

TECH TOOLS FOR ACTIVISTS

Published : 2014-09-09
License : None

TECH TOOLS FOR ACTIVISM

1. AN INTRODUCTION TO THIS BOOKLET
2. SECURING YOUR EMAIL
3. ANONYMOUS BLOGS AND WEBSITES
4. MICROBLOGGING BEYOND TWITTER
5. BROWSING THE INTERNET
6. ORGANISING AND NETWORKING
ONLINE
7. MOBILE PHONE SECURITY AND
ANDROID APPS
8. PUBLISHING AND NETWORKING NEWS
9. PRODUCING AND PUBLISHING MEDIA
TO THE INTERNET
10. GREEN COMPUTING
11. HIDING & DELETING THINGS ON YOUR
PC

1. AN INTRODUCTION TO THIS BOOKLET



This booklet will help you to:

- use email securely
- publish news and upload media anonymously
- make your web browsing more anonymous and secure
- use Facebook and Twitter more securely
- get organised online without relying on corporate social networking sites
- use encrypted messaging on mobile phones
- hide stuff on your computer so it can't be found
- find a more secure and decentralised replacement for Twitter
- support free software, open licences and decentralised/federated communication.

Why this booklet is important:

This booklet provides an introduction to the effective use of technology for activism, with links to step-by-step guides and further information. It is written with a UK focus; we invite people to translate it to their own languages and cultures.

The tools discussed here could be of use to:

- journalists wanting to protect themselves and their sources
- researchers investigating corporate and state wrong doing
- NGOs, charities and campaign groups
- local environmental or pressure groups
- anyone communicating digitally who doesn't trust the authorities of tomorrow

Free Software and Free Network Services

Nearly all of the tools discussed in this booklet are free software based. Free software programmers dedicate millions of hours to writing virus-free, highly secure software that respects your privacy. You may already know Firefox, OpenOffice, and GNU/Linux operating systems such as Ubuntu and Mint Linux, which are used by hundreds of millions of people worldwide.

The free software we discuss is free to use; you can also see how it works, adapt it and redistribute it freely. These rights are protected in the software's license, usually the GPL (General Public License). If you change and re-distribute free software, you must release your changes under the same license so that everyone benefits. <http://ttfa.net/gpl>

Free software is written by people who see software as inherently political, the goal to ensure that we retain control over our own information infrastructure. ttfa.net/freesoftware

"The long revolution is creating small federated microsocieties, true guerilla cells practising and fighting for this self-management. Effective radicality authorises all variations and guarantees every freedom." Raoul Vaneigem

The same philosophy can be applied to online **network services** - social networking and video sharing sites such as Facebook and YouTube. Many people are creating free network services which support federation and freedom for the information users contribute; these issues are explained in a talk by Eben Moglen, "Freedom in the Cloud". ttfa.net/freecloud

Introduction to safer communication

Over the last two decades the information revolution has radically changed the way political activists communicate; but alongside the new opportunities, there remains the age-old problem of how to get information to your allies confidentially. Using an alias (or aliases) is an equally old but still effective security technique.

As long as very few people know the connection between your online and real identities, it will not be easy to discover your identity if your alias is incriminated. This requires having an email provider who will not (or cannot) disclose your personal details if they are pressured by the police. Communicating securely is everyone's business. Even if your activism is currently legal, you can help make the internet safer for everyone and help the "open web" with some of these security practices.

2. SECURING YOUR EMAIL

What you can learn from this chapter:

- differences between independent versus commercial email providers
- how to sign up for an activist email account and mailing lists
- how to encrypt your email.

WHY USE INDEPENDENT EMAIL?

Email is decentralised and therefore can be very secure. However, many people use less secure forms of communication such as commercial webmail providers (Google, Hotmail, Hushmail etc.) and social networking sites. Be aware that these companies will:

- log your usage and hand over all your data to the authorities on demand
- reserve the right to terminate your account as they see fit.

Happily, there are alternatives. **Independent email** services are run by media activist collectives such as **riseup.net** or **aktivix.org**, who understand the need for privacy, anonymity and trust. Unlike corporate providers, they will not give your emails to the authorities without a warrant and a legal fight. If that happens, they will make it public if they can, so you (and thousands of other activists) will know about it.

Independent email providers provide a web interface over an encrypted connection, and encrypt all messages sent between themselves; an email from an aktivix user to a riseup user is encrypted both as it's composed and when it travels between aktivix and riseup.

Sign up for independent email

Signing up for an independent email address is not an immediate automated process, because of spammers. For example, **aktivix.org** issues email addresses through a friend-of-a-friend basis. If you know someone with an **aktivix.org** email address, you can fill in the sign up form at **www.aktivix.org**

Alternatively, you can sign up for an account at **riseup.net** or **autistici.org**. You will need to fill in a short form letting them know why you want the email and they normally respond in 24 hours.

WHY USE INDEPENDENT EMAIL LISTS?

A dedicated mailing list can handle large email lists which you can't manage manually. People can subscribe to or unsubscribe from the list and the server handles security, privacy and archiving; members of the list don't automatically know the email addresses of all the other members. Lists provided by activist collectives are only as good as their weakest point: if just one address is "@googlemail.com", you can't consider the list to be secure.

If your list is small enough to manage manually, remember to use the **BCC** (blind carbon copy) field for their addresses rather than the To or CC fields. This keeps every recipient's address private.

Set up an email list

Collectives that provide **mailing list services** include the following: aktivix.org, riseup.net, autistici.org. We recommend aktivix.org. Email **aktivix-request@lists.aktivix.org** to request a list; stating your request simply in the subject line (e.g. "Subject: request for list for XYZ group/purpose") makes it easier to separate from sp@m. Not all names are possible, so be prepared to change. Think about the following points when creating a list:

- open or closed: can anyone subscribe or do subscriptions need to be approved?
- public or private: is the list to be advertised to the world, or is it run on a need-to-know basis?
- announce or discussion: is the list for receiving information only or for discussing something?
- moderated or not: are posts to the list to be moderated?

ENCRYPTING YOUR EMAIL

If you are concerned about privacy but not using a secure webmail service, are communicating with someone who is not, or want an addition of level of personal security, you can encrypt your email.

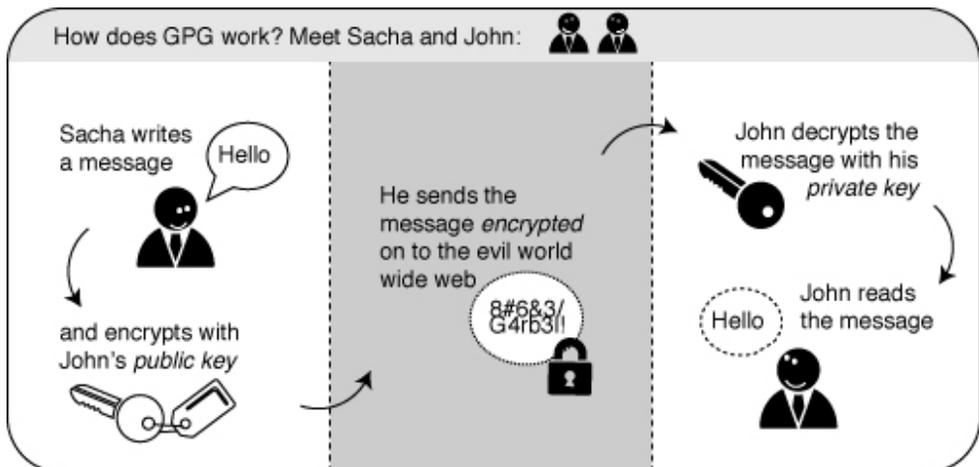


Encryption is the process of taking a plain text message and converting into something that looks like gobbledygook, which can be decrypted and read by the intended recipient. The free software tool of choice for this is called **GPG (GNU Privacy Guard)**. Many people find GPG tricky, so be prepared that it may take time - but it is worth it.

GPG encryption uses pairs of numbers called **key pairs**: a public key and a private one. You give your public key to anyone you wish to have encrypted communication with, but keep your private key absolutely secret, as it is used to decrypt email sent to you. It is so secret that it needs protecting with a **passphrase**, which is basically a very long password.

By encrypting email using the recipients' public keys, the sender can be assured that only the authorised recipients will be able to read it - **privacy**. If the email is signed by the sender's GPG key, the recipient can be assured of the identity of the sender - **authenticity**.

Step-by-step instructions to set up and use GPG with the Thunderbird email client can be found in the book Basic Internet Security and there is an online course which TFA run at P2PU.org; you can even earn a badge. imc.li/ttdpz



WHAT NEXT?

- Try to set up an email account with aktivix.org, riseup.net or similar.
- Encourage your contacts to set up secure Email accounts.
- Try using GPG encryption.

3. ANONYMOUS BLOGS AND WEBSITES

"According to the statement provided to the Court on 22nd November 2010 ... Automattic Inc (WordPress) were prepared to make a 'voluntary disclosure' of the website's creator [and] did not appear to question the sheer extensiveness of the UoS request for information within this 'Document request' ... this is in my opinion, a clear breach of privacy and has far reaching implications for all bloggers who have an account with WordPress." Gary Duke, University of Salford lecturer sued for libel. ttfa.net/gary

This chapter will:

- recommend secure blogs and websites
- discuss the issues of anonymous blogging
- explore different ways and tools to blog anonymously

Issues with mainstream blogging sites

Many activists and campaign groups use free blog sites such as Blogger.com or Wordpress.com. However, these sites log IP addresses that reveal users' identities, and can be required by court decisions to reveal this information. There have been cases where Wordpress.com has handed over identities of bloggers and taken down websites on request of the authorities. Fortunately, anonymous blogging is possible (see also the chapter on using VPN, Tor and other ways to browse the internet anonymously).



Use secure blogging services

We define "secure" as not logging IP addresses or any details of those who are uploading to or viewing the site.

Network23.org is one secure blogging service; they do not log any personal data, apart from your email address for password resets. You can sign up for an account from an independent email (see the chapter on email for more information) for complete anonymity. Other blogging services that don't log IP addresses include <https://blogsport.eu> and <https://noblogs.org>

Get more secure hosting

Wordpress is free software that you can install on your own server. If your server is configured correctly, and you install the **remove ip** module for Apache [ttfa.net/removeip], you can ensure your blogs do not capture users' personal data. Other website software such as Joomla or Drupal can also be set up in this way.

Tachana.org offer secure privacy-conscious website hosting to radical and grassroots groups internationally. ox4.org was set up by activists in the Oxford area who "like doing activism, supporting activism infrastructure, and techie stuff". Their level of security is not as high as Tachanka.

Wordpress Networks

If you want to set up your own anonymous blogging service, a **Wordpress Network** is a good way to save time and effort. This is a multi-user set-up which reduces the site administrators' workload: when you update the code for the main site, all subsites are also updated.

The process of using a Wordpress network blog is nearly identical to a normal Wordpress blog. There is a basic help guide on the FlossManuals site: ttfa.net/flosswp

WHAT NEXT?

- sign up for a free secure blog or website at Network23.org
- encourage people and groups to move insecure blogs to better hosting
- work with trusted friends to set up your own anonymous blogging service (if you're a bit techie)
- install the remove ip module on your server

4. MICROBLOGGING BEYOND TWITTER

"Imagine my surprise this morning when, without warning, my shiny new Twitter account (@d_seaman) was suspended and taken offline. My crime? Talking too much about Occupy Wall Street ... [and] the controversial detainment without trial provisions contained in the FY 2012 National Defense Authorization Act (NDAA)." ttfa.net/twitsuspended

This chapter will:

- explain the issues and limitations of Twitter
- show the advantages of Status.net
- encourage you to sign up to identi.ca or indy.im

THE LIMITS OF TWITTER

In recent years Twitter has been an invaluable tool to human rights campaigners and a great source of activist news. But its centralised structure makes it subject to pressure from the authorities to release personal information of Twitter users. ttfa.net/twitsubpoena.



STATUS.NET

Status.net is a microblog service similar to Twitter, but it's decentralised: you can have an account on identi.ca or indy.im, or you can run your own Status.net installation.

Sign up for an account on <https://identi.ca> or, if you know someone who uses <https://indy.im>, they can invite you to use that service - it is invitation only to avoid spam users. Both of these communities have a vibrant user-base; indy.im is more activist oriented, while identi.ca is wider with a lot of computer enthusiasts.

Status.net has some neat features; you can:

- attach pictures or video to posts without using third parties like twitpic or plixi
- create/join groups; posts to a group go to all its members, if they are following you or not
- take an RSS feed from a blog and bring its latest posts into your timeline using brdcst.it
- install a Status.net app to read and update from a smartphone.

How is Status.net useful for activists?

Using Status.net via <https://indy.im> or <http://identi.ca> allows you to update your Twitter status. Once you have signed up for Twitter using anonymous browsing, you don't need to return to these sites. You can then 'tweet' without revealing your identity. This is possible because:

- your connection is encrypted; your network provider cannot see the content of your updates
- Twitter will see the IP address of indy.im or identi.ca, not your own IP address
- indy.im **does not** log IP addresses; it cannot tell where an update is coming from
- the imcli link shortener does not log IPs, anyone clicking your links will not be tracked

Follow these steps to connect:

- log into Twitter and identi.ca (or indy.im)
- go to your identi.ca settings and click on the *Connections* link at the top of the page
- click on the *Twitter* tab & enter the details of your Twitter account & click "Authorize app"

The default preferences allow you to automatically repost your 'dents' from identi.ca to Twitter. You can change other settings under the *Twitter* tab which allow you to use Twitter but from within the more secure environment of a status.net account.

You can follow up this process by cross posting to a Facebook account or page from Twitter. In this way you are able to make anonymous updates to corporate social networks that normally log your details.

WHAT NEXT?

- Sign up to [identi.ca](#) or try to get an invite for an [indy.im](#) account.
- Try to get cross posting to your Twitter account working.
- Try using [brdcst.it](#) to add blog / web updates into the mix.

5. BROWSING THE INTERNET

In this chapter we look at ways to browse the internet anonymously using:

- anonymous networks (PAYG and public wi-fi)
- better search engines than Google
- Linux and an open source browser to reduce sharing personal information
- a public proxy and other methods for anonymity
- browser Add Ons to make browsing safer.

Visiting a website on the internet leaves a trail of information, both on our own computer and on the **server** (the remote computer that **hosts** the website): who we are, what we are looking at, when we looked at it and what pages we visited before and after the site we are currently looking at.

Most websites log your **IP (Internet Protocol)** address: this number is uniquely linked to you, via your ISP (Internet Service Provider). The police, scammers or advertisers use IP addresses to find out who has looked at what site and when. Browser software also discloses all sorts of information about itself, and, therefore, about you too, without you knowing it. There is more information on this in an interview here: ttfa.net/anonymizer. Taking steps to browse the internet anonymously allows you to:

- circumvent restrictions imposed by the state (or your boss) on what you can access
- avoid being traced when you visit or upload to websites
- avoid leaving a trail of visited sites visible to authorities, advertisers and scammers.

Approaches to using the internet anonymously

Using an internet cafe, library or public wifi avoids having a single IP address connected to you. However, these places may require ID (library card, passport or drivers licence) and/or have CCTV. There are no technical methods of security that are 100% reliable but there are a number of technical approaches to increased anonymity online. If you have techie friends, ask their advice; or join a mailing list in the further info chapter.

Here are some things to think about and pointers to more information:

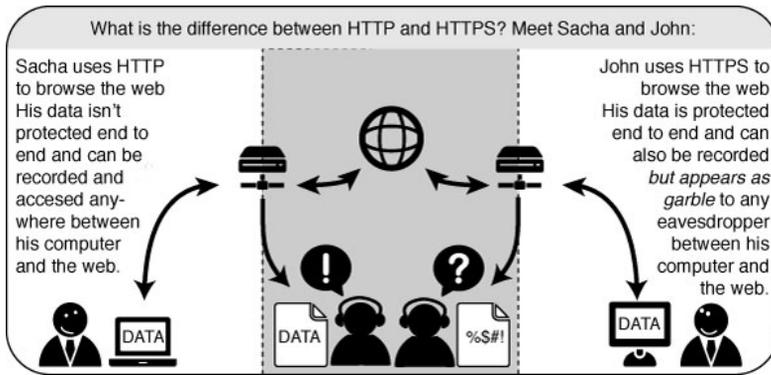
- Can the network you are using be linked to you? If you use a public wi-fi hotspot, or if you buy a **pay-as-you-go 3G adapter** with cash, and then credit it with top-up cards bought with cash (check for CCTV in the shop), there is less chance of leaving a trail of evidence that leads to you.
- Your browser and operating system store a lot of information about you; we recommend using **Firefox on a GNU/Linux system** to limit and manage this.
- A **Linux live CD** allows you to run Linux straight off a CD (or USB stick) on any PC. All your activity is stored in the computer's memory, leaving no trace when it is rebooted. **TAILS** is a great example. tails.boum.org
- You can hide some information about your network location by using a proxy (a computer that fetches web pages for you on your behalf) or better still a network of proxies and routers like the **TOR (The Onion Router) project** - a great description of using TOR is here. ttfa.net/usingtor
- Using a **Virtual Private Network (VPN)** may be a possibility for you. VPN and **tunneling** are techniques for encrypting data connections between yourself and another computer. ttfa.net/vpn

Better search engines

Google logs your IP address and collects, stores and sells information about you and your web activity. There are better alternatives, such as: Duck Duck Go - duckduckgo.com & Ixquick - www.ixquick.com.

MAKE YOUR BROWSER SAFER

We recommend using the Firefox browser; there are other good ones but Firefox (or some of its close relations) have great Add Ons as we will find out.



https is a form of encryption for browsing the web. You can tell if it is being used as you will see "https" instead of "http" at the beginning of the URL in the address bar of your browser. **Https Everywhere** is an Add On which forces your browser to use https everywhere it can: ttfa.net/https

Adblock Plus blocks advertisements on websites, but it also can be used to block other content that may try to track you. Adblock Plus relies on blacklists maintained by volunteers. adblockplus.org

Set a master password on Firefox: Firefox can remember your internet passwords - but this is a real security threat. Open Firefox preferences, select the security icon and check the "use a master password" box; more info here. ttfa.net/ffpassword

NoScript: this extension blocks all JavaScript, Java and other executable content that could load from a website and run on your computer, protecting you from threats such as cross-site scripting (attackers placing malicious code from one site to another) and clickjacking (clicking on an innocuous object on a page reveals confidential information or allows the attacker to take control of your computer). Visit noscript.net/getit for more information.

 **Flagfox** puts a flag in the location bar telling you where the server you are visiting is probably located. ttfa.net/flagfox

 **BetterPrivacy** manages **cookies** used to track you while visiting websites. Cookies are small bits of information stored in your browser; some track the sites you are visiting for advertisers. ttfa.net/betterprivacy

 **GoogleSharing** - If you are worried about Google knowing your search history, this extension helps prevent that. ttfa.net/googlesharing

WHAT NEXT?

- Read the online resource Basic Internet Security. ttfa.net/bis
- Install Firefox and learn how to extend Firefox with add-ons to ensure safer browsing.
- Try using TOR or a VPN.

6. ORGANISING AND NETWORKING ONLINE

Perry Sutcliffe-Keenan, 22, of Latchford, Warrington, used his Facebook account in the early hours of 9 August 2011 to design a web page entitled The Warrington Riots. The court was told it caused a wave of panic in the town. When he woke up the following morning with a hangover, he removed the page and apologised, saying it had been a joke. His message was distributed to 400 Facebook contacts, but no rioting broke out as a result.

This chapter will look at

- Social Networking Sites, issues and alternatives
- Anonymous Instant Messaging

Tools like Facebook, Google, Yahoo, Wordpress.com and many other Social Networking and email services have well documented security implications. It is so common for the state to spy on people using these services that they have easy-to-use guidebooks to make this more efficient. For an example of a document detailing how this works see ttfa.net/facbook.doc

There are several advantages to using Facebook to organise campaigns;

- There is no cost to using it
- There are high levels of engagement with the service
- Users are used to using the system to show support for campaigns

There are also disadvantages;

- Your account or campaign group / page may be suspended at any time
- Your details and those of any supporters are available to a wide number of authorities
- You are supporting a centralised networking system which almost certainly doesn't share your values

There is a great guide which gives tips about how you can change the default settings to use Facebook more securely for organising. The length and detail of this guide ironically shows us how difficult Facebook make it for you to operate with a reasonable level of security. The guide is here ttfa.net/fbguide

MORE SECURE TOOLS FOR ORGANISING AND NETWORKING ONLINE

If you are concerned about these implications of organising online and do not want to exclude people who are careful about their privacy, then there are alternatives you can use. Using these tools is also a great way to support a more decentralised and non-corporate future of communication.

Crabgrass

Crabgrass is a Free Software web application run by an activist tech collective called RiseUp who will protect your security and anonymity as, like you, they are all activists working for radical grassroots change. The site that they provide at we.riseup.net uses a piece of software called “Crabgrass”, which is an activist equivalent of a social networking site. It allows you to create groups, work collaboratively on documents, be as private or as public as you want to be (and even have a different private and public profile), control who can and can't be in the group based on whether you actually know them or not, and communicate securely by sending each other private or group messages.

You can also do live chat in a more secure way by using Crabgrass chat. When you are logged in to Crabgrass you can go to the Chat page (located on the main menu at the top). You can only chat with people that are members of groups that you have joined.

For more information on Crabgrass see ttfa.net/crabgrass

Instant Messaging - Internet Relay Chat (IRC)

The details of your Live chat provided by Yahoo, Windows, Skype and Gmail are regularly made available to law enforcement agencies.



IRC is a tried and test way of live / instant message chatting. Users install an IRC client or connect via a webpage and it is possible to chat in an encrypted way. A

lot of techies, free culture and software enthusiasts, media activists, hacker and crackers use this technology.

XChat is a great IRC programme which comes with Ubuntu and is easy to install on Mac. MIRC is an equivalent for windows.

Try it out by contacting us. You can log into the *irc.indymedia.org* server and join the channels #ttfa and #aktivix and say hi! Have a look at the settings in this Xchat network to be able to do this in an encrypted way. Note the /6697 port used for Secure (encrypted) communication. There is more information about IRC and getting it set up here - ttfa.net/irc

Instant Messaging - Using Off the Record Encryption & XMPP

There is an open standard for Internet chat called XMPP (formerly known as Jabber) this is a great decentralised alternative to tools like Skype and MSN messenger. It can also be extended to do all sorts of things like video chat, android phone chat, and most importantly for us, encrypted chat.

The first thing you will need an application that can use Xmpp

Hands On Guide: Have a look at this guide to using Pidgin and OTR encryption. It has a focus on entry level users and is targeted at Windows. imc.li/flsyj

Diaspora, Friendika and Distributed Social Networks

Diaspora got the attention of many when it raised over \$200,000 in contributions when the team offered to build an open and decentralised facebook. In short the time for the '*distributed social network*' had come and people were prepared to chip in to fund it.



The key to the success may lie not in any particular bit of software but in the ability for lots of different software to be able to talk to each other using open standards. If you think about it why shouldn't you be able to talk to friends and reshare their content across different networks. You can with email, why not with social networking.

There are many alternatives to Diaspora, these include friendica, jappix and movin.

They may operate in different ways but the aim is roughly the same. The following is a quote from the friendica home page.

*"The internet is our social network. What if social networks were more like email? What if they were all inter-connected, and you could choose which software (and even which provider) to use based purely on what they offered you? **Now they are!** Friendica is bringing them all together"*

The concept here is that that you can have news of the activities of different friends from different networks and websites all coming into one stream on friendica and interact with them from one place.

This is a great step forward in recreating the positive experience of using a site like facebook and you can be an early adopter. You can try a couple of the projects out and see how they work for you. There are several sites that are running friendica where you can sign up. There is a list of them here. dir.friendica.com/siteinfo

Other Networking Tools are available which embrace distributed ways of social networking and organising. **Lorea** is a software distribution consisting of the [Elgg open source social network engine](#) and a handful of plugins. Find it at lorea.org.

There is also a very impressive project called **Kune** which is similar in scope to Crabgrass but with more advanced features for networking and a public face for your projects. Find out more at kune.ourproject.org

While there is no simple replacement for Facebook at the moment there are lots of promising projects happening all over.

Don't forget Email & Mail lists & Microblogging

These areas are covered in other chapters but included here as they are so useful . Email is a great way of organising. You can be sure of who is sending email. It can be encrypted. You can set up your own email server or use one of a trusted group to be sure of its security. Using Email can bypass a lot of the security issues of organising online.

Twitter sells information about its users to third parties, is caving into government censorship and has started to suspend accounts. You use open source alternatives like identi.ca. See the chapters on securing your email and and microblogging for more information.

What Next?

- Get a secure Email address!
- Install and try out IRC.
- If you use Facebook check your settings and make it more secure.
- Set up a Status.net account on Indy.im by trying to get an invite from someone already on there or sign up at identi.ca
- Sign up for Diaspora, Friendica or a similar task and try it out.
- Use aktivix.org for emails lists.
- Set up a an account on Crabgrass (we.riseup.net)

7. MOBILE PHONE SECURITY AND ANDROID APPS

In this chapter you will learn;

- Some background info on mobile phones and security
- How to send encrypted SMS messages on an Android phone
- How to set up a VPN on an Android phone to allow safer browsing

Mobile phones are effective tools for organising and increasingly for documenting protest and political activism. While this is very exciting, the technology shouldn't be embraced blindly. The following information drawn from the Guardian Project website and Basic Internet Security book outlines some of the risks of mobile use and ways to overcome these threats.



SECURITY ISSUES WITH MOBILE PHONES

Physical security - A phone can be confiscated or stolen. If you are an activist, your address book and past SMS messages might be of special interest and/ or incriminating; it can be used just to gain knowledge of your network or for further social engineering. As a minimum safety measure you should always enable some kind of password protection on your phone (not just on your SIM card).

Voice - Although the voice on a GSM (mobile phone) channel is encrypted, this encryption was hacked some time ago and is not considered safe any more. Furthermore, if you do not trust the network(s) you are using it has never been safe.

SMS - Text messages are sent in plain text over the network, so they are also not considered secure, additionally they are not securely stored at your device, so anyone with access to it will be able to read them. If you are using an Android based phone read the section on 'Secure Text Messaging'

Smartphones - Smartphones are quite new, and unfortunately most advanced (and even some basic) ways of securing that are available on normal computers are not available on smartphones. They pose additional risk since you are also using them for things like agendas, and personal note taking. There are a considerable number of *malware* apps on the market which are passing your personal data to other companies. Check if your app's can be trusted.

Prepaid sim cards - In some countries you are still able to use prepaid locally bought SIMcards without identifying yourself. Beware that your phone also has a unique identifier (known as the IMEI number) so switching SIM cards will will not guarantee to protect your privacy.

USEFUL ANDROID APPS

The **FDroid Repository** is a catalogue of FOSS applications for the Android platform. Their website is a great first port of call if you are looking at installing some tools for your phone - <http://f-droid.org/>



Orbot: Anonymous Web Browsing

Orbot brings the capabilities of [Tor](#) to Android. Tor uses Onion Routing to provide access to network services that may be blocked, censored or monitored, while also protecting the identity of the user requesting those resources.



Orweb: a browser with increased privacy

Orweb is a privacy enhanced web browser that supports proxies. When used with [Orbot](#), Orweb protects against network analysis, blocks cookies, keeps no local browsing history, and disables Flash to keep you safe.



Gibberbot: Private and Secure Instant Messaging

Gibberbot is a full featured instant messaging application integrated with the [“Off the Record”](#) encrypted chat protocol. Our app is built on Google’s open-source Talk app and modified to support the Jabber XMPP protocol.



ObscuraCam: Secure Smart Camera

A secure camera app that can obscure, encrypt or destroy pixels within an image. This project is in partnership with [WITNESS.org](#), a human rights video advocacy and training organization.



Proxy Mobile Add-On

A [Firefox for Android Add-on](#) which exposes HTTP and SOCKS proxy settings through a new options menu. This enables the user to connect with Tor through [Orbot](#), as well as any network proxy service.



Data Wipe (“Poison Pill”)

Often individuals working as advocates and organizers can be detained by authorities in order to to gain access to information, leaving the data they are carrying unprotected and easily compromised.



K-9 and APG: Encrypted E-mail

K-9 Mail is an open-source app based on Android’s built-in Email app. The project is focused on making it easy to manage multiple accounts and large volumes of email, as well supporting OpenPGP encryption using [Android Privacy Guard](#).



CSipSimple: Encrypted Voice Over IP (VOIP)

CSipSimple is a free and open source SIP client for Android that provides end-to-end encryption using ZRTP. It’s compatibility with desktop SIP clients such as [jitsi](#) makes it an ideal solution for secure voice calls on android phones.



TextSecure: Short Messaging Service (SMS)

TextSecure, developed by [Whisper Systems](#), provides a robust encrypted text messaging solution, but it is only compatible with other TextSecure users.

SETTING UP A VPN ON AN ANDROID

PHONE

VPNs were mentioned in the section on browsing the internet safely. For instructions to set up a VPN on an android phone see here - <https://imc.li/mwkpj>

WHAT NEXT?

- Try setting up encrypted email on your phone with K-7
- Why not organise a mobile phone cryptoparty? A gathering where you test and skill share the use of some of these tools

8. PUBLISHING AND NETWORKING NEWS

In this chapter you will find out about;

- publishing news anonymously
- using tagging and Search Engine Optimisation to help people find your news
- using RSS and aggregation tools to help network news

The Internet has made it easy for everyone to publish news. Anyone can set up a blog or start twittering. This can make reaching your audience more challenging. Network Internet services which let you share your news often keep a record of who is visiting and updating your news site. This can cause security problems and legal problems as well.

POSTING ANONYMOUSLY

Blog sites like wordpress.com and blogger.com and social networking sites like Facebook keep a record of who uses their site. They do this by collecting the IP addresses. There are two easy solutions for posting your news anonymously. You can use Tor to post anonymously (see chapter "Organising Online"), or you can post to websites which do not log your IP.

Website and blogs hosted on certain independent servers: There are a number of services that host your website or blog anonymously, like noblogs.org and network23.org. There are also hosting providers that don't log IP addresses and can help you with security and anonymity issues. See this page for more info - ttfa.net/hosting



Indymedia and other secure open posting news sites: Indymedia volunteers coordinate the production and sharing of news content often ignored by mainstream media. The global IMC network is based on openness and broad participation: all software is Open Source, most lists are publicly archived, everybody can sign up to the wiki, log-on in chatrooms, or publish various newswire as long as it does not breach the guidelines.

NETWORKING NEWS

There are many different independent media collectives and individuals who publish news that is ignored by mainstream media. We can help spread the reach of this news by republishing it in anyway we can.

Tagging your content and SEO: Making sure your content shows up in search engines like Google has become a science called Search Engine Optimisation (SEO). Search Engine Optimisation is made easier by using Content Management systems like Drupal, Joomla and WordPress. SEO works better if you tag well.

Tagging your content makes also it much easier to find. If you use tags, your news can then be classified, better indexed by search engines, and via RSS feeds the content can be pulled into other websites (aggregation).

RSS and aggregation: Syndication offers some potential for posting anonymously. RSS feeds are an agreed standard to allow different sites to pull in and republish content from other sites. You could publish your news anonymously on Indymedia - which uses tagging, and an RSS feed - to republish it onto your convenient (but insecure) wordpress.com site.

Reposting or ReTweeting news: One of the reasons that blogging and Twitter really took off was that communities of bloggers or tweeters with similar interests would retransmit news from there peers by commenting on, linking too, writing supportive posts or simply just repeating their news. We shouldn't be shy to do the same with news of activism with the tools we have. Blogs, imported RSS feeds, repeating Twitter or Status.net posts and cross posting them to social network sites are all a vital part of getting the word out there.

be the media

Bethemedia.org.uk website: In the UK the Be The Media website aggregates news from many different media collectives and campaign groups. The goal is to be a node on the network of independent news which gathers and retransmits independent news. The sources page of BTM is a good first stop when looking for such sources in the UK.
ttfa.net/btmsources

WHAT NEXT?

- Find your local open-publishing news collective or start one up.
- Network your news, tag, repost and retweet till it hurts (in a good way)

9. PRODUCING AND PUBLISHING MEDIA TO THE INTERNET

This chapter will cover;

- Issues about using corporate media sharing sites like YouTube
- How to edit and upload images, audio and video using free, open and independent tools
- Adding videos to online subtitles

The Problem with YouTube (and similar services)

Corporate media sharing services like YouTube has vast potential audiences and are rich in features but there are a lot of videos on YouTube viewed by hardly anyone too. If you put in effort you could just as well build an audience in other ways. YouTube could suspend your account at any time. There are quite a few other corporate 'Web 2.0' services that offer a lot of functionality and provide a high degree of usability. However, none of the commercial services can be relied upon to offer anonymous posting and/or viewing.

Sharing Images

Many people who use Facebook are unhappy about what the licence you agree to allows Facebook to do with your images. If you use alternative image sharing website like Flickr to upload images you are able to choose your own licence. You may also want to try out a WordPress blog to upload and present your images. There are many themes specifically designed for uploading images (also known as Photo Blogging). Hosting images on your own blog gives you complete control over the licence and distribution of your images.

Adding Subtitles to online Video



Amara, created by the Participatory Culture Foundation [universalsubtitles.org], is a toolkit that makes it easy to add subtitles to any video on the web. Universal Subtitles uses only web standard technologies, specifically HTML5 and JavaScript, so it will be

accessible in nearly every browser.

To subtitle a video for Amara, your video first needs to be online. Once the video is uploaded, visit: <http://universalsubtitles.org/videos/create>

Once your video is uploaded and subtitled, it is easy to insert your video into any WordPress page or post. For full details on how to do this visit ttfa.net/unisubs.

Video & Audio sharing services

Archive.org contains thousands of digital movies ranging from classic full-length films, to daily alternative news broadcasts. All these movies are available for download, often in very high resolution, and are freely licensed. You can embed the video into other websites, but you can not create an RSS podcast there. They support open formats like Ogg video.

VisionOnTV.net is not a service where you can upload video. It does however help to promote Grass roots video reports and provides tips and training on how to make short videos using low cost tools. Get in touch with them if you have videos to share.

Engagemedia.org specialise in video from the Asia-Pacific region but are open to international video as well. They fully support and promote subtitles and open video formats.

Editing and Encoding video and audio

Audio editing and encoding: Audacity [ttfa.net/audacity] & Ardour [ttfa.net/ardour] are audio editors that can import, edit and export audio in a number of different formats. Audacity is a great starting application and Ardour is aimed at multi-track recording.

Video encoding: HandBrake [ttfa.net/handbrake] and Avidemux [ttfa.net/avidemux] are cross platform encoders which can convert DVDs and large videos files for archiving and distribution.

Video editing: For free software the situation is much worse for video editing. On Linux our recommendation is Kdenlive [kdenlive.org] which the most stable and usable option.

WHAT NEXT?

- Stop telling us what to do already we get the idea!

10. GREEN COMPUTING

This chapter will cover;

- Why should I worry about Green & Low Power computing?
- Ways of reducing power use and prolonging the life of your computer

Background Information

If you are concerned about the environment you may ask yourself. "Where does my computer come from and where does it end up?" The answers to these questions are unsettling. The issues of resource wars over Coltan [ttfa.net/coltan] and other heavy minerals and associated pollution caused by the production, energy use and disposal of computers [ttfa.net/waste] lead many of us to worry about our increasing use of computers, mobile phones and other gadgets. At the same time no-one really wants to be struggling with an old computer that takes forever to do simple tasks.

There are different ways to reduce the impact of your computing;

- prolonging the life of your computer and reducing power use
- buying low impact hardware and reusing old computers

Reducing Power use and prolonging the life of your computer

Install a resource saving operating system: Operating systems like Windows, OSX use a lot of processing power. A version of Linux (Ubuntu or Mint Linux) will use much less resources, less power and which therefore prolong the life of your computer. There are also specialised versions of linux like the popular Lubuntu (using LXDE) which aim at reducing the use of resources even further. These are

Turn off Wireless if you are not using it: Wireless is a very significant source of power use in computers and especially laptops. Why not get some Cat5 cable if you have a home network.

Reduce screen brightness and other tips: Ideally reduce the brightness of your screen. You can also have the screen automatically switch off after a short period of inactivity. There are also other power management settings like spinning down hard drives. You can set the graphics chip to it's lowest usable resolution. You might also want to disable 3d acceleratio. It's also worth mentioning the powertop utility.

Using Low-Impact Hardware

New Hardware: Examples of low energy hardware. LED monitors and small computers with no moving parts like the ones featured here - <http://www.aleutia.com/products>

It may be better environmentally to get a new low power set up than to recycle older computers. You can learn how to assess the embodied energy of different products by totalling up the impact of the manufacture, shipping and other factors.

Reusing Old Computers: Power use is not the only consideration when thinking of low-impact computing. Saving older computers from landfill and prolonging their life is a most valid thing to do.

An **LTSP** set up may be useful to reuse older hardware and if low power laptops can be sourced. LTSP stands for Linux Terminal Server project [ltsp.org]. The computers (often old and low power laptops) are run as 'thin clients' meaning the hard processing work is all done by one computer on the network. Laptops can be run without batteries from a shared power source. These factors save a lot of power.

There are many factors involved in reusing old computers. The best way to learn is just by trying it out. See if there are any community groups in your area that can train you to do it. Here are some very quick tips.

- keep a store of old hard-drives, power supplies, sound cards etc to use in computers that have missing or broken parts
- check the wattage (power use) of the computer you want to re-use (some old computers are very power hungry)
- Try underclocking the chip if you want a very low power computer for a media server etc
- install a low power version of linux on the computer if it is old - you'll be amazed how much quicker it runs



Re-using computers is a fantastic activity to do as part of a community project and there are some great examples out there. One example is the Access Space project in Sheffield, UK. [ttfa.net/as]

11. HIDING & DELETING THINGS ON YOUR PC

During the controversy over the Iran-contra affair, in 1986, Lieutenant Colonel Oliver North attempted to erase all the relevant e-mail messages on his computer; he repeatedly pressed the DELETE button, thinking that he was thereby expunging the messages. "Wow, were we wrong!" he later observed

After reading this chapter you will have the knowledge to;

- delete files and data securely so that no-one will recover them
- encrypt information on your computer
- give you an introduction to the encryption software TrueCrypt

Deleting Files Securely

With a harddisk even if you erased every piece of data, it is sometimes possible with (very) specialized hardware to recover pieces of the data. If the data is very confidential and must be erased with the greatest care, you can use software to "overwrite" all pieces of data with random data. When this is done multiple times, this will make the data untraceable.

Securely delete data under Windows: For Windows there is a good open source tool called "File Shredder". This tool can be downloaded from fileshredder.org

Securely delete data under MacOSX There are basically two build-in steps to make to securely delete your data on Mac OSX. You can find out how to do this here - ttfa.net/delete

Securely delete data under Ubuntu/Linux Unfortunately currently there is no graphical user interface available for Ubuntu to delete files secure. There are two command-line programs available though - **shred** & **wipe**.

Shred is installed in Ubuntu by default and can delete single files. **Wipe** is not installed by default but can easily be installed with using Ubuntu Software Center or if you understand the command line you can install it with `apt-get install wipe`. **Wipe** is a little more secure and has nicer options. It is possible make access to these program's easy by adding it as an extra menu option. There is more information on this here - ttfa.net/wipe

Hiding Files

There are three basic solutions for hiding files - **physical hiding**, **encryption** and **misdirection**. Physical hiding would mean using a portable medium such a USB key and keeping it in a secure location, only to be brought out for editing. Encryption is another solution which does not require any physical movement of media. Encrypted data cannot be read directly and must go through some kind of unlocking in order to be useful. Misdirection, hiding in a place on a device (i.e. a hard disk), a filesystem, or within another file or container, where nobody would think to look..

Using True Crypt

The tool **TrueCrypt**, which is is available for Window, Mac and Linux, uses both encryption and misdirection. **TrueCrypt** will protect your data from being accessed by locking it with a password that you will create. If you forget that password, you will lose access to your data! **TrueCrypt** uses a process called encryption to protect your files. Rather than encrypting specific files, **TrueCrypt** creates a protected area, called a *volume*, on your computer. You can safely store your files inside this encrypted volume. There is help online for installing, encrypting and using hidden volumes using True Crypt as part of the [Basic Internet Security book](#).

UPDATE: The developers of True Crypt have stopped working on the the project. While many are looking for an alternative in the long term, a software audit by @OpenCryptoAudit is that version 7.1a is safe to use. [It can be downloaded here.](#)

More Tips

Encrypting in Ubuntu: Ubuntu and offers the user the chance to encrypt the home directory and your entire drive during the installation process. The installation wizard will ask you to choose the partitioning method where we need to choose the 'Guided – use entire disk and set up encrypted LVM' option to encrypt our entire hard disk.

Virtual Memory: On all modern operating systems (e.g. Linux, Windows or OS X), there exists a feature called virtual memory. If you are not encrypting your entire hard drive you must also encrypt the pagefile or swap space to prevent people from reading the virtual memory.

When encryption doesn't work: If your computer/laptop has been bugged or compromised in some way and your keystrokes are being recorded, it doesn't matter how good your cryptography is. Using a secure operating system which prevents keylogger installation (such as Linux), is a useful first step towards enhanced security.

WHAT NEXT?

- Try out some of the software and techniques listed here.
- Spread the word about how to securely delete files.
- Try running a workshop on how to securely delete files
- Install TrueCrypt and try encrypting drive and creating hidden volumes
- Try encrypting your drives when you next install Ubuntu