Cryptoparty Handbook

Dear friends, scientists & scholars,

Today we'll reclaim our privacy and improve browsing experience step-by-step. There is a difference between protecting your grandma sharing cake recipes, and a human rights activist in a hostile country. Your granny might not be the right person to sell a prepaid SIM & burner-phone to. An activist might consider the below steps entry-level basics, even dangerous if not tailored to the individual. But we all need protection. Even more so if you assume that «you got nothing to hide».

> «Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.»
>
> – Edward Snowden

Those with nothing to hide still like curtains in their bedroom and prefer public restrooms equipped with locks minus the CCTV cameras. If you need further convincing, the movie "Nothing to Hide" is available free online.

The following pages contain a list of useful software, search engines, and additional privacy aids to help you take control of your digital privacy. A ***dictionary of terms*** *is located at the end.*

Email Encryption

Thunderbird is a desktop email client, which with its Enigmail extension is used for encrypting, decrypting, digitally signing and verifying digitally signed emails.
Supported platforms: Windows, Mac, Linux. [1][WARNING: Look at the footnote below!]

mozilla.org/thunderbird/

K-9 Mail is an Android email client, which when used with Android GPG agents like APG or OpenKeyChain can provide seamless exchange of encrypted and signed emails.
Supported platforms: Android.

k9mail.github.io/download.html

More: https://www.privacytools.io/#clients

Enigmail is an extension for Thunderbird that performs encryption, decryption, digital signing, and signature checking operations on email in Thunderbird client.

enigmail.net/index.php/en/
mozilla.org/en-US/thunderbird/

GPG Tools is a GPG manager for Mac OS, it works with standard mail client included in Mac OS. It performs encryption, decryption, digital signing, and signature checking inside email client.
Supported platforms: Mac.

gpgtools.org

APG (*Android Privacy Guard*) is a GPG manager for Android. It performs encryption, decryption, digital signing, and signature checking inside the email client. Works with K-9 mail client.
Supported platforms: Android

OpenKeyChain is a GPG manager for Android. It performs encryption, decryption, digital signing, and signature checking inside the email client. Works with K-9 mail client.
Supported platforms: Android

openkeychain.org

More: https://www.privacytools.io/#clients

PGP Public Key Servers:
http://pgp.mit.edu
http://pgp.key-server.io
https://keyserver.mattrude.com/

Mailvelope is an extension for Chrome and Firefox that allows you to encrypt messages inside a web browser on email service websites such as GMX, Yahoo, Gmail and Outlook.

mailvelope.com

Keybase is a program for secure messaging. It includes identity verification from social platforms and encrypted direct messaging on some, encrypted group messaging and git repositories.
Supported platforms: Windows, Linux, Mac, Android, iOS, Chromium/Firefox

keybase.io

p≡p

PEP (pretty Easy privacy) is another application for email encryption but with many operations automated, like key creation and key management. It does not use a keyserver but sends public keys in attachment and relies on trust-on-first-use.
Supported platforms: Windows (Outlook), Android, and soon IOS.

prettyeasyprivacy.com

Some of the Privacy-Conscious Email Providers:
https://www.privacytools.io/#email

Never trust any company with your privacy, always encrypt files on your machine.

Privacy-Conscious Email Providers

Protonmail is an open-source commercial free email service that uses PGP end-to-end encryption to protect its users' emails, as well as passwords to protect mailboxes from the service itself, so the provider shouldn't be able to read your emails. Supported platforms: Web, Mac, Linux, Windows, Android, iOS

protonmail.com

Tutanota is an open-source commercial free email service that offers end-to-end encryption for emails exchanged between its users.

tutanota.com

Never trust any company with your privacy, always encrypt files on your machine.

Password managers

KeePass is a free open-source password manager, which helps you to manage your passwords in a secure way. All passwords are in one database, which is locked/encrypted with one master key or a key file.
Also compatible password managers are: **KeePassX**, **KeePassXC**, **KeepassDdroid**
Supported platform: Windows, Linux, Mac, Android, iOS, browser.

keepass.info

Master Password is a password manager that does not store any passwords anywhere. You just need to know one password, and nothing else is stored. Passwords are generated on-demand from your name, the site and your master password. No syncing, backups or internet access needed.
Supported platforms: Windows, Linux, Mac, Android, iOS, Web

masterpasswordapp.com

More on: https://www.privacytools.io/#pw

Secure Web Browsing

Tor browser is a modified version of Firefox web browser configured for maximum privacy, security and anonymity that uses the Tor network by default for all networking.
Supported platforms: Windows, Mac, Linux, iOS, Android, OpenBSD.

torproject.org

Orbot is an Android application that connects to Tor network. It provides connection to Tor on port 8118 and allows other applications to use that port for secure network communication through Tor. Recently it also comes with VPN option to allow all or selected applications to use Tor.
Supported platforms: Android.

guardianproject.info/apps/orbot/

Brave is a Chromium based web browser that automatically blocks ads and trackers and has integrated password managers, making browsing faster and safer. It is compatible with most of the Chrome extensions, so it is easy to switch to Brave.
Supported platforms: Windows, Linux, Mac, Android, iOS.

https://www.brave.com/

Secure Web Browsing – other search engines

DuckDuckGo is a search engine that doesn't track you. Some of its source code is open-source, but it is proprietary software.

duckduckgo.com

startpage

Startpage search engine is just a Google search proxy that will protect you from Google linking your identity and searches.

startpage.com

searX

SearX is an open-source metasearch engine, aggregating the results of other search engines while not storing information about its users.
No logs, no ads and no tracking.

searx.me

Peekier is new search engine that doesn't keep logs and respects your privacy.

peekier.com

More: https://www.privacytools.io/#search

Secure Web Browsing – browser addons

Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web.

eff.org/privacybadger

HTTPS Everywhere is an extension that encrypts your communications with many major websites, making your browsing more secure. Works if websites have SSL enabled.

eff.org/https-everywhere

Cookie AutoDelete automatically removes cookies when they are no longer used by open browser tabs. With the cookies, lingering sessions, as well as information used to spy on you, will be expunged.

AdNauseam is a free browser extension designed to obfuscate browsing data and protect users from tracking by advertising networks. It does it by automating Ad clicks universally and blindly on behalf of its users.

adnauseam.io

More: https://www.privacytools.io/#addons

Secure Web Browsing - VPN

OpenVPN is an open-source VPN protocol implementation, recently audited and fairly reliable and secure compared to other VPN protocols.
Supported platforms: Windows, Linux, Mac, Android and iOS (OpenVPN Connect app for phones).

This is just a VPN client, you will still need VPN provider.
We suggest Riseup, Calyx or Autistici/Inventati organizations as free VPN providers. Check out these comparisons: https://www.privacytools.io/#vpn
https://secured.fyi/vpn.html

Bitmask is an open-source OpenVPN client with a nice intuitive graphic user interface. It uses Risup, Calyx, and other privacy aware projects that offer free VPN services.
Supported platforms: Linux, Mac, Android.

https://bitmask.net/

Wireguard is an opensource VPN application software that utilizes state-of-the-art cryptography, and it is faster than OpenVPN, and other VPN software.
Supported platforms: Windows, Mac, Linux, Android.

https://www.wireguard.com/

Never trust any company with your privacy, always encrypt files on your machine.

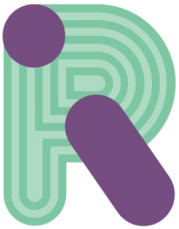
Encrypted messaging, voice & video

Signal is an application that provides encryption for instant messaging, voice and video calling, and file sharing. All communications are end-to-end encrypted, but require all participants to use Siglal and it works only over internet.
Supported platforms: Android, iOS, macOS, Windows, Linux.

signal.org

Wire app allows users to exchange end-to-end encrypted instant messages, as well as make voice and video calls, and share encrypted files.
Supported platforms: Android, iOS, macOS, Windows, Linux, web.

wire.com



Riot is application for secure decentralized chat built on top of new **Matrix** protocol. It has integrated support to communicate to other protocols as well like IRC, Telegram, Discord, WhatsApp, Skype and others. Inside Matrix, chats and file transfers are end-to-end encrypted, but not when using other protocols like Discord and IRC.

Riot.im

More at: https://www.privacytools.io/#im

Encrypted Instant Messaging - XMPP

Gajim is a multiplatform XMPP instant messaging client for desktop. It is offered through the provided extensions OMEMO and OTR encryption.
Supported platforms: Windows, Linux, BSD.

gajim.org

Pidgin is XMPP multiplatform instant messaging client for desktop. It is offered through the provided extensions OMEMO and OTR encryption.
Supported platforms: Windows, Linux, Mac, BSD.

pidgin.im

Adium is a XMPP multiplatform instant messaging client for Mac OS. It has integrated OTR support, and OMEMO support exists, but it has to be downloaded from Github and compiled (https://github.com/shtrom/Lurch4Adium).
Supported platforms: Mac.

adium.im

Coy is a multiplatform instant messaging client with integrated OTR support.
Supported platforms: Windows, Mac, Linux

coy.im

Conversation is an Android app for instant messaging with integrated support for OTR and OMEMO.
Supported platforms: Android

conversations.im

Xabber is a XMPP client for AAndroid with built in support for OTR.
Supported platforms: Android, web.

xabber.com

Zom is a XMPP client for mobile phones that comes with OTR/OMEMO built in support and automatic encryption of all messages by default, without user involvement.
Supported platforms: Android, IOS.

zom.im

XMPP/Jabber public servers:
xmpp.is
core.mx

More at: xmpp.net/directory.php

Operating Systems

Debian is a popular Linux desktop computer operating system and distribution that is composed entirely of free and open-source software, most of which is under the GPL license. From a privacy perspective it is much better than proprietary Windows.

debian.org

Tails is a live operating system that starts on almost any computer from a DVD, USB stick, or SD card. It aims at preserving privacy and anonymity by routing internet connections through the Tor network. It leaves no trace on the computer running it, and uses modern cryptographic tools to encrypt files, emails and instant messaging.

tails.boum.org

Qubes is an open-source operating system designed to provide strong security for desktop computing. Qubes is based on Xen hypervisor which provides virtualization and isolation of various operating systems and programs running on it simultaneously.

qubes-os.org

More at: https://www.privacytools.io/#os

Cryptoparty Dictionary

Threat model is a system or model for determining the level of security measures required based on the assumed ability of the adversary.

Plaintext is a human readable unprotected message.

Ciphertext is an encrypted plaintext message, that requires a password or key to be decrypted and understood.

End-to-End encryption is secure communication where only the participants can read content of exchanged messages, but no other actor between them can read the content.

XMPP (Exstensible Messaging and Presence Protocol) is near-real-time message communication protocol.

OTR (*Off-The-Record*) is a protocol for encrypted and verified/authenticated messaging between two participants over XMPP.

OMEMO (*OMEMO Multi-End Message and Object Encryption*) is protocol for encrypted and verified multi-client end-to-end encryption over XMPP.

Fingerprint is a short sequence of characters derived from public key or secure communication sessions. It is used to authenticate the participant in secure communication or to easily identify public keys.

OLM is algorithm for end-to-end encryption developed by Matrix and based on Signal’s double ratchet algorithm.

Signal protocol is a non-federated end-to-end encryption protocol for voice calls, video calls, and instant messaging.

PGP (*Pretty good privacy*) was a program and then become the standard for encrypting e-mail messages.

OpenPGP is the open-source implementation of PGP.

GPG (*Gnu Privacy Guard*) is a free and open-source implementation of OpenPGP licensed under GNU GPL license.

Public key is the part of a key pair in asymmetrical cryptography that can be publicly announced. Often attached to a certain email address, it is used by others to encrypt messages that only the person with the corresponding private key would be able to decrypt.

Private key is the secret part of a key pair in asymmetrical cryptography that is used for decrypting messages (encrypted to you using your public key) and digitally signing messages.

Key server is a server that is used to upload users' public keys, and it provides the web interface for easy search of other people's public keys. All key servers synchronize among each other.

SSL *(Secure Socket Layer)* is a cryptographic protocol for securing communication between the user's computer and server it is accessing.

IM (instant messaging) is near-real time messaging communication.

SRTP and **ZRTP** (Secure Real-time Transport Protocol and Zimmermann Real-time Transport Protocol) are cryptographic key agreement protocols for secure end-to-end voice and video communication.

Ip (Internet Protocol) address is the numeric address assigned to each device connected to the network.

ISP - (*Internet Service Provider)* is a company providing internet access to users.

Proxy (server) is another computer on network performing internet activity on the user's behalf in order to hide the user's IP address, location and identity from online services. Sometimes used to avoid censorship.

Tor network is a group of volunteer proxy servers, that relay encrypted messages between each other making it hard to determine who is who on Tor and who is searching what. It anonymizes the location and identity of the users, as well as content and privacy of their search, and helps users to avoid censorship.

VPN is a software technology that encrypts the user's network activity between VPN server and the user's computer. VPN server acts in a similar way like a proxy but with added encryption. This enables the user to hide their IP address and location from online services, avoid censorship, and protect against surveillance.

OpenVPN is an open-source protocol implementation of VPN.

Source: https://goo.gl/ivG521 *and Wikipedia*

Disclaimer

Every software and program mentioned in this handbook is open-source. We do not endorse any proprietary software or commercial products and services.
Closed source programs are more likely to have undisclosed functionalities and hidden backdoors.

Openvpn clients:

Mac: https://www.tunnelblick.net/
Windows:
https://openvpn.net/index.php/open-source/downloads.html
Linux: sudo apt-get install openvpn
Android and iOS: Openvpn Connect

OpenVPN for Android

OpenVPN for iOS

Free openvpn servers to try out, but do not use them for anything confidential (we do not endorse commercial products, this is just for demo):
https://www.vpnbook.com/freevpn
https://www.freeopenvpn.org/en/

[1]EFAIL is:
recently discovered vulnerability in way mail clients process active content of HTML emails, for example externally loaded images or styles, to exfiltrate plaintext through requested URLs
efail.de

Useful websites:

https://www.privacytools.io/
https://www.eff.org/node/82654
https://prism-break.org/
https://ssd.eff.org/en
https://myshadow.org/
https://securityinabox.org/en/
https://freedom.press/training/
https://pack.resetthenet.org/
https://cryptoparty.rs/

Internet Society
Serbia Belgrade
Chapter