On Loc

A Guide for Using
Secure Platforms

Contents

Why Use Secure and Encrypted Services?

As the information age thrusts towards more dystopian realities, the world wide web as we know it has become increasingly monopolized by Internet tech giants and interwoven into governmental systems of mass surveillance and social control. Facebook, Google, and related services not only track user activities, but also track private messages, search histories, ip addresses, location information, device information, and very often provide this information to advertisers. law enforcement, federal agents, and intelligence agencies.

While this climate affects all users, it presents very specific challenges for revolutionaries. The accessibility of private data can compromise communications, sabotage operations, and put comrades in very serious danger. Where COINTELPRO and related intelligence programs left a legacy of violence that destroyed the Black movements of the Sixties, the state repression of today has reached such levels that it must be assumed everyone engaged in revolutionary work is being monitored by the state at any given time.

What are Encrypted Services?

Encrypted services are services that protect sensitive data by scrambling messages and texts so that only trusted recipients are able to see it. Many different messaging apps, email providers, web pages, and browser plug-ins use encryption, Likewise, a VPN or "Virtual Private Network" is a way to encrypt your IP address, network traffic, and browsing history. For maximum privacy it is best to make use of both encrypted applications as well as VPNs.

The following is a guide for some specific tools and apps you can use to increase your operational and personal security. Keep in mind that the specific services named in this zine are safe for use only at the time of this zines publication. Very often, secure services that used to be safe become compromised due to program vulnerabilities or pressure from government actors to cooperate with intelligence investigations. Always research the service thoroughly before using to ensure that it has not been compromised.

What to Look for in a Secure Service

With so many options out there choosing the right secure service for you can be overwhelming. Before you make your decisions you should first evaluate your own security needs based on the level of privacy required for your activities. The following is a general check list for what to look for to ensure you choose the most secure option possible.

✓ Full End-to-End Encryption:

Anything that is secure has to have encryption. However, there are different kinds of encryption and some kinds are less secure than others. In addition, some secure software only encrypts a portion of your data, leaving metadata such as your IP address unprotected. End-to-end encryption means that communications between your device and websites, email addresses, and other devices are encrypted from source to destination. Full end-to-end means that the majority of your data is being encrypted, including metadata.

✓ Perfect Forward Secrecy:

Perfect forward secrecy is a way of encrypting that increases security by making it even more difficult for the encryption to be decoded. This is important because encryption can still be cracked by experienced hackers through the use of whats called decryption keys (although it is not easy to do). What perfect forward secrecy does is constantly change encryption keys so that if an encryption key is somehow decrypted it will not compromise your data as a whole.

✓ Open Source:

Any privacy company can claim that their service is secure but unless it is open sourced there is no way of knowing for sure. Open source means that the service is publicly transparent about its privacy practices and shares the coding it uses with the public to be audited by coding experts. This not only establishes that the company is trustworthy, but by sharing its coding publicly it also helps make the software better by giving experts the opportunity to point out possible flaws in the coding that can be patched up and improved upon. A service that is not open sourced cannot be taken on its word that it is truly secure and could be full of coding vulnerabilities.

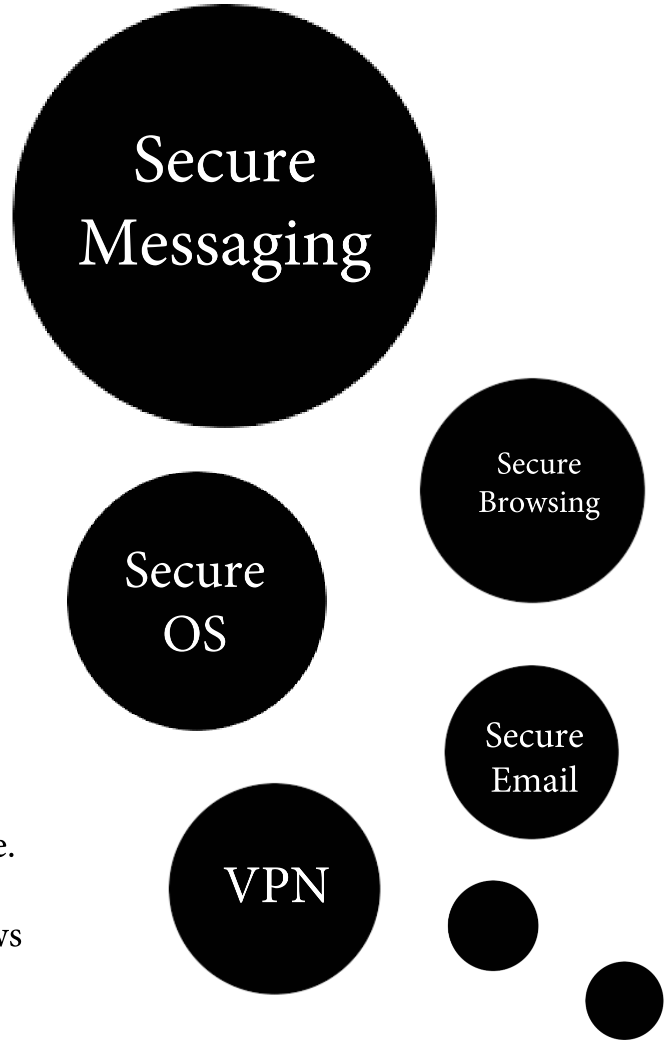
Taking a Blended, Decentralized Approach

The highest levels of security and privacy are best achieved by combining all of the different types of privacy tools discussed in this zine. For example, if you wanted to be as secure as possible while browsing the internet you might make use of a secure browser like Tor while using a VPN, while using a secure operating system like Tails. While you were on the internet you might use a secure email provider like Posteo if you were sending an email. Maybe you had to search something and used Duck Duck Go. Or maybe you used Jitsi Meet for a secure online conference meeting. These combinations blend different secure services together in ways that increase your privacy and anonymity.

When information is centralized in one place it is the easiest to target and surveillance. This is why, when cultivating a operational security culture, it is important to think in decentralized ways. Not only should we blend different kinds of secure services together, but we should also make use of multiple privacy tools that function in similar ways so that we diversify our usage.

Employing a multitude of different and similar secure services allow us to also organize our communications and activities based on varying levels of sensitivity. For example, perhaps you are using Wickr for a very specific project where it is better to be anonymous, but are also using Signal for more regular communication. Your use of both mean you are not discussing things on Signal that you are discussing on Wickr. Decentralizing our communications, and diversifying the secure services we use help keep our information and activities from being concentrated in one place and allows for flexibility if one or more of the services we use becomes compromised.

The landscape of mass surveillance is such that any secure service, no matter how repeatable, can succumb to federal, financial, or malicious pressures and become compromised at any given point in time. Because of this, an important part of operational security is always staying up to date on the latest news about system vulnerabilities and changes, including changes in service ownership and location. The secure services mentioned in this zine are only secure at the time of this zine's publication.



Secure Operating Systems

Your operating system (OS) is the system interface you use when you boot up your computer and provides the basic scaffolding that enables you to run programs, access the internet, and more. Everyday examples of OS are Windows 10, and Mac. Generally speaking the most popular operating systems are not geared towards privacy and can still be a security risk. Windows OS has been known to collect massive amounts of data and sends that data to Microsoft for diagnostics and other uses. Mac, although slightly more secure than Windows, is not open-sourced and its high level of device integration means that data is constantly being shared between macOS, your Iphone, and other Apple products, making it more vulnerable. Secure operating systems are ones specifically created for privacy, encrypting data that is stored on the OS, blocking tracking, and not logging data. For extremely sensitive activities a secure OS provides extra layers of protection when used in conjunction with a VPN and other privacy tools.

Tails

Tails is a portable, secure operating system that lives on a USB drive. When plugged into your computer, it temporary replaces your regular operating system, allowing for secure and encrypted computer use. To use Tails, you first have to shut your computer down while the USB is plugged into your computer. When you boot your computer back up, Tails OS will start instead of Windows, macOS, or Linux.

Tails boats a ton of useful privacy features, including encrypted Tor browsing by default, uBlock ad-blocker, Persistent Storage to encrypt stored data, and automatic memory deletion after shut down. It even has its own office suite. It is open-source and well-audited.

Oubes

Qubes is a permanent operating system you can install on your computer that maintains your privacy by isolating programs into compartments on your computer called "qubes." These qubes are organized by threat-level and compartmentalized so that if one program is compromised it does not compromise your computer. Qubes is Tor compatible and open-source.

Anonymity:

Anonymity in this context means that you can use the service without having to provide any personal information such as your email address or phone number that could make you readily identifiable. For example, some secure messaging apps require users to provide their real phone number. In some cases a burner number or front email address can be used to maintain anonymity. But generally speaking it is always best to choose a secure platform that does not ask for personal information so that you can use the application anonymously.

No Tracking:

The whole point of using secure platforms is to avoid being tracked. If the secure service you are using is tracking you it defeats the purpose. Information that is gathered from tracking your activities can be used against you when that information is leaked or turned over to law enforcement agencies. There is no reason why a secure platform should track its users.

No Logging:

User data is often saved on servers temporarily or permanently and can contain sensitive information about your activities. For this reason it is important to choose a secure service that has a no-logging policy. A secure service that logs your data is putting you at risk in the event that the service becomes compromised. A service that has no stored data has nothing to offer authorities and nothing to leak in the event of a data breach.

Based in a Country Without Information Sharing Agreements:

The country that the service is based in is an important factor to consider when choosing a secure platform. Many countries have information sharing agreements with other countries that oblige them to cooperate with foreign investigations and put pressure on privacy companies to hand over user data. The most notorious among these is whats known as the Five Eyes Alliance, an international surveillance network made up of the US, Canada, the United Kingdom, Australia, and New Zealand. They make up the core of two larger surveillance networks called the "Nine Eye Alliance" which includes Denmark, France, Holland, and Norway and the "Fourteen Eye Alliance" which in addition includes Germany, Belgium, Italy, Sweden, and Spain. It is best practice to avoid any privacy companies who's base of operations is located in these countries.

More on the Five Eyes Alliance

The Five Eyes Alliance was founded in the Cold War era originally as the UKUSA agreement signed in 1946, a multilateral agreement between the US and UK to monitor and share information with each other on suspected communists within their boarders. This played itself out in the close collaboration of national intelligence agencies. In the late 1950s Canada, Australia, New Zealand joined the alliance forming the original five country network. Later, the Nine Eyes and Fourteen Eyes Alliances were formed, which are essentially extensions of the original five country network. There is also the Forty-One Eyes Alliance, which includes all of these countries with the addition of the allied coalition in Afghanistan.

These information sharing arrangements were kept from the public for over half a century and the nature of these arrangements are still shrouded in secret. What is known is that these alliances have grown a far-reaching global surveillance network where intelligence agencies from different countries collect, analyze, decrypt, and exchange the personal information of individuals. That means that foreign intelligence organizations might already have information about you that was shared with them via these alliances. Its been known that agencies within the Five Eyes network have deep collaborative relationships, with cross-pollination even on the level of staffing and programs.

Five Eyes and related alliances have joint intelligence programs, one of the most horrifying being a program called ECHELON. ECHELON was originally developed to collect Soviet satellite communications by using ground-based signal stations and has since been expanded to intercept and monitor signal communication traffic coming from phone, email, and internet. In the year 2000 it was revealed ECHELON systems were used by UK Prime Ministers to spy on civilians and that the use of ECHELON bypasses domestic privacy laws.

The Five Eyes and related information sharing networks generally operate outside of domestic and international law. They do not fall under the jurisdiction of domestic legislation and these agreements remain completely unregulated by any international governing body, operate with no oversight, and no protections from privacy abuses. Because their operations are still kept in secret, oversight is made even more difficult, with much of the general public not knowing that these agreements exist, or if they do, have very little information about them. The secrecy and lack of regulation have allowed unbridled and far-reaching surveillance activities that we may never fully know.

Secure Video Conference Services

Video conferencing applications such as Zoom have been notoriously unsecure, have stored vast quantities of user data, readily provide that data to third parties, and are susceptible to information breaches. Skype and Microsoft based apps such as Teams aren't any better, and Google based apps such as Google Hangouts/Google Meet are integrated into the Google surveillance and data collecting apparatus. Secure video conferencing services encrypt your video conference data for two way and group conference calls and do not log your user data. A strong secure video conference option will be open-source and also not require personal information such as an email or phone number to use it.

Jitsi Meet

Jitsi is a secure, open-source video conference platform that is free, fully encrypted, and anonymous. It has the basic features of a video conference app, including encrypted message chats, and video recording, and similar to Zoom, generates a URL link for each meeting. A password can be enabled to protect entry into the meeting and is generally recommended.

Jitsi does not require any personal information to use the service, allowing it to be used anonymously. Minimum maintenance-related data is stored by Jitsi temporarily to improve the service but this is mitigated by the anonymity involved in using the service. Its anonymity also helps make up for the fact that it is based in the US.

Element

Element is a chatroom and chat channel application based in the UK that runs on a decentralized network and has optional built-in encryption. Although encryption is not default on Element, one of the best things about it is that you can use the app anonymously.

The only thing required to use Element is an email address, which you can easily control. The best way to register with Element is to use one of your secure email addresses you created with a secure email service such as Posteo or Tutanota. Element is open sourced and its encryption uses perfect forward secrecy. Its channel and chat room interface allow for more dynamic chat functions.

Because encryption is only a featured option and not the default, Element does not encrypt metadata or other information outside of its encrypted messaging chats. It also does not have self-destructing messages. For these reasons Element is less secure than Signal but still a great option for low-security communication that maintains user anonymity.

Wickr

Wickr is another strong alternative that couples secure full end-to-end encryption with anonymity. You do not need a phone number nor email address to use Wickr, keeping your identity safe. Encryption is by default in Wickr, and unlike other apps that have disappearing messages as a setting option, the messages you send in Wickr will automatic disappear and self-destruct by default.

The shredder feature completely destroys all conversations and files shared on the platform. Wickr does not log any user data or metadata. Wickr also bills itself as one of the most secure collaboration platforms, it being one of the only apps that actually supports end-to-end encrypted group chats and conference calls.

One of the only downsides to Wickr is that it is not fully open-sourced though some of its coding has been shared publicly. It is also based in the United States which presents some security concerns. However, because of Wickr's anonymity, ephemeral messages, and no-log policy, there is likely not very much data for the U.S. government to obtain.

Secure Search Engine Services

Google is notorious for collecting user data and profiling user habits to generate ad revenue. According to a 2018 study on Google's data collection practices, ad revenue generated from the profiling of user data accounted for 86% of Google's total revenue. Google follows and tracks your activity on over three million other websites. Google devices such as Android and Google Home are designed to collect even more data and apps such as Google Maps and Chrome were shown to collect data even while running in the background of most devices. Over a third of the data collected by Google was location data, with the average Android phone sending location data back to Google servers 340 times within a 24 hour period. Google saves and stores your Google searches forever as well as any other data it has obtained by tracking you including location data.

Although it is nearly impossible to fully escape the reach of Google, one of the first steps in moving towards more secure practices is cutting your usage of Google search and other Google products and devices.

Duck Duck Go

Duck Duck Go is a secure alternative search engine that does not track user search history, record your IP address, nor uses cookies. It also prevents a phenomenon called search leakage, (which happens when information about your search is sent to the website you click on in the search results), by redirecting that information so that it is not shared with outside websites. Duck Duck Go also has an encrypted feature that further protects your search.

It is perhaps the best secure search engine options out there and pairs excellently with Tor browser, enabling end to end anonymous and encrypted searching when Tor and Duck Duck Go are used together. Other private search engines such as StartPage might also refrain from tracking and storing your data but have less features, many do not have encryption, and do not prevent search leakage.

Secure Browsing Services

You are constantly being tracked by companies and advertisers wherever you go on the open web and because browsing history is often collected and stored by third parties, it is very important that you have some way of browsing that is secure. Section 215 of the Patriot Act passed during the aftermath of the 9/11 attacks in the United States allows state and federal law enforcement to look at your browsing history without a warrant. Web browsing service providers as well as third party companies that collect and store user data are obligated to comply with government requests for data and are legally prohibited from disclosing the details of these requests.

It should go without saying that Google Chrome is one of the least secure browsers you could use, as Google not only proactively gathers and stores very sensitive user data including location data across its products and platforms, but also readily complies with governments to give up that information when requested. Internet Explorer is even worse, mostly due to the very serious coding vulnerabilities that open the browser to malware and attacks by hackers. One of the best options for a default browser is actually Mozilla Firefox because of the plug-ins that are available that can make the browser more secure.

HTTPS Everywhere

HTTPS Everywhere is a Firefox plug-in that encrypts your browsing by using the HTTPS script in the URL of the websites you are visiting. HTTPS is basically the same technology used when you are being asked to provide sensitive information such as a credit card number on the payment page of a website and is symbolized by a lock at the top left hand corner of the URL to indicate the page is secure. HTTPS Everywhere turns every web page you visit into one of those secure pages.

The only downside is that a website must be able to support HTTPS in order for it to work. Most major websites do support HTTPS however, and issues are only likely to occur if you are visiting obscure or dated websites that do not have HTTPS capabilities. For browsing on the surface web, an updated Firefox browser with a HTTPS Everywhere plug-in is one of the best options for use aside from Tor.

Secure Messaging Services

Secure messaging services allow you to send private encrypted messages to recipients and some offer features such as disappearing messages and message deletion. When choosing a secure messaging service it is important to make sure it does not log any user data. End-to-end encryption should be a default on the application you are using since a lot of messaging apps only offer encryption as a setting option. The encryption should be fully applied, meaning not only are the messages encrypted, but also mobile numbers, user names, and metadata. It is also good for the app to be open-sourced. Like VPN and email services, apps that are based outside of the United States do add another level of security, however at the time of this zine's publication most of the more reliable secure messaging apps are based in the US. As long as the app does not log any data the security risks of being based in the U.S. are minimal. Never use Whatsapp for security as it is owned by Facebook and has had serious data breaches in the past.

Signal

Signal remains the gold standard for secure messaging. According to NordVPN, Signal's encryption protocol is now recognized as the most secure messaging app protocol out there. It uses perfect forward secrecy to protect encrypted messages by frequently switching encryption keys. In Signal, end-to-end encryption happens by default and is fully applied to metadata and other information including your attachment files.

It is completely open-sourced and well-audited. Signal also offers some handy features as well such as timers, self destructing messages, and disappearing messages. Signal does not collect personal information with one exception: it collects your phone number. The only main drawback of Signal is that you must provide a valid phone number in order to use it, meaning you cannot use it anonymously. People who you communicate with on Signal are generally able to see your phone number and Signal uses your phone number to identify your account. To solve this you can use a burner number for your Signal account. Signal is also based in the U.S. adding another dowside.

Secure Email Services

Secure email services use encryption to protect you email correspondence. Some services out there are free while others cost money, and although paid services might offer more features, there are some strong free options out there. When choosing a secure email provider it must always have end-to-end encryption. And similarly with VPNs, it becomes important for the provider to have a no-log policy and to be based outside of the United States in a country that does not freely share private information with foreign governments. Having an email address with a secure email provider can be extremely important when registering for other secure services that ask for your email address. It is always best practice to use your secure email for security-related things including registering for other secure services. Never use your personal email.

Posteo

Posteo is a paid open-source email service that has end-to-end encryption, spam blocker, no tracking, and a no-log policy so it will not store any of your user data.

It uses perfect forward secrecy to protect metadata and goes the extra mile by using IP stripping to remove your IP address from outgoing emails. Posteo also does not ask for any personal information such as a name, address, or back-up email in order to use it, allowing for a level of anonymity. Based in Germany, it is subject to Germany's information sharing agreements. However, because of its anonymity, no logging policy, and focus on encrypting metadata, this issue is easily mitigated. This was proven in 2013 when authorities tried to extract the identity of a Posteo account holder and failed.

Tutanota

Tutanota is a secure email service that offers both a free and paid plan. Tutanota is fully open-source, uses end-to-end encryption, perfect forward secrecy, and also has IP stripping. It offers a fully encrypted email calender and an alias feature that allows you to create multiple email aliases. It does not ask for personal information, providing anonymity. The downsides are that it does not secure metadata. Also, it logs user data for a period of 7 days and then deletes it.

The service is based in Germany, which has information sharing agreements. The anonymity somewhat makes up for this if not for its temporary logging and lack of metadata protection.

Duck Duck Go Privacy Plug-in for Firefox

Duck Duck Go also has a plug-in available for Firefox that not only sets Duck Duck Go as your default search engine but also has a few other useful features including tracker blocking, web page encryption, and the Privacy at a Glance feature that allows you to view whether a website you are visiting can be trusted or not. The plug-in will force websites you visit to use encryption if it is available, and similar to HTTPS Everywhere, the encryption will not work on obscure or dated websites. For mobile browsing Duck Duck Go also has a fully encrypted mobile browser available for IPhone and Android.

Tor

Tor is a web browser and private network that allows you to access the web anonymously through a series of routing and rerouting pathways that fully encrypts and obscures your personal IP address. Tor has been so effective at preserving anonymity that it is one of the only browsers used to access the "Dark Web," the hidden part of the Internet where illegal activities occur.

Before installing and using Tor it is important to have adequate virus protection, especially if you plan to use it to access the Dark Web.

The kinds of websites and users you might encounter on the Dark Web could open your device to malicious attacks if a strong anti-virus software is not installed. Even if you have no interest in using the Dark Web you should still make sure that you have good virus protection anyway since any system vulnerabilities could leak your personal information.

Tor does not work well with media plug-ins such as Flash or JavaScript, making it difficult to watch videos and other media in Tor's browser. Not only will doing so cause issues with connection speed, but using media on Tor can also leak your IP address. For this reason, Flash and Java are usually disabled in Tor by default. You should also use a VPN while connecting to Tor in order to further protect your IP address and prevent leakages while using the browser.

VPN Services

A VPN, short for "virtual private network", is a service used to disguise your IP address while using the internet. This is important because your IP address can carry important personal information about you including your location and browsing history. What a VPN does is send your address through an encrypted tunnel that hides you true IP address while often giving the appearance that you are accessing the Internet from a different location.

There are many VPN services out there and generally speaking any service worth getting is going to cost money. Most plans can range from 3 to 10 dollars a month and are usually apart of a yearly or bi-yearly plan. You will want to stay away from free VPN services at all costs. You will also want to pick a VPN service that does not log user information since many VPNs still save your activity history and can be forced to hand that information over to the feds if pressured or subpoenaed. For these reasons it is also helpful to choose a VPN service that is not based in the United States nor based within a country that has intelligence sharing agreements with the United States, since this makes it more difficult for the US to pressure for this information.

ExpressVPN

ExpressVPN was ranked number 1 for best VPN by Cnet.com and has a very good reputation for security. The service has a no-loging policy and will not save your activity data. It's policy was put to the test in 2017 when its servers were seized by Turkish authorities following an investigation that resulted in no logged data found.
ExpressVPN will only collect maintenance-related data including server location choices and server connection time. Based in the British Virgin Islands, it is generally safe from most information sharing requests from other countries.

It has fairly fast speeds and goes the extra mile to secure data leaks by changing its encryption keys frequently. It also has a kill-switch feature which prevents your data from leaking if there is a server connection error.

Surfshark

Surfshark has one of the fastest internet speeds in a VPN on the market and was shown to be even faster than ExpressVPN. It is compatible across a wide array of platforms including Mac, Windows, iOS, and even some streaming and gaming devices. Surfshark also offers a few unique features that can enhance your browsing security and bypass legal restrictions on internet use in certain countries. Camouflage mode lets you mask you VPN use so that your internet service provider cannot tell you are using a VPN. Surfshark is also base in the British Virgin Islands, making it less prone to pressure from foreign governments.

NordVPN

A long trusted VPN service with a solid track-record, NordVPN is one of the most well-rounded and popular of the VPN services. Based in Panama, it is safe from the pressure of foreign governments to access user data. Nord protects your encrypted data by using a feature called perfect forward secrecy, which changes the encryption keys constantly as new data is encrypted.

NordVPN also as a great feature called CyberSec, which actively blocks trackers, ads, and malware when enabled,. It can also add an extra layer of privacy and anominity through encrypting you traffic through Tor servers using the Onion-over VPN feature. It has a no logging policy which was put to the test in 2018 when one of its servers was breached but resulted in no data found. It is an open source service, meaning it practices strong transparency with its users and looks to its users for input to make the service better. Although NordVPN speeds are slower than the others on this list, it remains a popular and reliable choice with excellent features.