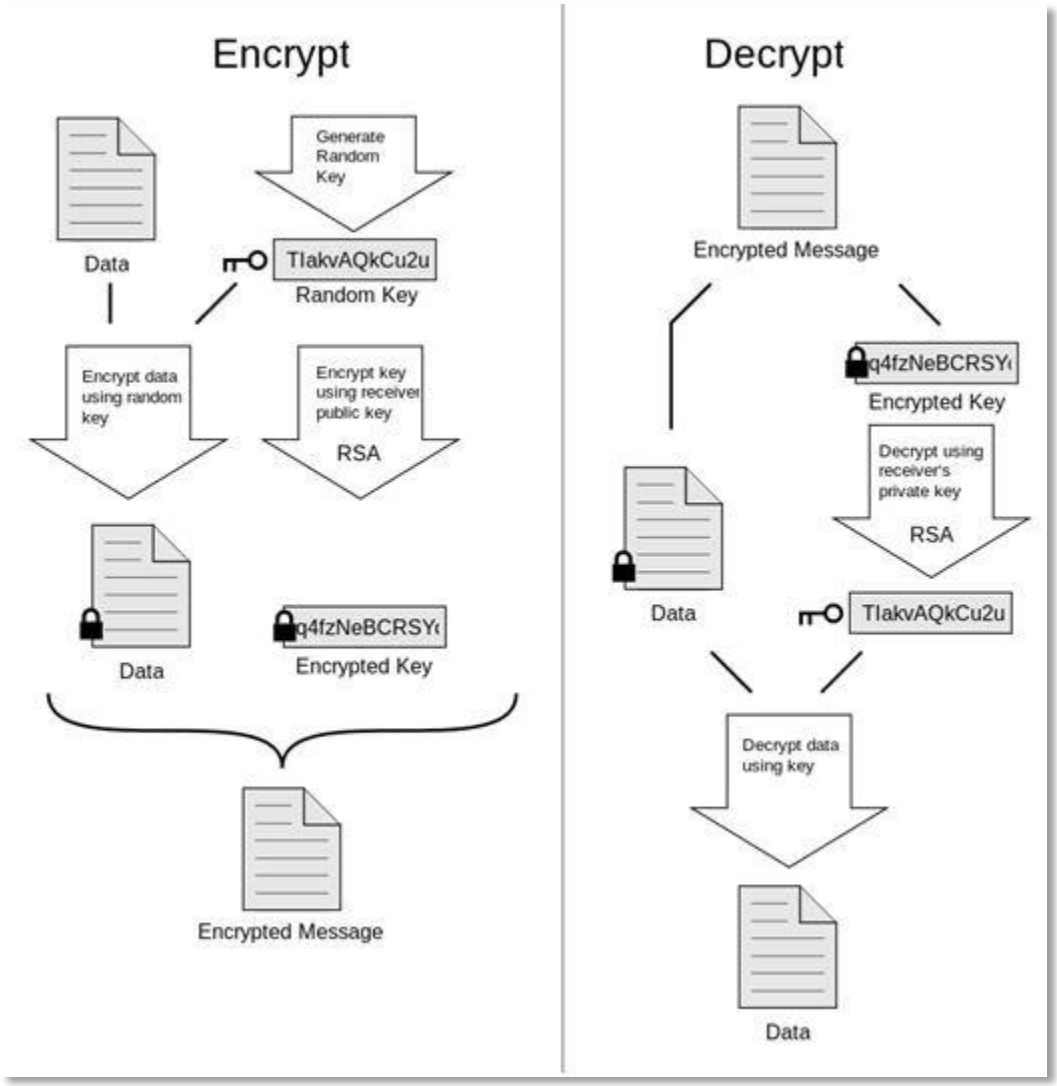
Many email services have incorporated SSL encryption to secure your emails. However, the key lies in end-to-end encryption as it encrypts your data at your end and decrypts it at the intended destination.

Use Email Encryption Tools

There are various end-to-end encryption tools you can use today. We have highlighted some of these tools earlier under the heading 'Email Encryption Tools'. The most popular among them all are PGP and GPG. Both the tools are free to use and encrypts all sorts of data, including the contents of your email. Here are our top 3 picks from different email encryption tools you can use:

Pretty Good Privacy (PGP)

PGP or Pretty Good Privacy is an open source and free encryption software. You can use it to encrypt all forms of content such as emails, text messages, files, directories, hard disk partitions, and other forms of communication as well. Here is a simple illustration, explaining how PGP works:



GNU Privacy Guard

GNU Privacy Guard or GPG is an upgrade of PGP and uses the same OpenPGP standard. GPG is also free to use software and allows you to encrypt all your data and communication. The open source nature of the encryption tool makes it compatible on various platforms, including Windows, Mac and Linux. GPG uses a command line interface and also offers more sophisticated versions for all the three platforms.

GPG Tools

For all Mac users looking for an email encryption tool for free, GPGTools provides you just that. The GPGTool is open source software and with it, you can protect your Apple Mail. GPGTools incorporates OpenPGP, helps to encrypts or decrypts your emails on Mac, and protect your email conversations from various cyber threats.

GPG4win

GPG4win is another free email encryption tool but exclusively for Windows users. GPG4win also utilizes OpenPGP along with S/MIME to safeguard your emails. The best part of GPG4win is that it can be integrated easily with any commonly used email services. you can even use a featured called GPGOL that encrypts Microsoft Outlook emails as well.

Infoencrypt

If you are looking for a web based service to encrypt the contents of your email, then Infoencrypt is the best tool out there. It is free to use and you do not require any software download to encrypt your emails.

Infoencrypt utilizes 128 bit AES encryption, which is strong enough to hide the contents of the email. The overall process for encrypting data using Infoencrypt is fairly simple. All you have to do is enter your data, select a password and encrypt your data.

Once you click on ‘Encrypt’, your data is encrypted into codes. To decrypt the message, the recipient will have to enter the password you selected and then decipher the data.

Honorable Mention

Apart from the three email encryption tools mentioned above, you should also check out Mailvelope. It is free to use web browser extension for Chrome and Firefox. Mailvelope offers end-to-end OpenPGP encryption and can be used with all major email platforms (Gmail, Outlook, Yahoo Mail, and GMX).

Other Precautions to Secure Your Email

Email encryption tools are just a small part of securing your emails from potential security breaches. There are other precautions you should also take into account when operating your email services.

- **Create Strong Passwords:** This is perhaps the most basic step towards email security. You should generate strong passwords for each of your accounts and don't use the same password for more than one email accounts or social media profiles.
- **Don't Click on Unsecure Links:** You should avoid clicking on links that are not secure. Many cyber-goons look to retrieve your private information when you click on these malicious links. Check all links before clicking. Hover your mouse over the links and see where you are being redirected.
- **Avoid Accessing Emails on Public WiFi Network:** If you are connected to the internet over free and public WiFi hotspots, try to avoid opening your emails unless you have a VPN or email encryption tool connected.
- **Keep UAC (User Account Control) switched ON:** Don't turn OFF UAC on your Windows OS as it monitors different changes that take place in your system. Instead of completely turning UAC off, you can decrease the level of protection.
- **Scan Email Attachments:** Various researches have shown that the majority of the viruses that infect users systems are obtained through email attachments. Some email services have built-in antivirus scanners which scan your email attachments. In any case, scan your email attachments before downloading.

How to Secure Your Conversations

The growing threat from various cyber criminals to governmental surveillances, it is imperative that you protect your communications from being breached. Having said that, you need keep this in mind that calls made over cell phones or landline are never secure. Governments from all around the world collect call information through metadata.

However, communication made electronically (such as over VoIP services) can be encrypted and protected from unwanted cyber-goons. There are various tools that you can use to safeguard your VoIP conversations and instant messages.

We have already mentioned some of these encryption tools under the 'Tools to Secure VoIP Conversations' and 'Tools for Securing Instant Messages' headings. Here is how you can use them to secure your VoIP conversations and text messages.

Use End-To-End Encryption Tools

The important thing to note is that all of these tools use end-to-end encryption. This is what makes your conversations safe from being monitored or tracked by unwanted entities. Some VoIP services, such as Skype use peer-to-peer protocols which make it difficult for anyone to trace your calls.

Signal Private Messenger

If your service doesn't use a peer-to-peer protocol, then you can use tools such as Signal Private Messenger for Android and iOS devices. Signal Private Messenger is developed by Open Whisper Systems, the same firm that created TextSecure and RedPhone. Signal Private Messenger combines the two tools, TextSecure and RedPhone, and allows you to encrypt your VoIP calls and instant messages.

Silent Circle

Another tool that you can use for securing your conversations on Android and iOS devices is Silent Circle. Within this security, a suit is a Silent Phone which encrypts your voice, video, and text based communications. Silent Phone is available in two packages, Basic and Plus. You can choose from either of the two depending on your need for security.

Gliph

When it comes to securing only your text based communication, you ought to try Gliph. It offers some slick features offered by this app and set it apart from other text encryption apps. You can use Gliph on your Android devices, iOS devices, and desktop PCs. You can secure your communication on any channel; choose a pseudo name to hide your real identity, and secures your privacy while making BitCoin payments.

Threema

Threema is a paid app for iOS, Android, and Windows Phone users and provides great features for securing your VoIP communications. Using end-to-end encryption, you securely send messages, files, videos, voice messages, QR codes, and much more. It also guarantees complete anonymity as each user is given a Threema ID and your original phone number or email address are not visible to others.

Turn off GPS, Google Now & Other Location Tracking Services

In addition to using different encryption tools, there are some settings on your mobile devices that you can use to secure your communications. For starters, you can switch off Google Now on your Android devices as it stores unholy amount of data about you and learns about your search behavior to predict what you want.

The data stored by Google Now includes just about everything, from search history, places you visited, your location, currency exchange rates (if it learns you are in a different country), nearby places, restaurants, and much more. All these factors lead to serious privacy concerns and we are just not sure if Google Now goes through our emails and other conversations to predict the things we want.

Apart from switching off Google Now, other services such as location tracking and GPS can also lead to privacy breaches. There are different anti-tracking / anti-spying GPS gears that you can get to stop from being tracked. However, if you are concerned about your privacy, it's better to leave these services turned off and safeguard your privacy from various threats.

How to Secure Your Cloud Storage

In today's day and age, you can access files, pictures, and almost any kind of data from anywhere thanks to cloud storage services. Having said that, all big cloud storage services like Google Drive, OneDrive, iCloud, and Dropbox are far from being secure.

The hacking of iCloud in August 2014 is just one example among thousands where private data, mainly photographs, of various celebrities were leaked on different websites. This shows the extent to which your data is not safe on cloud storages. So how do you safeguard your information before saving it onto the cloud? Here are some steps you can use to ensure security of your cloud storage.

Use Two Factor Authentication & Password Manager

Let's start from the basic – passwords. They are the key to securing any access points where your confidential data is saved. In order to secure your cloud storage services, we recommend that you use password manager and create different passwords for each cloud service.

In addition to generating strong passwords, using Two-Factor Authentication also strengthens your cloud storage security. What this will do is that it will ask for two queries before allowing you access to your cloud storage account. For instance, you might be asked to enter your password, which in turn sends a security code to your mobile phone that you need to enter for authentication.

Two-Factor Authentication isn't full proof but it does beefs up your cloud storage security. Think of it as adding two layers of security to your system; first you enter the PIN number and then you scan your fingers to access the storage device.

Encrypting Files Manually Before Storing on Cloud

The most secure method to safeguard your personal data on the cloud is by encrypting the files manually before uploading them onto the cloud. This way you can use any cloud storage service of your choice and don't have to worry about all security threats inherent in the cloud service.

Another precaution you can take before uploading the encrypted files is to switch on a VPN so that your entire internet connection is encrypted. For manually encrypting your files before uploading them to the cloud, you can use various tools.

Previously, TrueCrypt was popular file encryption software. However, it has now been discontinued due to various security-related issues. Nonetheless, there are numerous alternatives to TrueCrypt and some of them

include VeraCrypt, AxCrypt, GNU Privacy Guard, BitLocker, 7-Zip, BoxCrypter, DiskCryptor, and many more. Here are our top 3 picks for encrypting files manually:

BitLocker

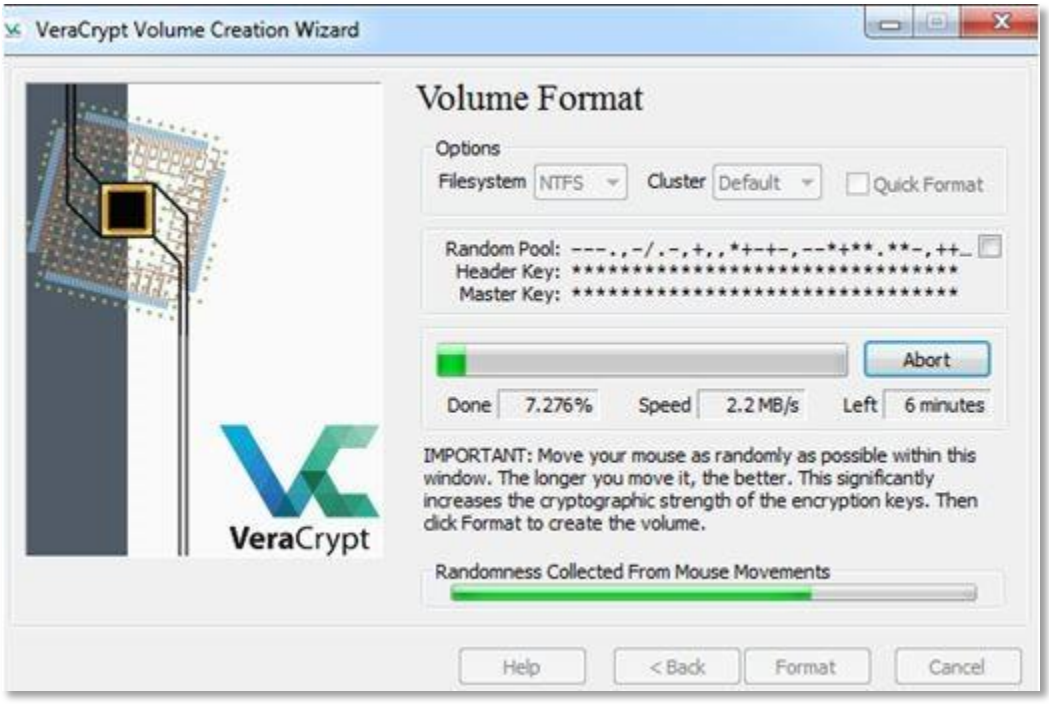
It is full disk encryption software that comes built-in to Windows Vista, Windows 7 (Enterprise and Ultimate), Windows 8.1 (Enterprise and Pro) and Windows Server. BitLocker uses AES encryption (128 bit and 256 bit) for encrypting your files.

BitLocker can also encrypt other virtual devices or volumes of data. You can choose from various mechanisms of authentication such as PINs, traditional passwords, USB key, and TPM (Trusted Platform Module). BitLocker is a great tool for Windows PC users and allows you to safeguard your confidential data.

VeraCrypt

VeraCrypt is nifty free-to-use open-source encryption software and a successor to the discontinued TrueCrypt tool. With VeraCrypt, you can encrypt a certain file, a partition, create virtual encrypted disks within files, or encrypt entire storage devices.

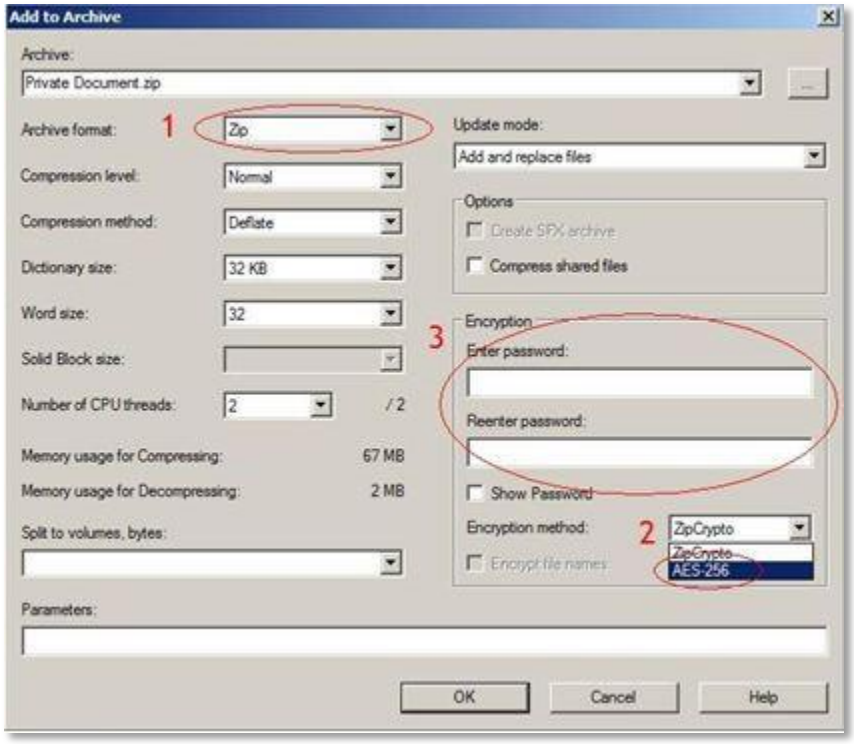
There are different encryption levels you can choose from in VeraCrypt as it supports AES, Serpent, and Twofish encryption ciphers. VeraCrypt solves the security flaws and vulnerabilities that were found in TrueCrypt and allows you to encrypt your files before uploading them on your cloud storage service.



7-Zip

7-Zip (or 7z) is primarily a tool for file archiving and allows you to compress and organize large volumes of files to send over the internet. In addition to this, 7-Zip also encrypts individual files or entire volumes using AES 256 bit encryption levels and is available on Windows, Mac OS X, and Linux.

The 7z software is free to use and its open source nature makes it free from governmental interference. You can safeguard your files via password and they will only decrypt once the correct authentication password is entered. This lightweight file compression/file archiver is excellent at encrypting files and you can use it encrypt your data before storing it onto cloud services.



Check Terms of Service & Privacy Policy of Cloud Service

This may sound like a painstaking task but if you are concerned about your privacy then it's a good idea to go through the privacy policy, terms of service, and other legal agreements of the cloud service. This will reveal the stance your cloud service has on your privacy and security.

There are some services that encrypt your data at server level and have no idea what you are storing on their cloud storage services. On the other hand, there are some services that use fancy terms and reserve the right to access your data whenever they want.

If the terms of service, piracy policy, and other documents do not provide clear indication of your privacy then dig a little deeper and inquire the customer support. Checking such service agreements is a good practice, in our opinion and you should also follow it if data protection and privacy are your top concern.

Use Cloud Services that Automatically Encrypt Files

Now if you are doubtful about using popular cloud services such as iCloud, OneDrive, Google Drive or Dropbox, and are worried about your privacy then there are various alternatives to such cloud services. These alternatives also encrypt your data before you upload them onto cloud.

There are various cloud services that offer encryption as part of the process. Previously, a famous service, Wuala offered file encryption before uploading but now has been discontinued. Nonetheless, here are two cloud services that will safeguard :

- **SpiderOak:** is a versatile cloud service that encrypts your file locally on your computer/ device before uploading them onto the cloud. SpiderOak is available on Windows, Mac, Linux, and also has apps for iOS and Android. SiperOak follows 'Zero-Knowledge' policy where it has no idea what you upload as the files are encrypted on your PC and are protected by a password you set.
- **Tersorit:** is another cloud storage service that encrypts your files locally on your system using AES 256 bit encryption level and requires you to set a password to decrypt your encrypted files. Tersorit offers exclusive apps for Windows, Mac OS X, Android, iOS, and Windows Phone, allowing high flexibility.

Ditch the Cloud & Use BitTorrent Sync

We have touched upon various steps that you can use to secure your cloud storage services and different precautions you should take before uploading. Here is one alternative method you can use to store and transfer files across different platforms without using the cloud, Bitorrent Sync.

Unlike other cloud services, BitTorrent Sync uses a peer-to-peer network rather than cloud servers to store and share your data. One of the main advantages of this is that since your files are not stored on the cloud, no one can access them without your permission. Similarly, you can upload an unlimited amount of data without having to pay a dime.

However, the downsides of this method are that at least one of your systems has to be switched on and connect to the internet so that you can access your files. Also, your ISP bandwidth and data caps can hinder the overall process of storing and transferring files.

So BitTorrent Sync is a clever way of saving data onto other platforms without having to use the cloud. However, we would recommend that you do not think BitTorrent Sync as an alternative to cloud services; rather it should be used in combination and should supplement your cloud storage service.

Countries That Violate Your Privacy

There are different countries with different laws and regulations. Although these regulations are made in the best interest of the people (or what they are portrayed as), many a times countries enforce laws that compromise the privacy of an individual.

Primarily, these regulations are in the form of mandatory data laws and intelligence agencies storing mammoth amounts of user information without their consent.

We touched upon the subject of governmental surveillance earlier and showed how different laws and agencies work in gathering user metadata. Here we will list down some of these countries, how they compromise your privacy, and how you can protect yourself.

Australia

Australia might be famous for many reasons but netizens will remember it for the mandatory data retention law implemented in October 2015. According to this law, your internet activity such as browsing history, IP address, sessions durations, and much more will be recorded by your ISP and telecom services for up to two years.

That's not all! Other aspects of your communication via email or phone will also be stored on the basis of this data retention law. To protect your privacy from this law, you should use a tool that helps you encrypt your internet activity (such as an Australia VPN) and use other tools that encrypt your communication over emails, VoIP services, and cell phones.

China

China has some of the strictest internet censorship laws compared to other countries. Placing regular bans and restrictions on social media channels, China is a place that is not at all friendly towards the internet. With that being said, the online privacy concerns of users in China are not as severe as other nations but anything regarding the Chinese government does not go unheard.

Over the years, many journalists, websites, personal blogs, and social media channels have faced the wrath of the Great Firewall of China. Any criticism of the Chinese government can lead to ban, restrictions and even jail time.

You can use a VPN to safeguard your privacy and encrypt all your internet traffic. However, China has blocked numerous VPN services and you'd have to dig deeper to find the one that are still working in mainland China. One VPN service that works perfectly in China (so far) is ExpressVPN.

USA

The United States does not have a strict data retention law in place. However, the intelligence agencies operating in USA are notorious for spying on US citizens. Thanks to Edward Snowden, the antics of NSA (National Security Agency) were revealed and how they violated one's privacy by collecting metadata.

These agencies have been operating with unimaginable freedom thanks to different laws such as the US Patriot Act and the PRISM program. Although the US Patriot Act has now expired, the bulk data collection of user by various intelligence agencies might never stop.

NSA is one agency brought to the limelight. Other agencies such as FBI, CIA, DHS or DEA may still be conducting unwanted surveillance on US citizens and recording their every move made online. We would recommend that you use a USA VPN for encrypting your online traffic and other encryption tools listed in this guide to protect your privacy against governmental spying.

European Nations

In 2006, the European Union (EU) adopted a new directive called the EU Data Retention Directive (DRD). According to this new data retention framework, members of European Union were required to have their ISPs and telecom companies store the following data of their users/subscribers for a period ranging from 6 months to 2 years:

- Phone numbers of incoming calls and outgoing calls.
- IP addresses of users (location) of the communication.
- Time, date, and duration of the communication.
- The device used for communicating with others.
- Text messages, emails, and phone calls sent and received.

These were some of the major aspects of the Data Retention Directive. Upon request from the court, police and other investigating agencies could have access to other information such as your internet traffic data, the content of phone calls, and invade your privacy on whole new level.

Countries such as Germany, Slovakia, United Kingdom, Italy, France, Norway, Spain, Netherlands, Poland, Sweden, and other EU nations have transposed the directive into their legislation. However, on April 2014, the European Court of Justice declared the directive as invalid on the grounds of interference of right to privacy and protection of personal data.

These countries would have to reevaluate their laws on data retention and formulate new ones that comply with EU Court of Justice. Having said that, your privacy is still at stake and we recommend that you use the encryptions tools to safeguard your privacy as it is not certain whether the government is still recording your data or not.

United Kingdom

Although the United Kingdom (UK) is part of EU and had adopted the Data Retention Directive in the most severe of forms, there are other factors that we need to highlight which compromise your online privacy.

The British intelligence agencies such as GCHQ have been reported to conduct blanket surveillance on UK citizens. The intelligence agency has also been working in collaboration with US counterparts (mainly NSA) and has been sharing user information of all sorts with each other.

If that's not all, UK is part of Five Eye intelligence alliance with USA, Australia, New Zealand, and Canada. This joint alliance between the five nations allows them to have uncontrollable power and spy on one another's citizens, share information with each other, and collect enormous amounts of metadata of netizens. The true picture of this alliance and the extent to which they conduct surveillance was revealed in the documents leaked by Edward Snowden (former NSA contractor).

One way to protect against blanket surveillance is to encrypt all your online activities. A UK VPN helps you to keep all your internet activities protected by encrypting your web traffic; while other tools such as Signal Private Messenger allows you to safeguard your VoIP communications (voice or text).

Russia

The Russian government has been notorious for blocking several social media channels, blogs, websites, and other forms of communication medium. The Russian media watchdog, Roskomnadzor, overseas all modes of communications and is strict in blocking or adding websites to blacklist if anything is spoken against the Russian government, politicians, or the president.

This creates several problems if you are a journalist or a blogger as your online freedom is certainly restricted by a great degree. In the past, many journalists have been prosecuted for raising their voice against Vladimir Putin or the Russian government.

Another factor about Russia that puts your privacy at great harm is the latest data retention law. According to this new legislation, businesses operating in Russia (physically or through websites) are required to store user data on databases located in Russia. This creates a huge problem for tech giants like Facebook or Google and puts your personal privacy in grave danger.

Canada

Since Canada is part of the Five Eye alliance, your privacy is less than secure. Like we discussed earlier, the Five Eye nations conduct unwanted surveillance on citizens and share your private information with each other.

Similarly, there are certain laws implemented in Canada that also violate your online privacy. For starters, the Bill C-51 gives governmental agencies like CSIS or the police unprecedented power to share user information; this, in turn, gives a further boost to Five Eye alliance.

If this wasn't enough, the Canadian government now requires all ISPs and telecom companies to keep logs of user's activities and report any activity that leads to infringement of copyright laws. This is a big problem for Canadian based VPN services like TunnelBear. However, a VPN still remains as one of the solutions for securing your online privacy as it encrypts your internet traffic.

Enhance The Use Of Antivirus, Firewall and Anti-Malware

We have discussed numerous security and privacy threats so far in our privacy guide and how you can protect yourself against them. But we cannot leave out the significance of using antivirus, firewalls, and anti-malware.

These three programs form an important security barrier that will protect you from various threats. Online threats such as viruses, malware, hacking, spyware, adware, Trojan horses, and others alike can lead to serious problems such as destroying data, stealing and leaking confidential data, hindering you from accessing your own files, and ultimately disabling your computer.

This is why it is important that you use antivirus software along with firewall and anti-malware programs. Here we will show you how to enhance the use of antivirus, firewalls, and anti-malware to boost your defenses against such online privacy threats.

Antivirus Software

Many viruses infect your device and then spread throughout the system by making copies of themselves. Although many of them may be harmless, other viruses are really dangerous as they are designed to steal your data, slow down your computer, allow spammers to infiltrate your system, delete important files, and even crash your systems.

Antivirus software is designed to protect you against different viruses. It scans your system regularly and looks for patterns and programs that are dangerous to your device. Antivirus utilizes specific signatures or definitions of known viruses to signal them out.

This is why companies that develop antivirus software continuously release updates for virus definitions. Here we would also advise you to always keep your antivirus software up to date and perhaps change the settings to update automatically. And, if you don’t have an antivirus by now then you should get one right away.

Free Antivirus vs. Premium Antivirus Software

Choosing an antivirus can be tricky, considering the host choices that available to you in the market. Each provides the basic antivirus service but can be differentiated in terms of price, performance, and features. However, it all comes down to whether you go for a free antivirus service or get a paid one.

The general notion is that free antivirus services are just as good as premium antivirus services. The main difference between paid and free lies in the additional features offered to you by a premium antivirus software.

Free antivirus software will provide the same virus detection and protection features as a commercial antivirus but will lack in other characteristics such as anti-theft option, additional firewall, anti-spam feature, phishing filters, and more. On the other hand, a paid antivirus works more like a security suit and you get all these additional features for a certain price.

Top Antivirus Services

Now that we have cleared up the difference between free and paid antivirus services, you can consider these antivirus providers (free & paid):

- **AVG** is available for free and also as paid service. The free service offers basic antivirus features; protection for your Mac and Android devices, remote protection feature, and also scans the web, Twitter and Facebook for malicious links. The paid service offers more additional benefits such as a firewall, anti-spam feature, data protection and more.
- **Avast** is another free to use antivirus service and is available on Windows, Mac, Android and iOS devices. The free version will provide you with antivirus service, a password manager feature, and browser protection. Apart from the free version, Avast also offers a variety of paid services as well. You can choose from a complete security suite to individual add-ons.
- **Norton Security** by Symantec has been a long-running service in the antivirus industry. The Norton Security suite is a paid service and you can choose from its different variants, depending on the features you want.
- **Kaspersky** is also a renowned commercial antivirus service and offers different packages. You can purchase the standalone antivirus service or go for the total security package.

Firewalls

Firewalls are a program that monitors the data traffic entering and leaving your system. You can configure the firewalls to prevent data from leaving or entering your devices based on a different set of rules.

Firewalls are really important when it comes to defending against cyber criminals such as hackers. They block all forms of communications that originate from unwanted sources and stops hackers from identifying you over the internet.

All the latest operating systems have built-in firewalls and it's a good practice to leave them turned 'On'. Alternatively, there are third party firewalls that you can use such as Comodo Internet Security Pro or various antivirus security suits also include a firewall add-on.

Anti-Malware

There are numerous cyber threats that sneak into your device and can be very destructive. Threats such as adware, spyware, Trojan horses, and even viruses can be categorized under malware and will compromise your privacy. Since antivirus software protects you from various viruses, it is also important to protect against spyware and Trojan horses as well.

An anti-malware program provides you protection against all such threats. Although security suites have features that protect you against malware, it is a good idea to run independent anti-malware (anti-spyware) software alongside your antivirus.

If you are a Windows 7 or higher users, then Windows Defender scans your PC for any signs of spyware and other malware programs. However, you can also use free anti-malware programs such as Malwarebytes or Spybot Search & Destroy.

Use Antivirus, Firewalls, & Anti-Malware in Combination

When we said that these three programs form an important security barrier, we weren't just kidding around. When all three of them are used alongside each other, they form a formidable partnership and complement each other.

Each one of them is designed for a specific purpose and they overcome the weaknesses or vulnerabilities of each other. When you have configured them on the highest level of protection, an antivirus, firewall, and anti-malware will protect you from threats that are designed to inflict damage to your online privacy and security.

Just remember not to run two antiviruses at the same time on one system as both might contradict each other and leave you vulnerable. On the other hand, some security experts have even stated that running two or three anti-malware software is a good idea as no one anti-malware program is sufficient to track all the security threats.

Tips and Tricks For Online Privacy

Heart Bleed Bug

The heart bleed bug is a major vulnerability that can be exploited by hackers to attack any connected client or server to steal data, allowing them to expose any encrypted content, username/password or private keys. It gets its name from the flaw found in the heartbeat extension of OpenSSL implementations.

It was caused by poorly written code and exists on all versions of OpenSSL which were released between March 2012 and April 2014. Considering that up to 66% of all websites have OpenSSL encryption, it can be considered one of the worst security bugs in IT history. Since the attacks exploiting this bug do not leave any trace, the extent of data being stolen remains unclear. There has been some discussion of scraping OpenSSL altogether in favor of biometric techniques.

To protect against this vulnerability, it is recommended for businesses to upgrade to the latest version of OpenSSL encryption on their websites. The associated OpenSSL certificate should also be reissued with new keys. Internet users are recommended to change the passwords that they have for OpenSSL implemented websites. Those engaged in online banking should keep a close eye on their financial transactions.

Whonix

Whonix is a Linux Distribution which has been designed with the aim of providing maximum privacy, anonymity, and security on the internet. Whonix is a distribution of two virtual machines, a “gateway” which solely runs TOR and “workstation” which is a completely isolated network. It runs on other operating systems using a supported virtualizations engine such as “Virtual Box”.

Pros

Since it achieves its purpose by forcing all communications through the TOR network (gateway), there are certain advantages of using Whonix:

- You remain anonymous as your real IP address is hidden.
- Prevent DNS leaks and provide maximum protection against malware.
- It is compatible with any software package, being able to work in conjunction with VPN.
- It prevents misconfigured applications from leaking your real external IP.

Cons

Whonix does have its own set of drawbacks.

- Since it utilizes the TOR network, your internet speeds can be compromised considerably.
- Compared to other examples of Linux distributions, a higher level of maintenance is required.
- It uses up extra resources since it needs virtual machines or spare hardware to work.

Switch to Linux Operating System

Many users concerned about their privacy can make a switch to Linux as it has a number of advantages over other major operating systems in terms of online security and privacy.

- One of the most crucial advantages of Linux is that anyone cannot run any file or program without having administrator rights, including access to the root files of the OS. This means that in the event of viruses, spyware or hackers compromising the system, they will be unable to cause irreversible damage to the system.
- Currently, Linux has a market share of 1.71% compared to 88.8% for Windows and 7.6% for Mac. Having a small market share compared to Mac OS and Windows makes it a less attractive target for carrying out malicious attacks and is rarely the subject of attack by cyber criminals.
- Being an open source OS, Linux is free from tampering by governmental agencies and the chances of a NSA back door are highly unlikely.
- Another benefit of its open source nature is that countless users can see its code, quickly point out any exploits or flaws and fix them. This minimizes any chances of malware being hidden inside codes; also the security fixes arrive much quicker on Linux compared to other OS.

All in all, this makes it more secure compared to many other commercial operating systems but even Linux's cyber security is not impenetrable. Users can boost their privacy protection on Linux even more by enabling a firewall (if disabled), restricting the use of root privileges, installing a VPN and keeping the software up-to-date.

Some concerned readers might be reluctant to make the switch to Linux as they might have a use for their existing operating systems but they don't need to switch out entirely. With the use of a virtual machine (explained earlier), one can use Linux within another operating system.

Use Librem Laptops Running Qubes OS

Ever wondered if there were any laptops that use open source software and hardware, and are built solely for protecting your privacy and security? Purism provides just that with its Librem notebooks. Currently, they offer two models, Librem 13 and Librem 15.

Both are high end laptops and are built with one thing in mind, to provide you top-notch privacy and security from various threats originating from different sources. From the hardware to software used in Librem notebooks, privacy is a paramount feature.

Purism's philosophy states that it prioritizes privacy, security, and freedom; and it would only use open source hardware or software that don't violate a users right to privacy. Both the laptops come with a built-in operating system developed by Purism, called PureOS. This OS uses open source software and comes with popular Windows and Mac software preinstalled.

Qubes OS

However, if you want to take your privacy and security to another level then we recommend that you step up Qubes OS on your Librem laptops. Qubes OS is a security focused operating system and is built upon Xen hypervisor.

Qubes provides security and privacy through isolation; it separates your digital lives by running these operations on virtual machines. One thing that sets Qubes OS apart from other operating systems is that the OS assumes that your system will be breached. In doing so, it classifies different subsystems and prevents any cyber-goon from gaining full access to your system.

Qubes is supported by different virtual machines. Some of these include Fedora and Debian Linux VM, Whonix, and Windows Microsoft virtual machines. Having said that, one problem that users face while using

Qubes is to find the correct hardware support for the OS. Since virtualization takes up a lot of resources, you would need processors that support virtualization (Intel VT-x or AMD-v), considerable hard disk space, and plenty of RAM to make full use of Qubes OS.

Protect your BIOS with Password

While most operating systems can prevent unauthorized users from logging into them, they can't prevent them from booting other operating systems, formatting the hard drives or using a live CD for viewing your personal data.

On your computer's BIOS, you can set up a password to prevent such outcomes from happening without your permission. To set up a BIOS password on your computer, you will need to do the following:

- Start your computer, during the boot-up process, press the appropriate key. On most computers it is F2, otherwise, you can view the computer's documentation or do a quick Google search on the "BIOS KEY" of your computer model.
- Once on the BIOS settings screen, locate the password option, usually found in the security section.
- There configure your password settings according to your preference and enter your password.
- You can set different passwords for different purposes e.g. one for booting up the computer and one for accessing your BIOS settings.

CAUTION: A word of warning though, once you have set up a password on your BIOS, it can be hard to reset it, especially on a laptop. Information on how to set up reset a BIOS password can be found here.

On Windows 8 and Mac Computers

On a computer running Windows 8 and Macs, UEFI firmware is used instead of BIOS. You can head over to the Windows 8 boot option where you will find UEFI firmware settings where you can set up the password. To access the settings on Windows 8, either swipe in from the right edge of the screen or press the Windows key + C. Then click on the power button and from the options, click restart while holding shift.

On Mac, you can reboot the system and hold Command + R to enter Recovery mode. Once there, go to 'Utilities' –> 'Firmware Password' and set up your password.

Note that a BIOS or UEFI firmware password will protect your computer from accessing your hard drives through the interface, there is still the risk of a person using his physical access to your computer and changing your password or removing or inserting a hard drive. Therefore we recommend also encrypting your hard drive as well to ensure maximum protection.

DNS Servers

DNS (Domain Name system) server is required for linking you up to the right location or website on the internet. Most people use the DNS server provided by their ISP or a free public DNS such as Google DNS. However, doing so compromises your privacy as your DNS service provider can track and monitor your online activity. The stored information can then be used for targeted advertisement.

Even with a VPN connection, DNS leaks can still occur. To ensure maximum privacy protection, we recommend switching to OpenDNS servers and using DNS encrypting tools alongside a VPN. DNSCrypt is one such tool, available on the Windows, Ma, and Linux platforms. DNSCrypt is open source software that can be directly downloaded from the Open DNS's Website.

Alternatively, you can search for VPN clients with built-in DNS leak protection and set one up. Popular VPN with this feature include PureVPN and Private Internet Access(PIA).

Check Flash Player Settings

To protect your online privacy, you need to control the permissions and access to personal data you give to websites you visit. You can go to your Flash player settings to do so. By far, the most widely used flash player is the Adobe Flash Player.

To configure your Flash player setting, go to the official website where you will find the Adobe Flash Player Manager. The manager comprises seven tabs, six of which controls a different aspect of your privacy and security. Each of them is mentioned below with a recommendation on the best settings.

Global Privacy Setting

This controls the permission for websites to use your camera or microphone.

Recommendation: Select “Always ask” as you may require some sites to use your peripherals for tasks such as video calling or voice command.

Global Storage Settings

This controls how much space will be allocated to cookies and other flash content on your computer from unvisited websites. Storing content from third parties can be risky in terms of online privacy as it can allow websites to keep tabs on your information or monitor your activity.

Recommendation: Configure the settings as shown in the screenshot. Denying the storage of cookies may impair the functionality of some websites but this is rare. The best advice is to experiment with the settings, going from the most restrictive options to slightly less if you encounter broken websites.

Global Security Settings

This controls whether flash content using an older security rules (Content created before Flash 8) can interact the internet or not.

Recommendation: The best choice is to select “Always ask”. This way you will not have to compromise between security and functionality. In case of websites that you can trust and are secure, you can list them as exceptions in the section at the bottom.

Website Privacy Settings

This controls the access privileges visited websites have. You can configure these privileges for each individual website here, allowing you to restrict access from less trustworthy websites.

Website Privacy Settings panel

Recommendation: The preference it up to you. It is best to select ”Always ask” for most websites, only selecting the second options for websites you trust and visit regularly.

Website Storage Settings

This allows you to micro-manage the amount of flash content like cookies that can be stored on your computer by individual websites you have visited.

Website Storage Settings panel

Recommendation: Use this panel to set the limit to 100 KB only for trusted websites that cannot function properly without storing flash content.

How to Generate Strong Passwords

We have pondered upon using strong passwords throughout our privacy guide and here are some tips you can use to generate strong passwords. Passwords ensure that only the authorized individual is able to access their accounts. Users should make sure they have strong passwords that do not get easily cracked by hackers trying to break-in to their account. A strong password should have:

- **A minimum of 12 characters**: the longer the password, the harder it is to crack using brute force attack.
- **Should include numbers, symbols, capital letters and lower case-letters:** using a combination of different types of characters will make it harder to crack by brute force attacks.
- **Should NOT be a word found in the dictionary or a combination of them:** avoid using easy to guess common words found in the dictionary e.g. Blue Dinosaur as a password is not safe.
- **Must not depend on obvious substitutions:** g. using “Blue Dino$aur” instead isn’t going to make it any safer.
- **Use a phrase as password:** you can use phrases or short sentences as your passwords. This is an effective method of ensuring strong password as phrases are more difficult to crack.
- **Add random spaces:** you can also add random spaces in between your passwords (if allowed). This minimizes the chances of your password being cracked and helps to ensure its strength.
- **Avoid using the same password for multiple accounts**: This will ensure that if one of your account get’s compromised by hackers, they will not be able to log in to your other accounts using the same password.

Password Manager

A problem of making strong passwords is that they can be hard to remember. Solve this problem by making use of a *password manager* which will allow you to store and organize strong passwords. With the help of a password manager, you only need on 'master password' which in turn allows you access to your entire password database. Here are some password managers that you can use:

- **Dashlane**: A powerful password manager with a sleek interface. Dashlane offers free as well as paid service and you can automatically change the password of different websites. It generates strong passwords and other features include advance form filling and receipt capture for online shopping.
- **LastPass 4.0:** is another great password manager and is available for free. You can also select the premium version. Some of its features include such as the ability to sync passwords across different devices, automated and enhanced password sharing, audits passwords with a security challenge.
- **LogMeOnce Password Management Suite:** A free password manager offering a range of great features. Some of them include stolen device tracking, automated password changing and secure sharing.
- **KeePass:** Here is a free password manager for Windows that you can use. It is open source software and protects your passwords using 256 bit AES or Twofish encryption algorithm. You can even carry KeePass on USB stick and run it on other Windows system without the need for installation.
- **KeePassX:** KeePassX is an unofficial version of KeePass but offers far more features. Firstly, you can use KeePassX across different platforms (Windows, Mac, Linux, etc.). It also has a password generator and also uses 256 bit AES or Twofish encryption algorithm.

Conclusion

Now that we have come to an end, we hope that our guide will help you secure your privacy and security against numerous threats on different platforms. Privacy is one thing no individual should take for granted or compromise on.

Protecting your online privacy and security might look like a daunting task but it is not impossible. We have tried our best to lay things out as easy as possible and help you set up defenses for safeguarding your privacy.

Using the various tools, following basic security guidelines, and paying attention to smallest of privacy details, you can easily minimize any chances of being attacked by cybercriminals, governmental surveillance, and various other privacy and online security threats.

Lastly, do give us your feedback and suggestions for improvement in the comments below. Also, if you have any query regarding your online privacy and security, do let us know, we will be delighted to help you!