

# Citizen FOSS

*Snowden's toolkit – for the Rest of Us.*



A Presentation & Guide by Sean O'Brien

[sean@webio.me](mailto:sean@webio.me) | [sean.obrien@yale.edu](mailto:sean.obrien@yale.edu)



## Citizen Four (2014):

Film following **Edward Snowden** as he shares NSA spy documents and attempts to flee Hong Kong. "Citizenfour" was one of Snowden's pseudonyms.

## FOSS (English, acronym):

Free and Open Source Software. "Open Source" is often a business term for **Free Software**. The "free" means "freedom" but, usually, it also costs nothing.  
*Synonyms:* Software libre, FLOSS.

“ ...many people forget – maybe people haven’t seen *Citizen Four*, for example... but if you watch closely in credits, they thank a number of **FOSS** projects, including Debian, Tails, Tor, GnuPG, and so on and so forth.

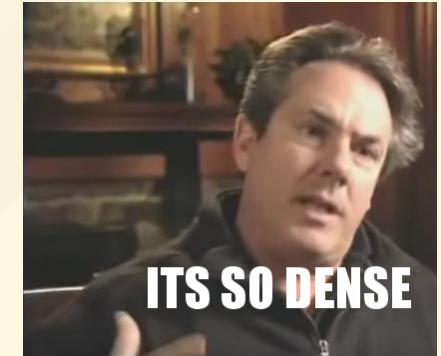
And that’s because what happened in 2013 **would not have been possible without Free Software**. I did not use Windows machines when I was in my operational phase because I couldn’t trust them.

”

– Edward Snowden, [\*keynote at LibrePlanet 2016\*](#)

# These Slides are Detailed

This is a presentation **and** a guide.



[Grab a copy here](#) ➔

Refer back to it later, read it slowly, & click the links.

- If you don't do everything in the demonstrations or fall behind, that's okay. **Learn 5 new things.**
- If you don't have a computer/phone, or it's acting up, make a friend in the room and follow along.

**Sharing is Caring:** Please copy, share, and remix!

# TL;DR - Shorter, DIY Version

- Watch these three videos on [privacy](#), [Free Software](#), and [Tor](#).
- Try [Jitsi Meet](#), [DuckDuckGo](#) or [StartPage](#), and [Up1](#).
- Use [Cryptocat](#), [Ricochet](#), or [Tor Messenger](#).
- Install [uBlock](#) or [Adblock Plus](#) and [HTTPS Everywhere](#).
- Browse with [Tor Browser](#) and use [OnionShare](#).
- **Android only:** Install [F-Droid](#). Use [Orfox](#), [Silence](#), [Kontalk](#).
- **iOS & Android:** Try [Signal](#) instead of Silence and Kontalk.
- E-mail via [Tutanota](#) or [Protonmail](#), or [follow this PGP guide](#).



# Etherpad for Live Q & A

Let's name a new pad at <https://pad.riseup.net>

...this pad will self-destruct in 30 days.

- This is "Security by Obscurity".  
**Do not** type info in the pad you wish to remain private.  
If the pad name is guessed or shared, anyone can view it.
- [Riseup.net](#) hosts awesome services.  
Donate if you can, they almost had to shut down in 2016.

Other options:

[Mozilla's public Etherpad](#) | [Try Ethersheet for spreadsheets](#)

# Why Privacy Matters

**It's not about "having something to hide"**



[Watch on YouTube](#) ➔

# Snowden Documents

## Major takeaways:

### 1. The Bad News:

All popular communication services have been compromised by **government and corporate surveillance**. Mass data collection, software backdoors & exploits, government information requests, data breaches.

### 2. The Good News:

Snowden was able to communicate extremely sensitive information despite this, using a combination of **FOSS** and Operations Security (**OPSEC**) training.



# Bad News

## Many services still compromised

### Say 'Hi' to the NSA in Your Next Email

Sources say Yahoo let government malware scan the contents of all emails sent to Yahoo accounts. And why would the feds stop with Yahoo?

Andrea Castillo | October 11, 2016



EMAIL | SHARE ▾ | PRINT

It's been a rough month for Yahoo. Within a few weeks, the struggling tech-company was accused of undermining its customers' security and privacy, after a massive hack of user-data from 2014 was followed-up this fall with allegations of involvement in an unprecedented government surveillance program. The question now is whether more tech companies are secretly complying with federal orders to spy on us.

#### RELATED ARTICLES

[DOJ USES VAGUE COURT REQUEST TO TRY TO DEMAND](#)

For Yahoo, the woes started in late September, when chief information security officer (CISO) Bob Lord delivered some harsh news on the firm's official Tumblr account: Yahoo



Dominic Lipinski/ZUMA Press/Newscom

In 2016, we learned Yahoo! had new spy software for the NSA. That year, 500 million Yahoo! accounts were also breached.

# Good News

More privacy software, easier to use than in 2013

Social Networks	
Proprietary	Free Recommendations
 Facebook	 <b>buddycloud</b> Open source, federated social network. <small>Servers</small>
 Google+	 <b>diaspora*</b> Community-run, distributed social network. <small>Servers Web Services</small>
 LinkedIn	 <b>friendica</b> Distributed, federated social network. <small>Servers</small>
 Twitter	 <b>GNU social</b> Self-hosted, decentralized social network. <small>Servers Web Services</small>
	 <b>Hubzilla</b> Hubzilla is a powerful platform for creatin... <small>Servers Web Services</small>
	 <b>Movim</b> Private, decentralized social network ser... <small>Servers Web Services</small>
	 <b>pump.io</b> Self-hosted social stream server. <small>Servers</small>
	 <b>RetroShare</b> Secure P2P communications platform off... <small>BSD GNU/Linux OS X Windows</small>
	 <b>Salut à Toi</b> Multi-frontend, multipurpose communica... <small>Servers</small>
	 <b>Syndie</b> Distributed, anonymous forum software. <small>GNU/Linux OS X Servers Windows</small>

A list of alternative social networks from [PRISM Break](#).

# What about iPhones, WhatsApp, Facebook?

Some U.S. corporations now encrypt some communication, making **mass surveillance** like PRISM difficult.



- Why trust these companies? Fool me twice, shame on me.
- On Facebook & WhatsApp, your **metadata** and **social graph** are stored and studied.
- Apple knows **who** you talk to, even when they don't know **what** you say to them.

This data can be used for **targeted surveillance** by police and intelligence agencies.

# Demonstration:

## Hands-on with

# Jitsi Meet

# Secure Audio/Video Chat

Let's name a new room at <https://meet.jit.si>

...this chat room will self-destruct when everyone leaves.

- Peer-to-Peer and End-to-End Encryption
- Password-protected rooms, no user limit, screen sharing
- Built-in Etherpad, text chat, optional YouTube streaming



Other WebRTC options: [appear.in](https://appear.in) | [Talky](https://talky.chat)

# Making First Contact

## Establishing a trusted connection

Privacy tools require **trust** and a **shared secret**. That secret could be a username, a URL, a passphrase, or an encryption key.



- Share a secret using tools you learn about today.
- Meeting in person may be the best method.
- Etherpads, pastebins/imagebins like Up1, and "burner" temporary e-mail accounts are good options.

Try to use **Tor Browser** or **Orfox** for first contact  
(*we'll cover this later*).

# Demonstration:

Chatting with

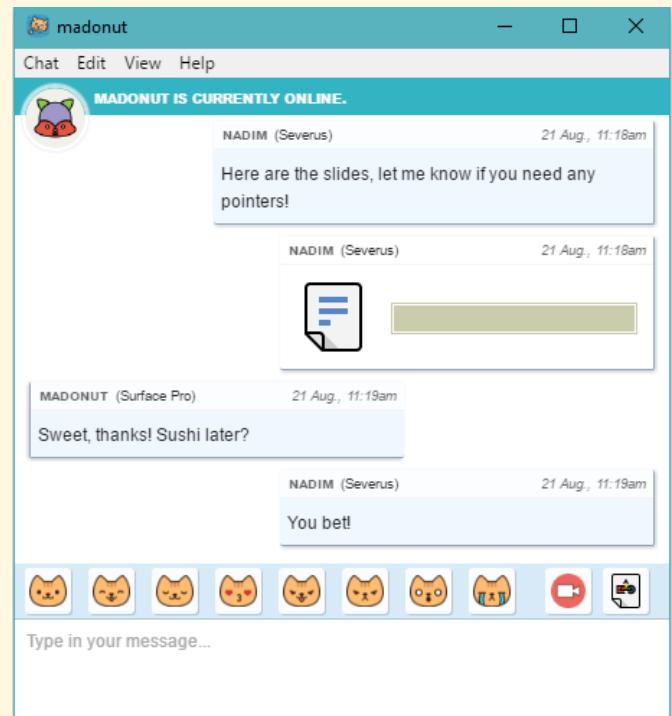
Cryptocat

# Secure Instant Messaging

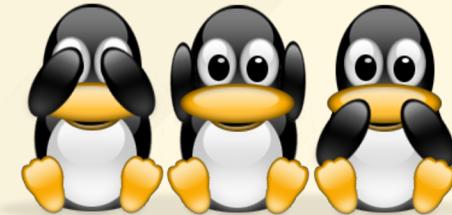
Download & install from <https://crypto.cat>

Choose a (non-identifying) username. Share it with the person to your left, add them as a buddy.

- End-to-End Encryption and Forward Secrecy
- File sharing, including video and large files (though it may be slow).



# Off The Record (OTR)



Text chat/IM is very safe, **if configured correctly**.

**Jabber (XMPP)** is the basis for most IM (Google Chat etc.) but you need a trusted service provider. Try [DuckDuckGo XMPP](#), or join [Riseup](#), [MayFirst](#), or the [Free Software Foundation](#).

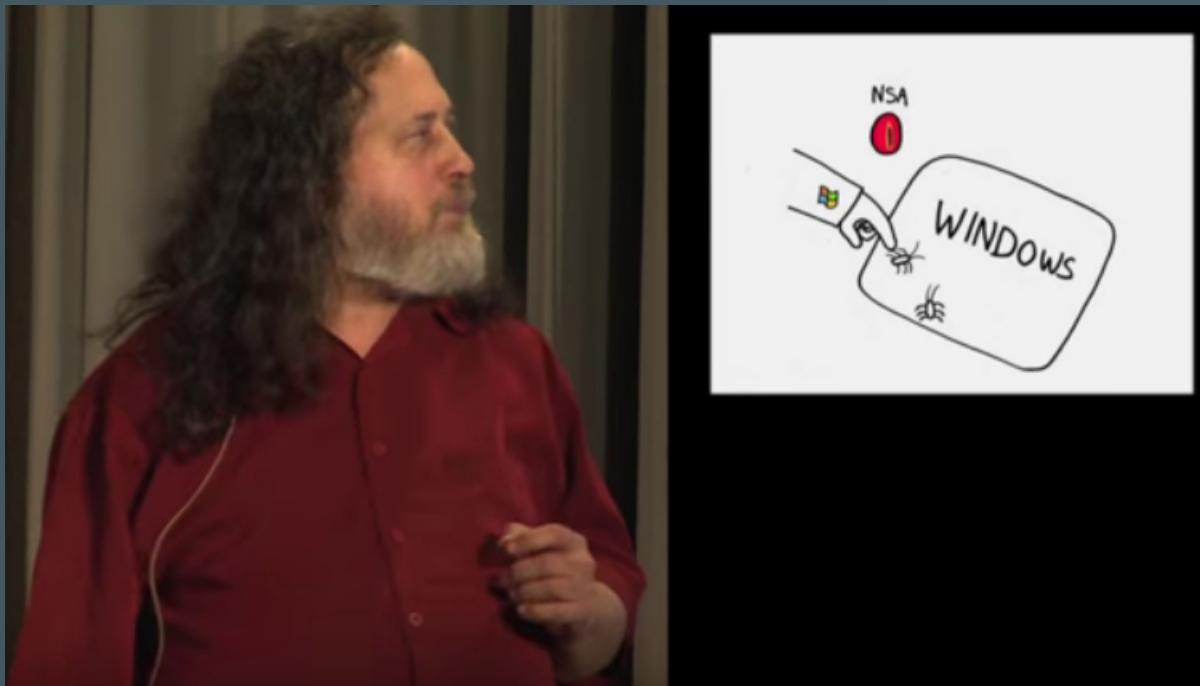
Use [Pidgin](#) (Windows & Linux) and [Adium](#) (Mac) with XMPP. Check the settings and make sure you're not logging chats.

**Set up OTR** for truly private XMPP. [Follow this OTR guide](#)

**Too complicated?** Try [Ricochet](#) or [Tor Messenger](#).

# Free Software in context

Digital security requires software freedom.



[Watch on YouTube](#) ➔

# Picking Ain't Easy

Start by eliminating proprietary software and services with **advertisements**.



- Ads are not only obnoxious, they may inject malware, even **if** developers try to avoid it.
- Favor GNU GPL and other Free Software licenses.
- Read the EFF messaging scorecard, Wikipedia, FOSS community reviews, & online forums.
- Look for warrant canaries & transparency reports.
- Browse Tactical Tech & resources listed later.

# Demonstration:

Focus on

# Better Browsing

# Browser Warning!



We'll focus on Firefox (Iceweasel/IceCat).

Mozilla values privacy & has a solid track record.

**Why not Google Chrome?** Most of the following tips will also work on Chrome & Chromium (100% FOSS version). Chrome contains **proprietary** code, has serious privacy issues, and reports back to Google several ways even if you try to opt out.

**Can I trust Chromium?** Maybe. Webcam/microphone spyware has been included with Chromium (not just Chrome) in the past, but it has since been removed. You will have to turn off the Google defaults and avoid Google services, however.

# Breaking Ads

Try these addons & tweak the settings.

[How to install](#) | [How to remove addons](#)



- **Essential:** [uBlock](#) or [Adblock Plus](#), [HTTPS Everywhere](#)
- **Recommended:** [DuckDuckGo Plus](#), [HTML5 Vid Everywhere](#)
- **YourMileageMayVary:** [Privacy Badger](#), [Disconnect](#), [LibreJS](#)
- **For the Adventurous:** [NoScript](#) (turns off all JavaScript)
- **Facebook users:** [FacebookBlocker](#), [Facebook Disconnect](#)  
**Warning:** Facebook is a surveillance network and even casual communication is carefully studied.



# Better Search w/ DuckDuckGo

DontTrack.us: problems with Google, contrasted with DDG.

DontBubble.us: filter bubbles, which DDG doesn't create.

**!bangs**: Allow you to search other sites. These searches originate from DDG's servers, masking your identity.

edward snowden !g

Google

chelsea manning !w

Wikipedia

richard stallman !yt

YouTube

debian gnu linux !gi

Google Images

Other search engines: [Startpage](#) | [Disconnect](#)

# Mo Passwords, Mo Problems

Here are some password strength, storage, and retention strategies.



**Passphrases:** Can be a favorite song lyric, movie quote, or joke. I would also add numbers and special characters:

Cecil+Harambe4ever

**Strength:** Follow these guidelines on [password strength](#)

[\*\*KeePass\*\*](#) (Windows/Linux) or [\*\*KeePassX\*\*](#) (Mac): Organize your passwords in an encrypted database.

**Browser Password Manager:** [In Firefox](#) | [In Chromium](#)

# Onion Routing via Tor

Be truly anonymous on the Internet.



[Watch on YouTube ➔](#)

# Demonstration:

Try out

Tor Browser Bundle

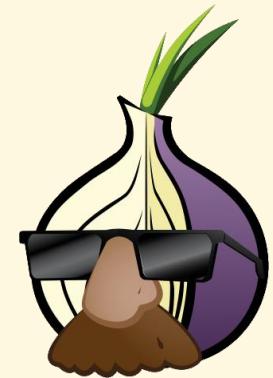
# Anonymous Web Browsing

## Download Tor Browser Bundle

It's Firefox, but anonymous! Security plugins pre-installed.

### Tor is the standard for anonymity.

The Tor network thwarts the NSA's best efforts to break it (we know this [thanks to Snowden](#)).



- **However:** Using Tor is not a magic bullet. Vulnerabilities may occur over time, so **update often** (TBB will nag you!)
- **TBB Settings:** Go with the defaults. Customization makes you more susceptible to [browser fingerprinting](#).
- **Bridges:** [Use if Tor is blocked](#) or you need extra protection. 27

# Rolling in the Deep

Wikileaks submissions and other anonymous [.onion](#) services run on the Tor network.



Use TBB for the "normal" Web **and** the [Deep Web](#).

Try it In TBB: [thehiddenwiki.org](http://thehiddenwiki.org)

[Onionshare](#): Easy way to share files via .onion URLs.

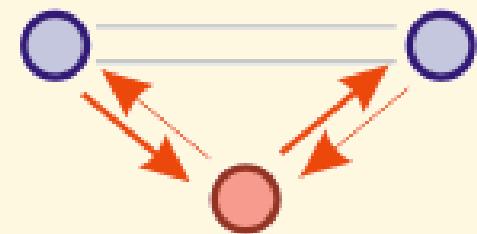
Other Deep Web networks: [I2P](#) & [Freenet](#)

**Remember:** True security and anonymity requires hard work and careful actions to get right ([OPSEC](#)).

# "Forget Tor. Just use a **VPN**"

VPNs route traffic through a ([trusted?](#)) computer but do not provide the anonymity & security of Tor. Free ([gratis](#)) VPNs may be malicious. Most reputable VPN accounts cost money.

- [What is a VPN good for?](#)
- Look for a [warrant canary!](#)

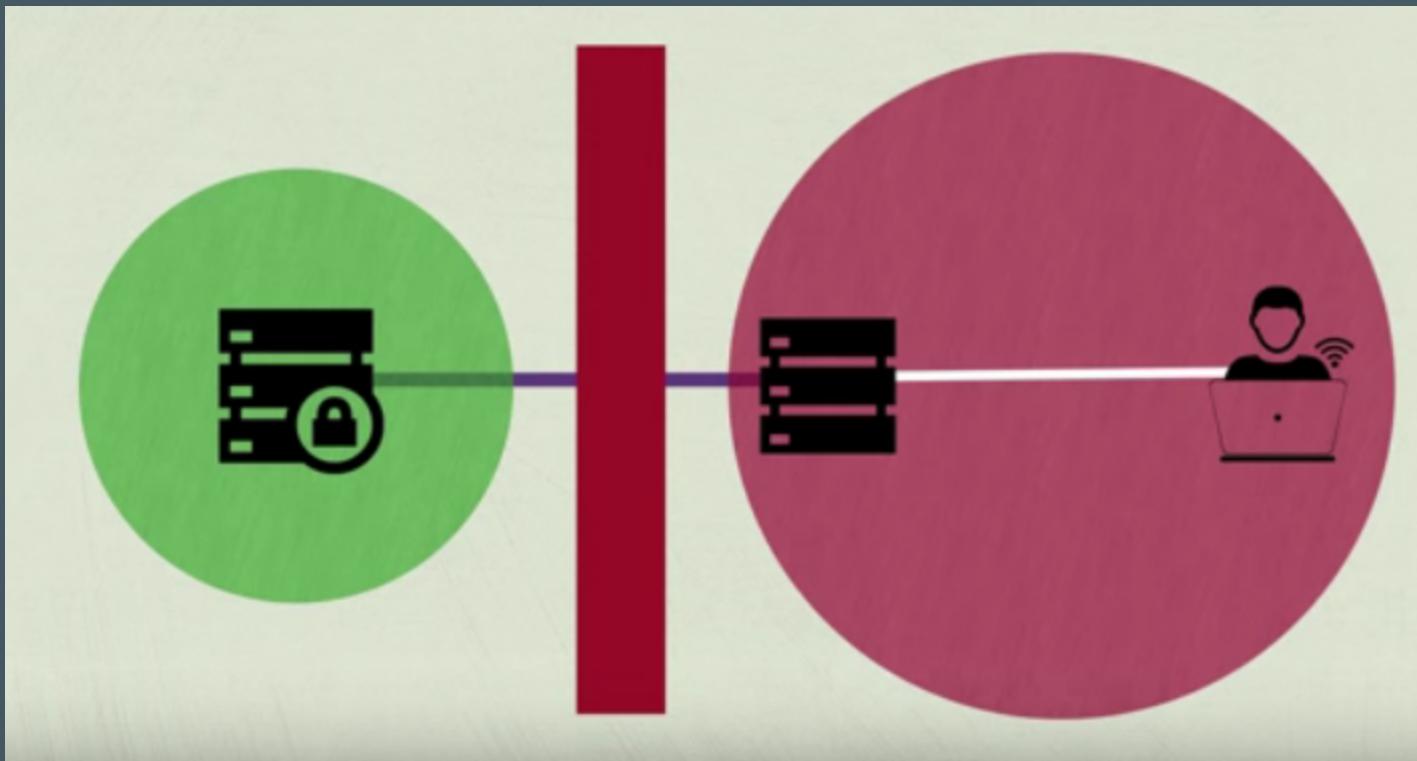


**Do your homework before trusting any service.** Choices:  
[Riseup Red](#) (legacy) | [Riseup Black](#)

[VPN.ht](#) | [PIA](#) | [Doublehop](#) | [AceVPN](#) | [CyberGhost](#) | [SumRando](#)

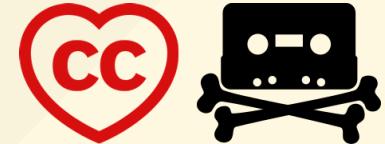
# How a VPN Works

Watch this before you try any VPN.



[Watch on YouTube ➔](#)

# Sharing Is Caring



...but love is a battlefield. Practice safe sharing.

Use [OnionShare](#) for single files. P2P / BitTorrent requires trade-offs: speed, anonymity, ease-of-use, size of network.

[RetroShare](#) | [Tox](#) | [GNUnet](#) | [Tribler](#)

**Remember:** Sharing may run contrary to copyright law in your country.

- Share copyleft, [Creative Commons ShareAlike](#) & [Free Culture](#) works.
- BitTorrent over Tor is a [bad idea](#) & may [de-anonymize](#) you.
- Set up [blocklists](#) to block potentially-malicious peers.

**Dropbox-like solutions:**

[SparkleShare](#) | [SpiderOak](#) (*some parts proprietary*)

# Demonstration:

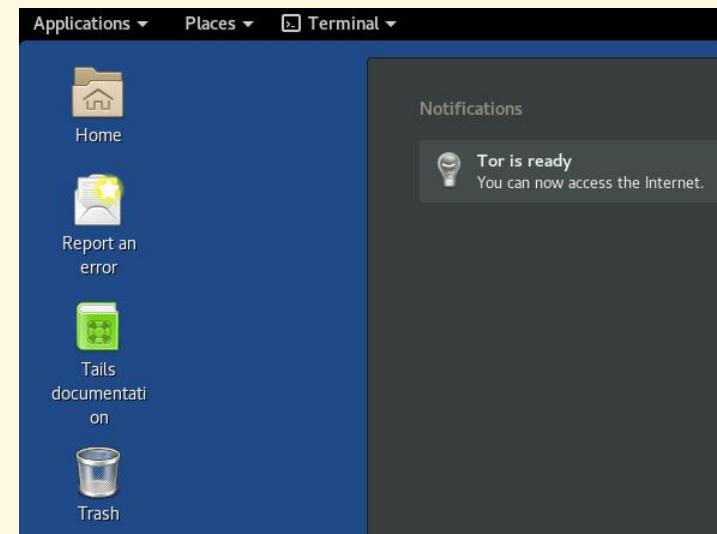
"The Amnesiac Incognito Live System"

Tails

# Tails is the Tor operating system

## Follow the [Tails Installation Assistant](#)

- Tails **does not use your hard drive**, or require any hard drive at all.
- Tails boots from USB stick, CD/DVD, or [virtual machine](#).
- You may optionally set up [persistent storage](#) for Tails.  
Otherwise, all files go **\*poof\*** when you shut down.



Not working? [Try Whonix](#).

In contrast to Tails...

## Windows can't be trusted.



- Surveillance is difficult or impossible to turn off.
- Microsoft gathers metrics on every Windows user (what users type, how long they browse, use apps, play games...)
- Bitlocker & SecureBoot: Microsoft stores your encryption key after the first time you use Windows Update, and there is a "skeleton key" backdoor in SecureBoot leaked in 2016.

Macs also contain proprietary software and have spying, control mechanisms, & DRM malware.

# Security Is Not Proprietary

Recall [Richard Stallman's TED Talk](#).



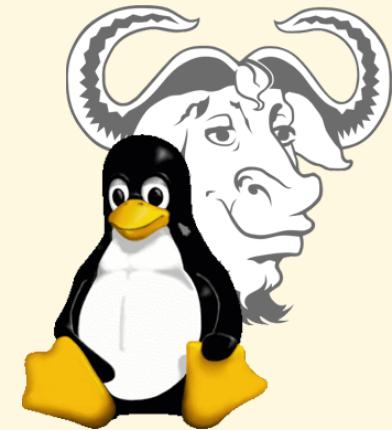
- Proprietary code is secret, often buggy and/or malicious.
- FOSS is a [basic requirement for security](#). Even then it requires "[many eyeballs](#)".

**Fortunately**, there is a lot of high-quality FOSS available, and many users, developers, & security experts worldwide.

# What Can the "Average User" Do?

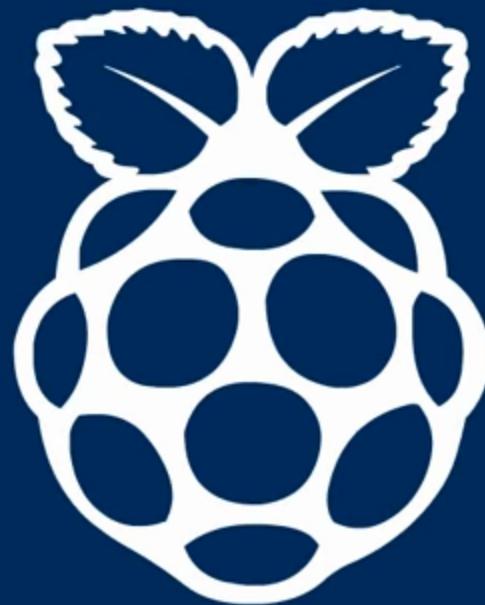
Try [GNU/Linux](#), a popular & friendly family of FOSS operating systems. [Tails](#) is only one member of this family, and may not fit your [threat model](#).

- GNU/Linux is installed on billions of [Web servers](#), [IoT devices](#), supercomputers, TVs, media centers, phones, tablets, & gadgets.
- Not only for [hackers](#) or bearded white men. [Many millions](#) worldwide use a [GNU/Linux Desktop](#).
- Similar features as [Mac OSX](#) due to its [Unix-like](#) design.



# What is "Linux"?

"Linux" explained, in four minutes.



[Watch on YouTube](#) ➔

# The GNU/Linux Distro For You



**Most libre** (no proprietary drivers, codecs, etc.)

[Trisquel](#) | [gNewSense](#) | [Guix](#) | [FSF list](#)

**Most popular** (big community == good support)

[Linux Mint](#) | [Ubuntu](#) | [Debian](#) | [Fedora](#)

**Some "favorites"** (list changes frequently)

[Xubuntu](#) | [Korora](#) | [Manjaro](#) | [Elementary](#)

**Very secure** (not for n00bs) [Qubes](#) | [Subgraph](#)

[DistroWatch](#) | [FSF common systems list](#) (mainly [Unix-like](#))

# What about my phone/tablet?



Let's concentrate on [Android](#) variants, which are based upon GNU/Linux.

**Stock Android is insecure.** It includes proprietary apps from [Google](#), the vendor (e.g. Samsung), & ISP (e.g. AT&T). It may have backdoors for [foreign spies](#).

**Some Android devices are restrictive.** Your current device may not allow you to "free" it. If so, [keep freedom in mind](#) for your next device.

**iPhone/iPads are restrictive,** with many pitfalls for security & freedom. If you must use one, [jailbreak](#).

# There is a world beyond Google.



# Finding a ROM

ROMs in the [modding](#) community are loosely equivalent to distros / [firmware](#).

- [Copperhead OS](#) - Security is the priority. Only available for Nexus phones.
- [Cyanogenmod](#) or [OmniROM](#) - For many devices.
- [XDA-Developers Forum](#) - More alternatives.



**Blackphone from [Silent Circle](#)** - Made by prominent security experts, relies upon proprietary services.

# Demonstration:

## Getting started with

# Apps



1. Install F-Droid, the FOSS app store for Android.  
You may have to "allow unknown sources".

2. Add the Guardian Project repository in F-Droid. GP offers privacy apps like ObscuraCam.

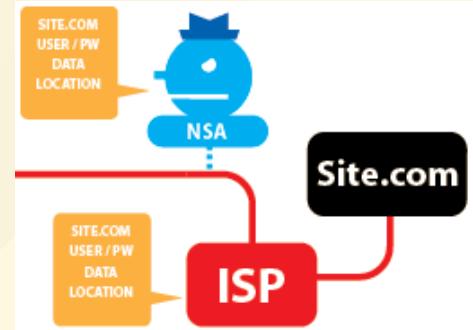
3. Install Orbot & OrFox, Tor and Tor Browser for Android.

4. Try Silence & Kontalk. Silence enables encrypted SMS/text.  
Kontalk is like a truly-private WhatsApp.

5. Search for other FOSS apps, like ad blockers.

What about Signal? Signal enables private calls / texts on Android & iOS.  
It requires a Google or Apple account & relies upon proprietary services.

# What about my Router?



Your gateway to the Internet may be insecure. Default router / modem firmware has many vulnerabilities and is often under attack.

- DD-WRT - FOSS firmware for many routers.
- Tomato - A family of FOSS firmware mods.
- OpenWRT - More like a distro for your router.

DNS vulnerabilities - OpenNic is an alternative DNS provider that routes around censorship and protects your network from DNS hijacking.

# Intro to Encryption

How math can keep us secure.



[Watch on YouTube →](#)

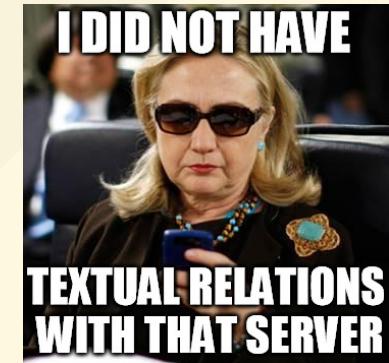
# Encrypt Your Storage

Encryption works, but is only as good as the implementation. FBI had a hard time getting into that iPhone. If they tried, Apple could get in more easily.



- Android & variants also have full-disk encryption.
- VeraCrypt is great for Desktop OS's and USB flash drives.
- Full-disk & home directory encryption are easy checkbox choices when installing all major GNU/Linux distros.
- More GNU/Linux options. Use Cryptkeeper for folders.

Above all, don't trust cloud storage like Dropbox.



# Plugging the E-mail hole

Expect large, consistent **data breaches**.

**Major e-mail providers can't be trusted.**

Even years after the Snowden disclosures, Yahoo! created new NSA wiretaps and leaked 500 million accounts. Google actively studies e-mails, even spying as you type.

**E-mail is a two-way street.**

Messages have to be private **on both ends**. Your buddy @gmail.com is giving the conversation to Google.

# E-mail is an easy target

jpodesta  
p@ssw0rd

- E-mail is often sent and received insecurely, yet users treat it as a secure channel.
- Inboxes are utilized for personal data storage.
- Weak passwords & password sharing is common, especially under work pressure.
- Junk/spam filters play a cat-and-mouse game.
- Phishing scams are increasingly-sophisticated.

**Don't assume spies are too cool for phishing.**

Malware sent via e-mail is a common tactic.

# Demonstration:

Up and running with

# Encrypted E-mail

# The Road to Private **Webmail**



Create a [\*\*Tutanota\*\*](#) account. Use **Tor Browser** if you can.

- **Pros:** Very easy to use, encrypts **metadata** (subject, sender, recipient) as well as **message content**. Android & iOS [apps](#).
- **Cons:** Encryption only to other Tutanota addresses. Can't download your mail locally via **POP** or **IMAP**.
- [\*\*Protonmail\*\*](#) is a similar service, with encrypted, [\*\*password-protected e-mail\*\*](#) to non-Protonmail users.

Tutanota & Protonmail are **not as flexible or popular as PGP**. They work best if everyone uses the same webmail provider.

# You Down with PGP? Yeah, GnuPG!

Install [Thunderbird \(Icedove\)](#) and follow the [E-mail Self-Defense Guide](#) to try [PGP](#).



- **Pros:** The standard. Use almost any e-mail address. Easy [key sharing](#). Multiple [trust models](#). Allows for download.
- **Cons:** More complex to set up than webmail-only solutions. No privacy for metadata / e-mail headers / message subject.

**Keep It Local:** Get your e-mail off of someone else's servers!

Use [POP](#) or [IMAP](#) to download in a mail client like [Thunderbird/Icedove](#).

**E-mail Hosts:** Try [Riseup](#) or [Mailfence](#), or [browse this list](#).

Mailfence has easy Gmail, Yahoo!, & Office365 import, quick [PGP setup](#), and has [calendar / document sharing](#). Some features require paid account.

# Avoid **Web** Publishing Traps

Sharing isn't just about conversations.  
The Web is for publishing *World Wide*.



**Social networks** like Facebook are walled gardens with constant surveillance. Consider federated social networks.

Find trustworthy hosting for Websites, Blogs, & Wikis. Big hosts like WordPress.com censor and take down websites.

- MayFirst is great for activists and has defense from DDoS.
- Consider Tor Browser users and turn off CloudFlare.
- Set up SSL/TLS via Let's Encrypt to protect your users.
- Don't force users into ad networks just to view & comment.

**Remember:** Etherpad and Up1 for quick copypasta.

# Secure Comms Strategy

**Make a plan and stick to it.**



- The **What**: Choose a few crypto, sharing, & publishing tools.
- The **How**: Try these tools, figure out how they work.
- The **Where**: Find safe places to share secrets, on & offline.
- The **When**: Describe scenarios when you will use each tool.
- The **Why**: State clear reasons to use each tool.
- The **Who**: Identify "experts" who can help & teach others.

**The Only Constant Is Change!** Try new software, keep up on tech news & potential threats, and re-evaluate over time.

# Resources

- Free Software Foundation: [fsf.org](http://fsf.org)
- Tor Project: [torproject.org](http://torproject.org)
- Electronic Frontier Foundation: [eff.org](http://eff.org)
- [Digital Security For Journalists](#)



[Cryptoparty](#) | [Riseup](#) | [Tactical Tech](#) | [PRISM Break](#)

[MayFirst](#) | [Encryption Works](#) | [Reset The Net](#)

[Digital First Aid](#) | [H-Node](#) | [DRM-Free](#)

**[Digital Security Helpline](#)**: 24/7 multilingual support

# Sources

