

PVD Cryptoparty Digital Safety Workshop

How-to Guide

Table of Contents

[Table of Contents](#)

[Attributions](#)

[Licensing](#)

[Disclaimer](#)

[Introduction](#)

[Basic Security Essentials \(beginner\)](#)

[Password Hygiene \(beginner\)](#)

[Basic Password Guidelines](#)

[Password Managers \(beginner-medium\)](#)

[Two-factor Authentication \(beginner\)](#)

[Android Mobile Security \(beginner-advanced\)](#)

[Android Basic Security/Privacy Steps](#)

[Android Apps](#)

[Android Rooted Apps \(require an already rooted device\)](#)

[iOS Mobile Security \(beginner-medium\)](#)

[iOS Basic Security/privacy basic steps](#)

[iOS Apps](#)

[Privacy Enhancing Browser Extensions \(beginner-medium\)](#)

[Using Tor For Anonymous Browsing \(beginner\)](#)

[Tor Instructions](#)

[Tor Windows Installation](#)

[Tor MacOS Installation](#)

[Installing Tails OS \(medium\)](#)

[Chat, IM, & VoIP Encryption \(beginner-medium\)](#)

[Email Encryption \(medium-advanced\)](#)

[Hard Drive Encryption \(medium-advanced\)](#)

[Hard Drive Encryption with VeraCrypt \(medium\)](#)

[MacOS only File and Hard Drive Encryption with File Vault and File Vault 2 \(medium\)](#)

[Hard Drive Encryption with LUKS \(advanced\)](#)

Attributions

This work has been collated and curated by Richard Tavares.

This work includes material from the following sources:

CryptoParty Brief How-tos <https://www.cryptoparty.in/learn/how-tos>

Security in a Box - Digital Security Tools and Tactics <https://securityinabox.org/en/>

Surveillance Self-Defense <https://ssd.eff.org/>



This work is licensed under a [Creative Commons Attribution 4.0 International License](#).

Disclaimer

1. Security and anonymity are never 100% effective
 - a. Human error, forgetting a step, logging into facebook or google etc. can break anonymity
 - b. Bugs, new security flaws are constantly discovered, no OS, or software is 100% secure
 - c. Even anonymous behavior is analyzed, and could be correlated to a your actual identity
 - d. When you're anonymous/encrypted what you do, or communicate may be hidden, but the fact you are using anonymity/encryption, will be known to snoopers, and who you are communicating with, and some of your traffic could still be intercepted
2. Use of cryptographic tools are legal in this country but not all
3. cryptoparty is for beginners
4. Journalists and activists are welcome but should seek advice of experts:
<https://www.eff.org/> & <https://tacticaltech.org/>

Introduction

1. Assets: what digital objects/ information are valuable or worth protecting from outside eyes? What are the consequences when these dig. objects are compromised?
2. Risks:
 - a. Loss- losing access or integrity of dig. obj.
 - b. Disclosure- private information is publicly revealed
 - c. Interruption- network services become disrupted
3. Threats:
 - a. Identity theft/fraud
 - b. Viruses, malware, ransomware, etc.
 - c. Data collection
4. Adversaries:
 - a. Cybercriminals
 - b. Private companies (usually advertisers, and trackers, but many apps, stores, and services collect user data)
 - c. Government agencies, or states
5. Free software & decentralized services

Basic Security Essentials (beginner)

1. Set OS, antivirus, malware protection updates to occur automatically
2. Use antivirus/anti-malware programs to protect your system
 - a. Antivirus
 - i. Windows: Microsoft Safety Scanner, F-Secure, Kaspersky, Trend Micro, ClamAV
 - ii. MacOS: ClamXav
 - b. Anti-malware
 - i. Windows: Malwarebytes, Spybot, ComboFix
 - ii. MacOS: Malwarebytes, MacKeeper
 - c. The preceding applications offer free and premium services, as well as trial periods for the premium service, your mileage may vary
3. Use a firewall
 - a. Windows: enable windows firewall, or install Comodo
 - b. MacOS/Linux have built-in firewalls
4. use hard drive/ file encryption
5. Back up your data to ext. hd or to cloud
6. Use strong passwords and consider using a password manager

7. Setup two factor authentication (2FA) for all online accounts
8. Browse the web, esp. untrusted sites using anonymity tools such as Tor, or VPN
9. Keep in mind that “private browsing,” and “incognito mode” prevents the browser from storing the browsing history, cookies, form data etc., ***but it does not provide anonymity, or prevent servers, or websites from identifying you, logging your traffic, and storing personal information.***
10. Avoid conducting business, personal matters, and accessing sensitive information, from an open, or unsecured WiFi network, if you must, do so using a VPN or Tor.
11. When doing business, conducting personal matters, or accessing sensitive information, ensure that the sites you are using have a secure encrypted connection (check for HTTPS, and lock icon in address bar), if the service you are using doesn’t offer an HTTPS connection, request that they do so.
12. Encrypt personal communications such as, emails, phone calls, text messages, and chats
13. Use file encryption for valuable or vulnerable files, and use encryption when sharing files online
14. Securely delete sensitive files using [Eraser](#) (Windows) [Ccleaner](#) (Windows & MacOS), or [BleachBit](#) (MacOS & Linux)

It requires time and effort to be secure. You must decide how much time and effort to put in. There is a tradeoff between security/anonymity and convenience. The more secure you are the less convenient browsing and communicating can become. For instance, you might not need anonymity to check the weather or news, on the other hand, it may be worth the effort when researching highly personal or subversive subjects, or when communicating with particular individuals or organizations.

Password Hygiene (beginner)

Basic Password Guidelines

1. Avoid using the same password for multiple accounts, at the very least have several passwords that can be used at different security levels
2. Avoid using words that can be found in a dictionary
3. Use upper-case, lower-case, numbers, and symbols
4. Avoid easily guessed common substitutions e.g., 0 for o, @ for a, ! for i, etc.
5. The longer the password, the harder it is to crack
6. Strive for a complex password that can be easily remembered without writing it down
7. Don’t use personal details such as birthday, phone number, pet name, etc.

8. Change your passwords often, once every three months for accounts which need high security
9. Keep it secret, don't write it down or share with others unless absolutely necessary
10. One strategy for creating strong, memorable passwords is to incorporate acronyms, or the initialize remembered phrases such as song lyrics, e.g., egsthefm&mm (Everybody's got something to hide except for me and my monkey)
11. Use randomly generated passwords, and store them in a password manager, (see next section).

For reference, here is a list of example passwords, and how long it would take to crack (from passfault.com)

Sample password	Time to crack with an everyday computer	Time to crack with a very fast computer
bananas	Less than 1 day	Less than 1 day
bananalemonade	2 days	Less than 1 day
BananaLemonade	3 months, 14 days	Less than 1 day
B4n4n4L3m0n4d3	3 centuries, 4 decades	1 month, 26 days
We Have No Bananas	19151466 centuries	3990 centuries
W3 H4v3 N0 B4n4n45	20210213722742 centuries	4210461192 centuries <u>Passfault</u>

Password Managers (beginner-medium)

Password managers store passwords in an encrypted database for secured storage.

Link	Difficulty	OS

KeePassDroid	medium	Android
MiniKeepass	medium	iOS
KeePassX	easy	Windows, MacOS, Linux
Password Safe	easy	Windows

The preceding list is just a few examples of free password managers. There are many other premium password managers as well. Some features to consider are local vs. cloud storage, browser integration, and built-in password generation. KeePassX is a good choice because it is open source, meaning the code is publicly reviewed for security flaws. It also features local storage, and has a built-in password generator. Password managers should be set up with a very strong password, this password must protect all of the other passwords in the database, so make it as long as possible, write it down, and store it in a safe place if necessary. If you lose this password you will lose access to your password database.

Two-factor Authentication (beginner)

Two-factor authentication (2FA) adds an additional layer of security to your accounts. Usually this means verifying your identity by sending a code through SMS, or generating a code on a mobile device. Accounts using 2FA are more secure, and in addition to using a strong password, 2FA is an effective way of protecting accounts from unauthorized access.

1. To find out whether a particular service offers 2FA, check <https://twofactorauth.org/>
2. To learn how to enable 2FA for popular services such as, Facebook, Twitter, and Instagram check here: <https://www.turnon2fa.com/tutorials/>
3. Using [Google Authenticator](#)
 - a. Login to your Google Account, and [enable 2-step Verification](#)
 - b. Install Google Authenticator, from your device's app store
 - c. On your computer go to the [2-step Verification settings page](#) (must be logged in), and click Android or iPhone for your device
 - d. Open app, select Begin setup, choose Set up account
 - e. ***Android**
 - Using QR code, select Scan a barcode, Authenticator may prompt you to download a scanner app if your device does not have one installed already
 - Using secret key, select Enter provided key then enter the email address of your Google Account in the "Enter account name" box. Next, enter the secret key on your computer screen in the "Enter your key" box. Make sure you've chosen to make the key Time based, then select Add.
 - f. ***iPhone** Tap the plus icon, Tap Time Based. To link your mobile device to your account:
 - Using Barcode: Tap "Scan Barcode" and then point your camera at the QR code on your computer screen.
 - Using Manual Entry: Tap "Manual Entry" and enter the email address of your Google Account. Then, enter the secret key on your computer screen into the box next to Key and tap "Done."
 - g. **Potential issues** if you are using a third-party mail reader or app, or are seeing a "password incorrect" message when accessing your google account through an app, you will need to create an App Password that is unique for each app, (go to My Account, Sign-in & security, App Passwords) for more info see: <https://support.google.com/accounts/answer/185833?hl=en>
 - When using an App Password, you may want to write it down or store in a password manager, once you accept the password you won't be able to see

it again, so if you get logged out and don't have the app password you will need to create a new one.

Android Mobile Security (beginner-advanced)

Android Basic Security/Privacy Steps

1. Set security updates to automatic (*Settings -> Security -> Security policy updates*)
2. Make sure device software is up to date (*Settings -> About device -> Software updates -> Check for updates*)
3. Make sure all apps are up to date (*Google Play Store -> Menu -> My Apps & Games -> update all*)
4. Enable Lock SIM Card (*Settings -> Personal -> Security -> Set up SIM card lock*) You will set a pin that needs to be entered when phone powers on. No calls can be made without SIM card and PIN.
5. Use Screen Lock (*Settings -> Personal -> Security -> Screen Lock*) use PIN or Password to create a strong password (swipe and pattern are not secure)
6. Set a security lock timer (*Settings -> Lock Screen -> Secured Lock Time*) automatically locks your phone after the specified amount of time, requiring reinput of PIN or password to unlock
7. Encrypt phone and SD Card (*Settings -> Personal -> Security -> Encryption*) Set password and encrypt device storages, make sure the device is fully charged and connected to power. Process takes an hour or longer, during which you will not be able to use the phone.
8. Turn off Wi-Fi, Bluetooth (*Settings -> Network*), Near Field Communication (NFC) (*Settings -> Connect and share*), and Tethering and Portable Hotspots (*settings -> Network -> Tethering and Mobile hotspot*). Only connect to devices and networks that are trusted.
9. Turn off Wireless GPS, GPS location, and mobile data (*Settings -> Network -> Location -> Off*) when you're not using GPS to reduce location tracking. Turn off Wifi and Bluetooth GPS scanning, which connect your device to untrusted networks and devices to improve location accuracy (*Settings -> Network -> Location -> Improve accuracy*)
10. Block your caller ID (*Phone dialler -> settings (top right 3 dots) -> Call -> More settings -> show my caller ID -> Hide number*)

Android Apps

Topic	Link	Difficulty	Description
Antivirus/anti-malwar	Avira	easy	Scan device and prevent threats

e			
Antivirus/anti-malware	Malwarebytes	easy	Scan device and prevent threats
Antivirus/anti-malware	Lookout	easy	Scan device and prevent threats
Anonymous Browsing	OrBot + OrFox	easy	Proxy With Tor/Private Web Browser
Anonymous Browsing	Psiphon Pro	hard	Free VPN service for Android, with premium subscription option
Anonymous Browsing	OpenVPN Connect	medium	Ad-supported VPN service for Android
Phone calls, messaging, chat	Signal	easy	encrypted phone calls and messages; WhatsApp alternative
Phone calls, messaging, chat	Wire	easy	encrypted phone calls, video chats and messages; WhatsApp alternative
Chat	Conversations	medium	encrypted chat (jabber plus OTR & OMEMO)
Chat	Surespot	medium	Secure messaging
Email	OpenKeyChain/K9 Mail	hard	encrypted e-mail
Email	APG	hard	Encrypt and decrypt single files for email
Passwords	KeePassDroid	medium	Password manager
Topic	Link	Difficulty	Description
Navigation	Transportr	easy	Map for Public Transport (formerly known as Liberario)

Navigation	OSMAnd	medium	OpenStreetMap with offline maps and navigation
Ad blocker	Ad Away	easy	Blocks banners, pop ups and video ads
Other	Wi-Fi Privacy Police	easy	prevent leaking which WiFis you've been logged into before
Other	F-Droid	medium	“App-Store” for free software
Other	Obscuracam	medium	Automatically blur and obscure faces in photos that you take
Other	Applock	medium	Allows user to password protect individual apps
Other	Cerberus	medium	Anti-theft, locate lost phone, and remotely lock, or wipe data
Other	Notecipher	difficult	Encrypted note-taking platform
Other	Panic Button	medium	Secretly send emergency SMS to alert a select list of contacts that you may be in danger
Other	SpideroakONE	medium	Share files between Android, a computer, and other users via an internet server, files are encrypted

Android Rooted Apps (require an already rooted device)

Topic	Link	Difficulty	Description
Ad-blocker	Ad-block Plus	difficult	Filters and blocks ads
Firewall	AF Wall+	difficult	Firewall app, gain control over which apps have access to the internet
Firewall	Droidwall	difficult	Choose which apps have access to the internet
Encryption	CryptFS	difficult	Allows user to change device encryption password so that there two distinct passwords for decryption, and device unlock
Encryption	Cryptonite	difficult	Create encrypted folders on Android to store sensitive files
Other	SnoopSnitch	difficult	Monitors mobile radio networks to alert you to the presence of possible threats
Other	X Privacy	difficult	Prevents Android system from sharing information like phone numbers, names, and locations with any other apps

iOS Mobile Security (beginner-medium)

iOS Basic Security/privacy basic steps

1. iOS is closed source code, meaning the code cannot be audited, verified, or completely trusted to be completely secure, or to protect a user's privacy.
2. Most apple devices are now encrypted by default.
3. Set a strong numeric/alphanumeric Password (*Settings -> Passcode/Touch ID & Passcode -> Set require passcode to immediately -> Disable simple passcode -> At least a six digit numeric code is recommended -> once you set code scroll to bottom it should say "Data protection enabled"*)
4. With data protection enabled, in passcode settings, device can be set to wipe after after ten failed passcode attempts.
5. Itunes has an option to create encrypted backups.
6. icloud users should use strong passwords for encrypted backups and be aware that it is possible for Apple to decrypt for law enforcement
7. Encrypted Devices running ios 8 and later cannot have files extracted without the user passcode, prior versions can, so update ios it possible
8. Device encryption is only effective when the device has been freshly powered down and rebooted, **without having been unlocked.**

iOS Apps

Topic	Link	Difficulty	Description
Anonymous browsing	Onion Browser	easy	Proxy With Tor/Private Web Browser
Anonymous browsing	Ghostery	easy	Block trackers
Phone calls, messaging, chat	Signal	easy	encrypted phone calls and messages; WhatsApp alternative
Phone calls, messaging, chat	Wire	easy	encrypted phone calls, video chats and

			messages; WhatsApp alternative
Chat	ChatSecure	medium	encrypted chat (with jabber plus OTR & OMEMO)
Passwords	MiniKeepass	medium	Password manager for iOS

Privacy Enhancing Browser Extensions (beginner-medium)

Will work with Chrome, Chromium, and Firefox. Those using Internet Explorer or Edge may want to consider downloading a more secure browser that shares less personal information.

To install extensions in Firefox: click menu top right, Add-ons, search for extension, then click install to add to browser

To install extensions in Chrome or Chromium: Click menu top right, More tools, Extensions, Get more extensions, search for extension, then click add to browser to install

Before you install extensions (optional)

To get a sense of what info the trackers are getting, and what trackers are associated with the sites you visit, check out these sites/extensions and do some browsing. Then, after installing the extensions do some more browsing, and check again to confirm extensions are working.

- <https://panopticlick.eff.org>
- www.smart-ip.net/geoip
- [6 Links that will show you what Google knows about you](#)
- Lightbeam (Extension, Firefox only)

Consider turning on the do not track feature, turning off cookies (*may affect functionality of some sites*), and never remember history, private browsing/incognito mode. Search how do I... for your particular browser.

As you think about security and privacy, consider setting up one browser as “secure and private” to test and use, while preserving the functionality of the other for personal accounts, videos, etc.

And keep in mind that having an open tab logged in to Google or Facebook may thwart your attempts at anonymity, and limit the functionality of your privacy extensions.

Consider changing your homepage/browser search bar to one of the following services which allow anonymous and tracker free searching.

- <https://startpage.com/>
- <https://duckduckgo.com/>
- <https://search.disconnect.me/>
- <https://metager.de/tor/en/>

Extensions List:

Ad-blockers

- [Adblock Plus](#)
- [AdGuard](#)
- [uBlock Origin](#) & [uBlock Origin Extra](#)
- [Adblock for Youtube](#)
- [Adnauseum](#) (Firefox only)

Tracker Blockers

- [Privacy Badger](#)
- [Disconnect.me](#)
- [Lightbeam](#)
- [Ghostery](#)
- [Abine Blur](#)

Script Blockers/ Forced Encryption (*may affect functionality of some sites*)

- [NoScript](#) (Firefox) & [ScriptSafe](#) (Chrome) - globally disables JavaScript, blocking unwanted potentially malicious scripts
- [HTTPS Everywhere](#) This extension restricts the browser to encrypted HTTPS connections which are more secure because of SSL/TLS encryption
- Consider purchasing the services of a Virtual Private Network (VPN) which routes your traffic through a separate encrypted network, and also anonymizes your IP address.
- Consider using Tor, a free service, which anonymizes internet traffic by sending encrypted packets through multiple volunteer run relays. The Tor network suffers from low bandwidth and lack of support for multimedia plugins, making video streaming, and file sharing difficult. Many services block users on the Tor network due to its association with spammers, and botnets.

Other:

- [uMatrix](#) manage cookies, javascript, images, css, and media content
- [Self-Destructing Cookies](#) auto delete for cookies without closing the browser

- [CanvasBlocker](#) Browser Add-on to change JS-API for modifying canvas to prevent Canvas-Fingerprinting
- [CertificatePatrol](#) shows updates of SSL certificates
- [RequestPolicy](#) XSS prevention, and cross site scripting control

****It is a good idea to install multiple ad/tracker blockers because no advertizer/tracker server list is 100% complete (they're always changing). With multiple blockers running you may encounter errors/conflicts, if that is the case simply disable the culprit causing the issue. It is also good practice to occasionally go into each extension and manually update the server list, or subscribe to additional lists.****

With ad-blockers/trackers enabled you should experience slight performance improvement as your browser is no longer connecting to trackers, and downloading pesky ads. If you are viewing ad-supported content you may want to consider 'whitelisting' that site, or temporarily disabling your ad-blocker.

Using Tor For Anonymous Browsing (beginner)

Tor is a free, volunteer run service that enables private anonymous browsing by masking a user's IP address through several layers of encryption. Using the Tor Browser makes it more difficult for sites to learn your identity, and it makes it harder to monitor your online activity. Only activity performed in the Tor Browser will be anonymized, activity in other apps/browsers will not be routed through the Tor network.

Disclaimer: Using Tor is not a silver bullet to protect your privacy, Tor can protect against some forms of surveillance, and make it more difficult to monitor or block your online activity. However it is not 100% effective, your ISP, and the DNS servers will continue logging information about you. Tor does not mask your MAC address, a unique number associated with your computer's network hardware, which can be used to identify you or your computer. Furthermore, your online behavior is constantly analyzed, and patterns in your anonymous behavior can possibly be linked to your non-anonymous online behavior. There are some steps you may want to take while using Tor in order to actively protect your privacy, and avoid compromising your anonymous identity, check out the tips listed here <https://www.torproject.org/download/download-easy.html.en#warning>

Tor Instructions

1. Download Tor Browser Bundle at <https://www.torproject.org/download/download-easy.html.en>
2. The site should recognize your Operating System, confirm you are downloading the correct file.
3. **Optional** for extra security download and check associated signatures
4. Open and run the file from your downloads folder, or default download location.

Tor Windows Installation

1. Follow steps of installer wizard
2. Run Tor Browser for first time -> click connect to route traffic through Tor
3. When browser opens, a green onion, and congratulations will alert you that Tor has been configured correctly.
4. Click onion icon in toolbar to change security setting, or request a new Tor identity (useful after logging into a site, doing a location revealing search, etc.)
5. You can check Tor status here <https://check.torproject.org/> and you can confirm that sites are not logging your true IP here <http://www.smart-ip.net/geoip>
6. Often Tor routes your traffic through a foreign country, you may experience network delays when using Tor, and when you connect to some websites they may appear in a foreign language.

Tor MacOS Installation

1. When the file opens you will need to drag the TorBrowser icon into the Applications folder icon.
2. When you run TorBrowser for the first time, click connect to connect directly to the Tor network.
3. When browser opens, a green onion, and congratulations will alert you that Tor has been configured correctly.
4. Click onion icon in toolbar to change security setting, or request a new Tor identity (useful after logging into a site, doing a location revealing search, etc.)
5. You can check Tor status here <https://check.torproject.org/> and you can confirm that sites are not logging your true IP here <http://www.smart-ip.net/geoip>
6. Often Tor routes your traffic through a foreign country, you may experience network delays when using Tor, and when you connect to some websites they may appear in a foreign language.

Installing Tails OS (medium)

Tails OS is a live amnesiac operating system, meaning each user session leaves no trace on the computer, on shut down all memory, files, history, etc. are wiped, and on restart it is a fresh system. Tails makes privacy and anonymity very easy for an average user. Tails routes all internet traffic through the Tor network automatically. Tor is a free, volunteer run service that enables private anonymous browsing by masking a user's IP address through several layers of encryption. Tails optionally will spoof your computer's MAC address, a unique number associated with your computer's network hardware, which can be used to identify you or your computer. Tails by default installs a suite of open source cryptographic tools which can be used to encrypt, files, emails, and messages. Tails can be installed to and run from a DVD, USB memory stick, or an SD card. USB sticks are recommended for performance, and ease of booting.

Disclaimer: Tails aims to make using Tor easier, and give users a tool to protect their privacy on the go. Tails is not a perfect solution, it can not protect from all types of attacks or surveillance, and it is a community funded work in progress. For more information see the warnings listed here <https://tails.boum.org/doc/about/warning/index.en.html>

Tails works fine even on older computers

Hardware requirements: (from <https://tails.boum.org/doc/about/requirements/index.en.html>)

- Either **an internal or external DVD reader** or the possibility to **boot from a USB stick or SD card**. (Google or search “how to boot to ... on a ...[your computer model])
- Tails requires an x86 compatible processor: **IBM PC compatible** and others but not PowerPC or ARM. Mac computers are IBM PC compatible since 2006.
- **2 GB of RAM** to work smoothly. Tails is known to work with less memory but you might experience strange behaviours or crashes.

For more advanced users, Tails can also be installed as a virtual machine in a virtualization manager such as VirtualBox.

<https://tails.boum.org> provides excellent installation instructions with pictures.

To install from scratch you will need 2 USB sticks at least 4GB, and another device to access instructions

To install from scratch in Windows <https://tails.boum.org/install/win/usb/overview/index.en.html>

To install from scratch in MacOS <https://tails.boum.org/install/mac/usb/overview/index.en.html>

If someone you know already has a Tails USB stick, or if you are installing to Linux you will only need one USB stick at least 4GB

To copy from another Tails to a PC

<https://tails.boum.org/install/win/clone/overview/index.en.html>

To copy from another Tails to a Mac

<https://tails.boum.org/install/mac/clone/overview/index.en.html>

To install from Debian, Ubuntu, or Mint Linux

<https://tails.boum.org/install/debian/usb/overview/index.en.html>

To install from other Linux distros

<https://tails.boum.org/install/linux/usb/overview/index.en.html>

Once Tails is installed to a USB stick, you will need to boot it. Plug in the USB and turn on your computer. If Tails does not start automatically, you will need to figure out the keys to press on start up to access your computer's BIOS or boot manager. Every computer is different so you will need to use a search engine to figure out how to do it with your particular model. Once you are in you will be able to boot from a USB disk, or change the boot order so that your computer boots from USB when plugged in, before attempting to boot from hard disk.

Once your Tails is up and running, you'll want to configure the system according to your needs, follow the guide here <https://tails.boum.org/doc/index.en.html> scroll down to First steps with Tails.

Congratulations! You can now browse anonymously with confidence! You can use your Tails stick on any computer that meets the hardware requirements! Don't forget to tell friends and family, now you can help spread Tails by making copies.


Chat, IM, & VoIP Encryption (beginner-medium)

- [Ricochet IM](#), available for Windows/Mac/Linux is an anonymized, end to end encrypted instant messenger. Ricochet uses the Tor network to send encrypted messages via a hidden service, which prevents your IP address and your location to be detected. Instead of creating a username, users get a unique address that looks like ricochet:rs7ce36jsj24ogfw. Users then share these addresses to add contacts.
- Off-the-record (OTR) messaging is an IM protocol employing encryption, and authentication to ensure messages are only understood by the intended recipients. There are a several chat clients that use OTR:
 - [Gajim](#) (Windows, Linux, MacOS)
 - ChatSecure ([iOS](#), [Android](#))
 - [Conversations](#) (Android)
- [TorChat](#) is another messenger, it employs Tor's hidden services to ensure anonymity, and is very easy to use.

- [Retrosahre](#) is an application for secure file sharing and chat
- Voice over IP encryption can be easily accomplished using the WebRTC framework that is built into most browsers. Chat/conference rooms can be created using sites, such as <https://meet.jit.si>, <https://talky.io>, and <https://spreed.me>.
- Voice over IP encryption can be done using [Jitsi](#), an open source, audio/videoconferencing and IM application available for Windows, Linux, and MacOS.

Email Encryption (medium-advanced)

Email encryption prevents the contents of your messages from being intercepted. Keep in mind that the subject lines are **NOT** encrypted, and that only the contents of the message are protected, your ISP, the servers, and eavesdroppers can still detect who you are sending mail to.

1. For quick one time emails, consider using a disposable email address such as <https://www.guerrillamail.com/> which allows access to a temporary email address to send and receive email. <https://riseup.net/>
2. Consider using an encrypted email provider such as [Tutanota](#), [Protonmail](#), or [Riseup](#)
3. For more trustworthy email providers and to compare their privacy policies check out [Prism Break: Email Accounts](#), and this helpful list of [privacy-conscious email services](#) put together by the users of r/privacy
4. The easiest way to do Email encryption is by using [Mailvelope](#) which is available as a Chrome Extension, or a Firefox Addon, and can be easily used with Gmail and other webmail services, [Mailvelope full documentation](#)
 - a. Set up:
 - i. Install to your browser
 - ii. Click on the Mailvelope lock icon, click options, click key management
 - iii. Click generate key, fill out information, and click submit (keys already in use can also be imported)
 - b. Import public keys for your mail recipients:
 - i. Your recipient's public key must already be uploaded to the keyserver
 - ii. Use Key search to search for your recipient's email address
 - iii. Click on the appropriate keyID
 - iv. Recipient's public key is displayed
 - v. Click the key symbol to import your recipient's public key to Mailvelope
 - c. Encrypting outgoing messages:
 - i. Login to your webmail (Gmail)
 - ii. Click the compose button  which will appear in the compose area of your webmail
 - iii. Compose your message in the pop up window, and add your recipient(s), whose public keys should have already been imported
 - iv. Click encrypt, and optionally sign
 - v. The encrypted text will be in a new email, and can be sent using the webmail send button
 - d. Decrypting incoming messages

- i. Encrypted messages will appear with a locked envelope icon, click to begin decryption
 - ii. Enter your password
 - iii. Mailvelope will decrypt the message if it has access to the private key corresponding to the public key with which the message was encrypted
- e. Mailvelope has additional useful features, see [full documentation](#) for more details

Depending on your threat model, trusting Gmail, Yahoo, or other webmail providers may not be an option. In that case it is recommended to use POP3/IMAP email from a trusted provider combined with an open source email client such as Thunderbird or Icedove. Full installation and how to guide: [security-in-a-box](#)

To use GPG encryption on your computer with Thunderbird:

- a. Have email account ready
- b. Install [Thunderbird](#)
- c. Windows users: install [gpg4win](#)
- d. Mac users: install [GPGTools](#)
- e. Install [Enigmail](#) for GPG encryption in functionality in Thunderbird
- f. For additional anonymity, and privacy (i.e., to prevent snoopers from learning the destination of your emails), install [Tor](#), and [Tor Birdy](#)
- g. Configure email account, [setup privacy and security settings](#)
- h. [Send and receive encrypted messages](#)

Hard Drive Encryption (medium-advanced)

Hard Drive Encryption with VeraCrypt (medium)

- [VeraCrypt](#) is free disk encryption software for Windows, Linux, and MacOS. VeraCrypt can be used to encrypt whole drives, volumes, USB drives, and SD cards. Encrypted volumes and drives leave no signature, and appear as random data giving the user some level of plausible deniability. VeraCrypt works with dual boot systems. For more information see the [Beginner's Tutorial](#) and the [VeraCrypt Online Documentation](#).

MacOS only File and Hard Drive Encryption with File Vault and File Vault 2 (medium)

- FileVault and FileVault 2 are (mac only) applications included in MacOS for folder and full disk encryption. Admin privileges are required, and users have the option of storing a recovery key with Apple.

Hard Drive Encryption with LUKS (advanced)

- LUKS (Linux Unified Key Setup) is an encryption method that works only with Linux. The easiest way to use LUKS encryption is to configure LUKS during installation of a fresh system, check with your particular Linux distribution's documentation to learn how.
- After an installation, the Gnome Disk Utility can be used to encrypt partitions as well as full disks (though this is difficult). LUKS encrypted drives will only be recognized by Linux systems, can not be used with Windows or MacOS systems. For more information, see this [guide on setting up LUKS with Gnome Disk Utility](#).