Security in-a-box provides the knowledge you need to recognise digital security threats and the tools you need to address them. It offers detailed, step-by-step instructions to help you use those tools effectively, as well as practical, non-technical advice for anyone who relies on digital technology to do sensitive advocacy work.

https://securityinabox.org
https://tacticaltech.org
https://frontlinedefenders.org

TACTICAL
TECHNOLOGY
COLLECTIVE

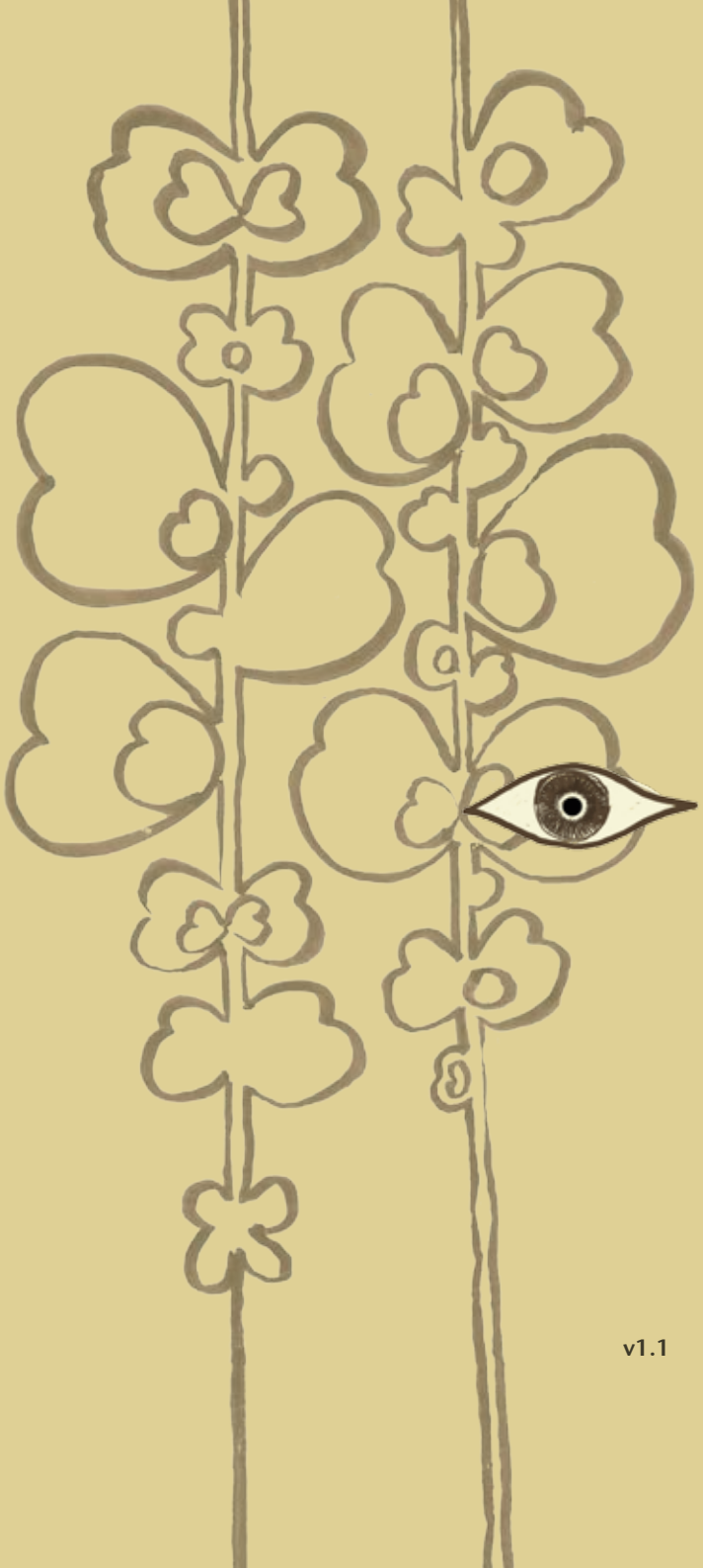
Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

ISBN 978-90-80-76901-3

TOOLS AND TACTICS FOR ADVOCACY

# security in-a-box

## community focus



v1.1

# security in-a-box

## community focus

**digital security tools and tactics for environmental rights defenders in sub-Saharan Africa**

TACTICAL TECHNOLOGY COLLECTIVE

TOOLS AND TACTICS FOR ADVOCACY


This guide was developed by
the Tactical Technology Collective

**Research and writing (Part I)** Samuel Maina
Coordination: Daniel Ó Clunaigh

**Writing (Part II)** Wojtek Bogusz
Dmitri Vitaliev
Chris Walker
Ali Ravi
Daniel Ó Clunaigh
Hadi Habbal
Anne Roth

**Special thanks** to the many human rights defenders who have contributed their inspiration, feedback and stories to the creation of this guide.

**Design & illustration** Lynne Stuart

**Funders** American Jewish World Service

v1.1: September 2014

## CONTENTS

# 1
# Introduction

# Introduction

## BACKGROUND

In many remote regions of sub-Saharan Africa, natural resources such as oil, gas, minerals, timber, agricultural land, forests, wildlife and water are found in abundance.

Communities living in these regions often depend on the land for their livelihoods.

These communities and the ecological environments on which they depend are, however, frequently disregarded by the multinational companies which, in partnership with governments, explore and exploit these resources.

Out of this situation, a community of environmental rights defenders (ERDs) often emerges, made up of people from both within and outside the local community.

ERDs aim to make sure that the extraction of natural resources does not harm the environment and is even of benefit to the local community. They work to defend the ecosystems affected, as well as the people dependent on these ecosystems, from unfair resource exploitation, environmental degradation, land grabbing and pollution.

ERDs also take it upon themselves to mobilise community support and take action against environmental rights violations, and to advocate for transparency in agreements and payments made between governments and private companies for natural resource extraction.

ERDs are sometimes framed by these same companies and politicians as enemies of development - sometimes even criminals. Governments often try to stop ERDs from doing their work so that resource exploitation can continue. Companies often try to stop them so that they can continue reaping profits without due diligence.

To achieve these goals, governments and companies can use digitally-obtained information to attack, harass or disrupt the work of these defenders. This can include information obtained through breaking into accounts with weak passwords, obtaining computers and smartphones through theft or raids, monitoring communications such as e-mails, text-messages or calls, and exploiting vulnerabilities in social networking accounts. Digital security is therefore crucial, in addition to personal and organisational security.

A June 2014 assessment of the digital security status of ERDs in Sub-Saharan Africa, however, revealed that this group has limited digital security knowledge and remains largely unaware of the digital security loopholes that can be exploited by adversaries to harm them or disrupt

their work.

This guide has been developed to lead you towards developing a digital security strategy that you can add to other security measures you are taking.

## ERDS IN SUB-SAHARAN AFRICA: DIGITAL SECURITY RISK AWARENESS

ERDs in Sub-Saharan Africa are mostly unaware of the digital security risks they face, and this makes them vulnerable.

A needs-assessment survey conducted in June 2014 found that of the 20 organisational representatives surveyed, only three demonstrated sufficient knowledge of digital security risks.

> ***Digital security knowledge among activists working on resource extraction is very low and they need a lot of support to harden systems.***
> Anonymous Human Rights Defender, Uganda

When asked if they faced any digital security risks, most responded, "Not that I am aware of."

There is a clear need for digital security materials, outreach, and training, to equip ERDs with a better understanding of their digital security risks as well as the technologies and tactics available to them to minimise these risks.

### *Using this guide*

We recommend starting with the first chapter, which goes through the basics of digital security, before advancing your knowledge in the later chapters.

The guide is designed to be read together with selected chapters in **Security in-a-Box**. In most cases, links to the relevant chapters are provided.

### What you can learn from this guide

This guide has been created specifically for Natural Resource Defenders, and explains the primary tactics and technologies which will be most useful in this context.

This guide includes:

- Introduction
- How to assess your digital security risk
- Basic computer hygiene
- How to secure your online collaborations
- How to secure your files in "cloud storage"
- How to use your smartphone more securely
- How to make a distress call in emergencies
- How to protect your evidence

This guide, along with all **Security in-a-Box** toolkits and materials, will be subjected to reviews and updates. Please feel free to send us your feedback to security@ngoinabox.org.

# 2
# How to assess your digital security risks

## 3. How to assess your digital security risks

In order to know what measures to take in order to be more secure, both digitally and in our day-to-day personal and professional activities, it's important to understand the nature of the risks you face so that you can make the right decisions about how best to stay safe.

Perhaps without realising it, you take decisions based on risk analysis every day: you may choose not to walk home through a particular neighborhood you consider dangerous, or to lock your office doors when you leave in the evening, to deter thieves. The idea of this section is to consider that same logic, as it applies to your digital activities, both as environmental rights defenders and as private people.

### 'SECURITY' AND 'DIGITAL SECURITY'

Your risk assessment and strategies for staying safe shouldn't just relate to your 'digital lives' but should, of course, also include your personal, physical, organisational and emotional security.

Each of us has our own definition of what constitutes 'security'. Traditional notions of security would include ideas such as the protection of a state, region, building or information system from external attack. However, while these concepts are quite valid, it is increasingly recognised that 'security' for environmental rights defenders can also mean many more things, such as the freedom to carry out your work without restrictions, the freedom to travel without fear, physical and mental health, justice and recognition. [1]

This guide focuses on one subset of 'security', which we call 'digital security'. Digital security refers to ensuring the ability to use digital information and information systems without interference, disruption, unauthorised access or data collection. That is to say, having control over the storage, communication, use and access of your digital information.

Sometimes, you may want to share information publicly in order to stay safe: for example, you may share your location with your friends and support network via text message or a social network if you find yourself being followed. Other times, you may want to keep information secret in order to stay safe: for example, you may encrypt your email conversations with your partners when organising a meeting, so that the location isn't discovered.

Which measures you should take to keep yourself and your information safe will depend on your own risk analysis.

## 'THE WHO' AND 'THE WHY'

In order to understand the risks we face and be able to effectively react, first we should know where they come from; that is to say, who is behind them, and why.

In order to 'map' the actors relevant to our work and our well-being, we might consider dividing them into three categories:

- **Resisting forces:** These are actors who try to prevent us from successfully carrying out our work.
- **Supporting forces:** These are our friends and allies, who try to support our project in one way or another.
- **Unknown forces:** These are other actors whose exact intentions, with regard to our security and the success of our work, are unknown or ambiguous.

### *Resisting forces*

Unfortunately, as an environmental rights defender you cannot always count on the full support of your state, your society, or at times even your family. Your work to defend environmental rights is often a direct challenge to power structures, whether in government, society or the family, and directly threatens those who currently wield that power.

As an environmental rights defender, you are often challenging big corporations that are profiting from natural resources without due diligence with regard to communities and ecological integrity.

This means that a number of different actors may take action against you to hinder or stop your work. In some cases it may be agents of the state, who often threaten, arrest, detain, mistreat and prosecute environmental rights defenders.

You can also expect resistance from big corporations such as oil companies, logging concessions, plantations and mining companies, whose primary objective is to reap maximum profits from natural resources often without regard for community rights and ecological integrity.

Getting a sense of who these actors are will help you to understand the nature of the threats to yourself, your community and your information. Different actors will pose different threats to your security, and indeed your digital security: while the state, for example, may have the capacity to listen to your mobile calls, or place viruses on your computer to monitor your online activities, non-state actors or even common criminals could gather a huge amount of information about you by just monitoring your Facebook page, if everything is open and public. If you think about what you are up against, you can take the right measures to keep them guessing, and keep working.



### *Supporting forces*

As part of this 'actor mapping' exercise, you should also consider the actors who are on your side, whether local, regional or international: these could include friends, community members, police, other organisations, embassies and so on. It will be important for you to spread your digital security practices among your allies.

### *Unknown forces*

Finally, you should also consider the actors whose intentions are unknown, but who are relevant to your safety. An example may be your Internet Service Provider (ISP) or companies such as Facebook or Google, on whom we depend on for a lot of our online activities and who may collect and store a lot of information about us. For example, an ISP, social network or e-mail provider could be legally pressured by a government to hand over information such as your browsing history, chat logs or emails. Due to the large amount of information they collect about your activities, they may also be targets for malicious hackers who want to access that information about you.

### *Assessing Risk*

Risk refers to possible events, however uncertain, that result in harm.

You can think of your risk as an interplay of the **threats** you face, your **vulnerabilities**, and the **capacities** you have.

- **Threats** refer to a declaration or indication of an intention to inflict harm. The higher the threats, the higher your risk. An example of a threat may be someone breaking into your email account and exposing your contacts, or using your emails as evidence against you.
- **Vulnerabilities** refer to any factor which makes it more likely for harm to materialise or result in greater damage. The more vulnerabilities you have, the higher your risk. An example of a vulnerability may be having a very short, simple and easy to break password, like '123456', or your pet's name.
- **Capacities** refer to abilities and resources which improve our security. The higher your capacities, the LOWER your risk. An example might be knowing how to create and store long, complex and varied passwords, thus making it very difficult for people to break into your email account. See Security in-a-box *Chapter 3: How to create and Maintain Strong Passwords*. [2].

It's worth noting that capacities and vulnerabilities are often "two sides of the same coin".

### *Identifying threats, capacities and vulnerabilities*

To begin with, as noted above, it's good to consider the threats you face. Threats may be targeted, that is to say, directly or indirectly related to our work; or they may be incidental, that is to say, not related to your work but to other factors, such as common crime.

Threats can also be environmental, or structural in nature. Examples of such threats may include data loss due to a power outage, or natural disaster.

It's a good idea to map out the possible threats you face, and consider how they might relate to your use of technology – your mobile/smart phone, your computer, email, social networks, and so on.

Once you have mapped them out, you can think about your capacities and vulnerabilities relative to each threat. Capacities and vulnerabilities can fall into a huge number of categories - geographical, social, familial, physical, structural, economic, and others. For the purposes of this guide and your use of it, it may be useful to consider those which relate to your use of technology and digital tools in particular.

It may help for you to map them out on a matrix, like this:

| Threats | Who? | Vulnerabilities | Capacities | Capacities required |
|---|---|---|---|---|
| | | | | |
| | | | | |

| Threats | Who? | Vulnerabilities | Capacities | Capacities required |
|---|---|---|---|---|
| Office raid, confiscation, legal action | Police, judiciary | Sensitive files are not protected, Computers have unregistered copies of windows, | Backups are regular and kept outside the office | Hiding sensitive information Using Free Software Deleting information securely |
| Arrest or abduction during demonstrations | Police, company security agents | Inadequate emergency alert systems | Always carry mobile: text friends where & when I go on a demonstration | Rapid smart phone based panic button |
| Burglary | Local delinquents | Old locks on office doors, organisation smartphones not kept in a safe place | Smartphones have SIM lock and no social networking apps | Smartphone encryption, and a safe place to keep them |



A matrix for an environmental rights defender might look like this:

This example is merely for demonstrative purposes and may have nothing in common with your own situation, and for the purposes of this guide, it only focuses on digital security vulnerabilities and capacities, which should only be one part of your risk analysis.

## THE 'RISK MATRIX': PROBABILITY AND IMPACT

It may be that you find there are a lot of threats to your work, and it can be difficult to get some perspective on where to begin. In these cases it can be useful to think of the different threats in terms of the **probability** of their occurance, and their **impact** should they occur.

It might help you to plot them on a 'Risk Matrix' such as this one:

| PROBABILITY | | | | |
|---|---|---|---|---|
| Very High | | | | |
| High | | | | |
| Medium | | | | |
| Low | | | | |
| IMPACT | Low | Medium | High | Catastrophic |

Whether the probability of a certain attack is Low, Medium, High or Very High is a question of your own subjective judgement. It is relatively safe to say that if a certain type of attack has happened to colleagues, friends or other human rights defenders in your context, its probility in your context is at least medium, high or very high.

Impact is similarly subjective and can really only be judged for yourself. However it's relatively safe to say that any type of attack which, if carried out, would prevent you or your organisation entirely from carrying out your work, its impact is high or catastrophic.

As before, you can plot the threats on the matrix according to their probability and impact. An example might look like this:

| PROBABILITY | | | | |
|---|---|---|---|---|
| Very High | | | Confiscation of materials | |
| High | | Burglary | | |
| Medium | | | Entrapment & Assault | Imprisonment |
| Low | | | | |
| IMPACT | Low | Medium | High | Catastrophic |

Once you have prioritised the risks to yourself and your work, you can then start to take action to reduce them through building the relavent capacities and integrating them into a security plan.

## FURTHER READING AND REFERENCES

Environmental rights defence is mostly about defending the rights of communities from being denied access to resources and being harmed by extraction and overuse. The right to a safe and healthy environment is one of the fundamental human rights recognized internationally.

Technologies and tactics prescribed for human rights defenders are therefore relevant to environmental rights defenders. The reading resources listed below can help you when assessing risk and planning for security. Some of these address not only digital but also physical, organisational and psychological well-being.

- *Front Line Defenders' Workbook on Security for Human Rights Defenders* in English and Arabic
- Protection International's *New Protection Manual for Human Rights Defenders*, 3rd Edition
- Protection International's *Protection Manual for LGBTI Defenders*
- Electronic Frontier Foundation: *Risk Management as part of the Surveillance Self Defense project*.

[1] Kvinna till Kvinna, Integrated Security Manual

## LINKS

[1] *http://www.integratedsecuritymanual.org/*
[2] *https://securityinabox.org/chapter-3*

# 3
# Basic computer hygiene

## 3. Basic computer hygiene

About 90% of environmental rights defenders who took part in the June 2014 survey indicated that they had suffered at least one malware attack during the course of their work. However, they still had not taken sufficient measures to limit future attacks.

Although most said they had anti-virus programmes in their computers, these were not always kept up to date. Some of the licenses of purchased anti-virus programmes had also expired, thus stopping updates of virus definitions. This situation can become critical. As one respondent described,

**Human Rights Defender Testimonies**

***"Right now, our computers are infested with viruses. Some of our systems have collapsed and our IT officer is working to clean the viruses from our computers and network. We usually get viruses from memory sticks and downloaded files from the internet."***

Anonymous Natural Resource Defender, Liberia

The survey found that the most common computer hygiene needs include:

a. Protection against malware
b. Keeping computer software up to date
c. Maintaining backups of information

### TAKING CARE OF YOUR COMPUTER

The first step towards digital security is to keep your computer in good working condition, free of malware and up to date. You will be better able to successfully implement some of the more sophisticated digital technologies and tactics if your computer is well protected from malware.

#### *Protecting your computer against malware*

Malware is the general name for any malicious and undesirable software that attacks your computer and prevents it from working correctly. Two common types of malware are viruses and spyware. Viruses get onto your computer through the internet, when you download an infected file, open/save an attachment on your email, or click on a bad link. One of the most common ways to pick up viruses in Africa is from infected movable media such as flash disks/memory sticks.

### Why do you need to protect your computer from malware?

Viruses can destroy, damage or infect the information on your computer, including data on external drives. They can also render your computer unusable and make it necessary to re-format your hard disk. They can also take control of your computer and use it to attack your colleagues' computers. Spyware, on the other hand, can steal your sensitive information and make it available to your adversaries.

### How do you protect your computer from malware?

Antivirus programmes are your first line of defence against viruses and spyware. To protect your computer against viruses and other malware:

- Get good antivirus software which also has anti-spyware properties. If your anti-virus software does not have antispyware, you should also download anti-spyware software, such as Spybot [1].
- Your Anti-virus software should always be kept up to date by connecting to the internet daily so that the program can download the latest virus definitions.
- Keep the software itself up to date by always downloading the latest version of the software. Normally, the software will inform you when it needs to be updated.
- If your computer is seriously infected and cannot start, or is too slow for you to run an antivirus scan, you should use an antivirus Rescue CD. Many antivirus companies provide free rescue disks. If you use Avast Antivirus, for instance, you can create your own Rescue Disk by navigating to Tools and selecting Rescue Disk. Read the *Advanced Virus Removal Methods* [2] section of Security in-a-box for guidance on using a rescue disk.
- To guard your computer against malware from malicious websites, you can use the VirusTotal web application. VirusTotal checks suspicious links and files for malware by adding the URL or file to the easy to use VirusTotal online portal [3]. VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. Avast also has an Online Security plugin [4] for browsers such as Firefox and Google Chrome which offers protection against known phishing and malware sites.

Since the best paid-for anti-virus software can be expensive, you should seriously consider brilliant free and open source anti-virus software Avast to protect your computer for free. There is also a good malware removal tool called **Spybot** that detects and prevents known spyware from infecting your computer. It is also useful in removing spyware that is already on your computer.

Read the *How to protect your computer from malware and hacker*s [5] chapter of **Security-in-a-Box** for more information on how you can keep viruses, spyware and hackers at bay.

### *Keeping your software up to date*

It is critical to always update your computer's software regularly and ensure that you have the latest version available. Keeping your software up to date limits weaknesses in the software that can be exploited by malware. Always keep your operating system (Windows, Linux, Mac OS, etc) updated by downloading the latest updates from the respective websites. Application software (Word, Excel, LibreOffice), either bought or open source, should also be kept up to date. Set your software to send you alerts about security updates, if such an option is available, so that you can get them as soon as they are released.

### Why do you need to update your software regularly?

Given the complexity of software development, a few errors and omissions are still left when software is released. These are called bugs. These bugs can cause vulnerabilities which can be exploited by malware. Luckily, software developers are always looking for these errors and constantly release updates to fix them.

### How do you update your software?

Most software on Windows will either update automatically or alert you to available updates, and point you to where you can download them. Windows operating system is set to auto-update by default.

If your settings are not set to auto-update (mobile-based GSM data providers often advise you to turn off automatic Windows updates to conserve your data bundles) you can turn this function on by going to your computer's Start menu, selecting All Programs and clicking Windows Update.

Alternatively, through the process above you can set Windows Update to inform you of available updates and let you decide whether to download them or not. This way, you can download and install all your updates when you are in a place with a good and affordable internet connection (e.g. your office)

### *Open Source software*

For most small organisations in Africa, keeping your paid-for software up to date can be a challenge. Sometimes you have to buy new licences, or whole new software suites, which can be a drain on your budget.

Consider switching to free and open source software (FOSS) such

as the office suite LibreOffice, and an open source operating system such as GNU/Linux-based Ubuntu.

Also consider using Mozilla Thunderbird as your email client and Firefox as your internet browser. As well as being free, FOSS software is also relatively more secure, as there are millions of volunteers looking at the source code and any one of them can spot bugs and fix them much quicker than engineers of proprietary software can. Independent developers are also constantly developing digital security tools to add to FOSS software.

Here are a few FOSS alternatives to your proprietary software:

**LibreOffice** [6]: a software suit that does most of what you need from Microsoft Offce.

**Mozilla Thunderbird** [7]: an email client alternative to Microsoft Outlook but more secure especially if used with Enigmail and GPG.

**Mozilla Firefox** [8]: an internet browser alternative to Internet Explorer. Firefox is always being updated to keep it more secure and reliable. It can also be expanded by adding security features. Read the *Keeping your software up to date* section for more information on how to keep your software up to date [9].

### *Keeping Backups of your information*

Loss of digital information from computer theft or collapse is fairly common in many countries in Africa. In some countries, confiscation and destruction of computers by government security agents is also something that you should be wary of.

Fortunately, you can take measures to ensure that you recover your most important information in the unfortunate event that you should lose a computer either through theft, system collapse, or confiscation/destruction by your adversaries.

Your best bet is to keep a backup of your important information. When creating a backup:

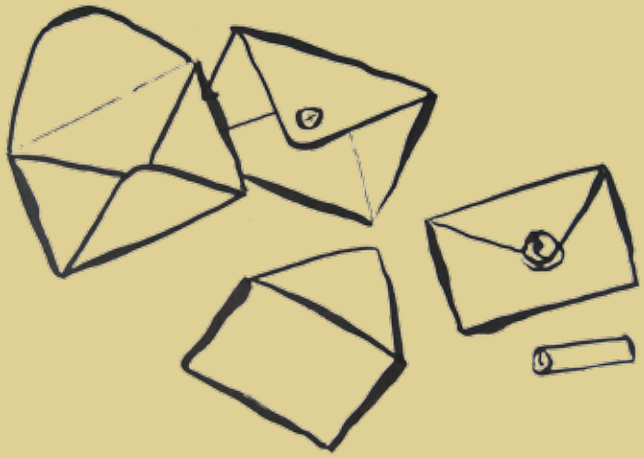
- Identify your important information and organize it in one place, such as a folder in your computer.
- Select a backup storage medium that allows you to replace your backup document with its latest version. An external hard disk drive (HDD), which connects to your computer via USB, has become the storage medium of choice for many. External HDDs can offer storage space of up to 6TB. It is, however, recommended that you store your backups on smaller HDDs, from 350MB to 1TB, which you can keep in separate locations.
- Keep your backups in a separate location from your computer. This ensures that you do not lose both the files on your computer and your backup at the same time. Keeping a couple of backups in different locations is good practice, as long as these too are secured.
- You can also store your backups on remote servers via the internet – on what is now known as the cloud. Ensure you choose a secure online storage service. Consider secure services like Tresorit and SpiderOak, which are both quite secure and reliable.

Read the chapter on *How to recover from information loss* for a more detailed explanation on how to back up and recover your information.

### LINKS

[1] *https://securityinabox.org/spybot_main*
[2] *https://securityinabox.org/dealingwithviruses#4.9*
[3] *https://www.virustotal.com/*
[4] *http://www.avast.com/lp-online-security-plugin*
[5] *https://securityinabox.org/chapter-1*
[6] *http://www.libreoffice.org/*
[7] *https://securityinabox.org/thunderbird_main*
[8] *https://securityinabox.org/firefox_main*
[9] *https://securityinabox.org/chapter_1_4*
[10] *https://securityinabox.org/chapter-5*

# 4
# How to secure your online collaborations



## 4. How to secure your online collaborations

Due to the nature of the work, environmental rights defenders tend to form networks, often sharing information through online platforms with low security. Most have email groups that allow for sharing of reports, photos, evidence and other information that may be sensitive. Yahoo Groups and Google Groups are among the most commonly used.

The Yahoo mail system that forms the basis for Yahoo Groups has faced many attacks due to what analysts think of as laxity in Yahoo security policy.

***Example incidents***

**In January 2013, a lone hacker, Shahin Ramezany, was able to exploit a hole in Yahoo's servers by leveraging a vulnerability – described as DOM-based XSS vulnerability – that is exploitable in all major browsers thus putting more than 400 million yahoo accounts at risk. As recently as April 2014, Yahoo mail was still being attacked due to similar vulnerabilities.**

Emil Protalinski, TheNextWeb.

Any information posted on open Yahoo and Google groups can also be accessed by anyone doing a simple Google search. Real names, email addresses, phone numbers, location and other sensitive information can often easily be found in the pages of these groups. There is no indication that defenders are taking any precautions when using these services.

Reports of attacks on rights and ERDs based on these vulnerabilities are largely unavailable, but this could be because of a lack of awareness. The mere existence of this threat should be sufficient cause for taking precautions.

**Human Rights Defender Testimonies**

***"In time of peace, prepare for war. We have a good government now, but we don't know how the next regime will be like."***

Anonymous Environmental Rights Defender in Liberia.

Secure online collaboration platforms such as Crabgrass on Riseup.net become should be considered in areas where environmental rights defenders may be at risk.

As an environmental rights defender, you will often find yourself working together with partners and needing to exchange information and documents via email. You may also be part of a network that shares information through an email group such as Yahoo Groups or Google Group. You can keep your online communication secure by taking the steps outlined below.

## SECURING YOUR EMAIL

The first step to ensuring that you are communicating as securely as possible is to secure your email by:

- Choosing to open an email account with a trusted email service such as Gmail instead of Yahoo, not known for security and privacy, or Hotmail, which inserts the **IP address** of the computer you are using into all of the messages you send.
- If you are using Gmail or certain other web services, using two-step verification to add a layer of security to your email login. Basically, Gmail's two-step means that once you sign in with your password, Google will send a verification code to your phone via SMS, voice call or the Google Authenticator app, depending on your choice. You must enter this code to access your account. Google Authenticator is available for Android, iPhone and Blackberry phones. This Wikipedia article explains more, and lists web services which also use two-step verification [1].
- Creating a strong password for your email account. Find out how you can create a strong password by reading *Chapter 3* of **Security-in-a-Box**: *How to create and maintain secure passwords* [2]
- Accessing your webmail through a browser that has added security features. Mozilla **Firefox** is a good free and open source browser you can use since it is more secure and can be extended to make your experience safer.
- Using a secure connection when using webmail accounts. You can learn more about secure connections, how to know if you're on a secure connection and how you can force your browser to connect securely by reading the *Keeping your webmail private* section of **Security in-a-box** [3].
- Opening a secure email account which has more security features, such as Riseup.net. **Riseup** is free and you can find out how you can use it by reading*Switching to a more secure email account* section [4]
- Encrypting the content of your email to protect it from prying eyes. You can encrypt your message using GPG but this might be a little difficult for those without advanced computer knowledge. An easier option would be to use Mozilla Thunderbird with Enigmail and GPG since you only have to set it up once. Find out how you can do this by reading the *Encrypting and Authenticating Individual Messages* section [5].



## SECURING YOUR EMAIL GROUPS AND LISTS

Once your email account and communication is secure, you can then extend the protection to your email groups and lists. You can move from your current groups and mailing lists such as Yahoo and Google groups to the more secure lists provided by technology collectives including Riseup.net, aktivix.org and autistici.org depending on the level of privacy you need. However, remember that if members of the email list continue to use insecure email providers, any unencrypted content shared on the list can still be accessed and shared by these providers.

**Riseup.net** allows you to create a mailing list through which you can send secure emails to your partners or within your network. Anyone can create a list at Riseup, but lists have to be approved before you can use them. They usually have criteria for accepting lists, including the proviso that your list should be of "progressive, radical, or revolutionary nature." It can take more than a week for your list to be approved but once it is approved you will be able to use one of the most secure lists available. Riseup has also developed a new tool for secure chat but as of July 2014 this is still being tested. Riseup, like other independent free services, needs donations to keep them running.

**Aktivix.org** provides you with the opportunity to create a mailing list to collaborate within your network using Gnu/Mailman. You can only get a list from Aktivix if you share their ideology which is clearly spelled out on their website. You also need to be recommended by someone who already has an Aktivix account. If, however you don't know such a person, you can request them to ask for recommendations from selected activists and tech collectives that you know. You are also requested to donate to keep this service running and free.

**Autistici.org** was started more than a decade ago. It provides internet support to activists and collectives from grassroots and social movements. Apart from mailing lists, they also provide anonymous remailing, chat, and instant messaging, among other services. The services are free but they recommend that you donate to enable them keep these services free.

To find out how to access and use the services mentioned above, you should go to their websites and read their instructions. Since we recommend Riseup.net, you can also find a brief explanation on how to get started with Riseup in the *RiseUp - Secure Email Service* section of Security in-a-box [6].

## SECURE VOICE AND CHAT COMMUNICATION

ERDs are often geographically dispersed, using Voice over Internet Protocol (VOIP) technology to hold virtual meetings and discuss sensitive issues. Skype is popular, used on both computers and smartphones. Chat, or Instant Messaging (IM), is often used for communication in real time.

The main problem with Skype is that it is a closed commercial product, and its technology is therefore not available to the public to analyse its security features and assess how safe it is. Alternative free and open source platforms whose technology is open for assessment, such as Jitsi, may be a better alternative for this community.

There are several options you can use to keep your voice and chat communications secure. We recommend Pidgin with OTR for chat, and Jitsi for voice, video and chat.

**Pidgin** is a free and open source instant messaging platform that allows you to manage several IM accounts in one place [7]. It works with most IM platforms, including the chat functions in Gmail and Yahoo. Off-The-Record (OTR) is a plugin developed for Pidgin which adds more security to your Pidgin sessions. You can learn more about working with Pidgin and OTR by reading the Pidgin with OTR – Secure Instant Messaging section in Security in-a-box.

**Jitsi** is a free and open source program that allows you to use voice, video and chat over the internet. It works with most the popular platforms available today, including Google Talk, Yahoo and Facebook. The advantage of Jitsi is that it offers voice and video encryption, allowing you to call other activists and defenders securely. Jitsi also supports voice conference calls. You can learn how to use it by reading the *Jitsi - Secure Audio, Video and Instant Text Messaging* section in **Security in-a-box** [8].

## SAFER USE OF SOCIAL NETWORKING SITES

Environmental rights defenders, like most rights defenders, sometimes have to depend on mass information dissemination to create public outcry, urging action from governments and companies when diplomatic channels fail and legal channels are compromised.

The growth of social media platforms such as Facebook and Twitter has made them vital advocacy tools for ERDs, and most are using them to expose major transparency, rights and ecological violation activities.

The risk here is that social media profiles can also be used to monitor and locate ERDs who are targeted by either governments or companies. Sensitive information such as names and phone numbers, as well as photos of self, family and home can be extracted from social media platforms and used to piece together your movement and association patterns, making it easy for adversaries to find and harass you, arrest you or disrupt your work. Sometimes, adversaries may use your social media pages and accounts to maliciously spread propaganda and try to discredit your work.

### Human Rights Defender Testimonies

***"In our campaign to fight the construction of a mega-dam and establishment of vast plantations along the Omo River in Ethiopia, activities which will drastically reduce the flow of the river and how much water comes into Lake Turkana, thus leading to catastrophic shrinkage and increase of salinity of the lake, we use both Twitter and Facebook to raise awareness and rally support for our cause. A particularly vocal supporter of the dam always attacks us on our Facebook page terming us enemies of Ethiopia and agents of the west who have been paid by Western governments to keep Ethiopians poor."***
Anonymous Environmental Rights Defender

## INCREASE YOUR SECURITY WHEN USING SOCIAL NETWORKING SITES

To improve your security when using social networking sites, you should take a precautionary approach to how you engage with these networks. A general precaution is to be aware of how much of your personal and sensitive information you are sharing on social networks, and how this can put you and your networks at risk. A good explanation of why you should take precautions when using social media tools can be found in *Chapter 9: How to protect yourself and your data when using social networking sites* [8].

You can take precautions by:

- Assessing and adjusting how you interact with social media sites: see the section on *General tips on using social networking tools,* in **Security in-a-box** [9].
- Considering what information you should be sharing on social media: see the section on *Posting personal details* in **Security in-a-box**. [10].

There are also alternatives to popular social media platforms (such as Facebook and Twitter) in development. **Riseup**.net, for instance is currently developing Crabgrass , a social networking and collaboration tool that, in the words of the collective, is designed to suit "the complexity of relationships that activist organizations face in the real world." See the Crabgrass guide or read more about Crabgrass in the

Riseup.net website riseup.net [11].

**LINKS**

[1] *http://en.wikipedia.org/wiki/Two-step_verification*
[2] *https://securityinabox.org/chapter-3*
[3] *https://securityinabox.org/chapter_7_1#Keeping_your_webmail_private*
[4] *https://securityinabox.org/chapter_7_1#Switching_to_a_more_secure_email_account*
[5] *https://securityinabox.org/chapter_7_4#Encrypting_and_authenticating_individual_email_messages*
[6] *https://securityinabox.org/riseup_main*
[7] *https://securityinabox.org/pidgin_main*
[8] *https://securityinabox.org/jitsi*
[9] *https://securityinabox.org/chapter-9*
[10] *https://securityinabox.org/chapter_9_1.*
[11] *https://we.riseup.net/*



# 5
# How to secure your files in "cloud storage"

## 5. How to secure your files in "cloud storage"

The nature of the work carried out by environmental rights defenders requires travel to remote areas where extractive and ecological abuse is happening. This necessitates a means of accessing stored information; for example, to educate local communities on their rights and to inform them of the current developments concerning the issue that is being addressed.

ERDs therefore often need to carry around computers, and sometimes also backup external hard disks. This opens up the risk of losing information, should devices be stolen or confisticated. Many defenders have directly expressed a need for online solutions for storing their sensitive information in a way that they can access it safely and rapidly from any location where there is internet coverage.

**Human Rights Defender Testimonies**

***"I usualy back up my important information every two weeks. I store the backup in an external hard disk which I travel with whenever I go. This hard disk and computer can be taken or lost and I can lose all my information. I think we need a secure online backup system".***

Anonymous Transparency Activist, Tanzania

Secure online storage is not only useful for storing information that is needed in the field, but can also be used as a more reliable alternative to portable media like external hard drives and memory sticks.

Often, you will find that you cannot rely on your external drives and flash disks. Other times, you may find yourself in the dilemma of not wanting to travel to risky locations with your external disks, but needing to access your stored files while you're there. In such cases, you will need to have your files stored in a secure and remote location and still be able to access them whenever you need them. Secure loud storage is a viable alternative.

You should, however, be cautious in your choice of cloud service. There are many cloud services to choose from. Among the most commonly used in Africa are Google Drive and Dropbox. However, although both promise privacy of your files and give you control of who can view your files, it is advisable to take the security of your cloud usage a notch higher. We recommend two ways of making your cloud experience more secure:

- Securing your files when using popular cloud services
- Switching to a more secure cloud service

## SECURING YOUR FILES WHEN USING POPULAR CLOUD SERVICES

Generally, when using a cloud service, you should add a layer of security by:

- Creating and using strong passwords to log into the cloud service. Learn how to create strong passwords by reading *Chapter 3: How to create and maintain secure passwords* [1]
- Encrypting your sensitive files before uploading them onto the cloud servers. Find out how you can encrypt your files in the in *Chapter 4: How to protect the sensitive files in your computer.* [2]
- Storing copies of your files in more than one cloud service. For instance, you can store two copies of the same file in both Dropbox and Google Drive.
- Ensuring that only a few people you trust get access these files, and only when you need to share the files with them.
- Use secure connections when accessing your files on the cloud. *Chapter 7: Securing your email* [3] has an explanation on how you can ensure that you are accessing web services using a secure connection. It also points you to tools that you can use to make accessing web services secure.

## SWITCHING TO A SECURE CLOUD SERVICE

Nothing is ever 100% secure, but you increase your level of security much more if you use cloud services that are designed with security in mind. Most of the popular cloud services such as **Dropbox** and **Google Drive** are generally thought to be fraught with security and privacy problems.

There are, however, several free and more secure alternative cloud services out there. Tresorit and SpiderOak offer free, security-conscious services which are worth considering.

**Tresorit**: 5GB of storage free, although you can only store files not exceeding 500MB. Since the capacity is so small, the free service would be useful in keeping only the most sensitive of your information. The paid-for service is relatively affordable.

Tresorit security is threefold: Your files are encrypted on your computer (thus eliminating the need for you to encrypt your files manually) before being uploaded onto the cloud; the company does not have access to your files and cannot modify them; and the company does not know your password (the flip side of this is that if you forget your password you lose control of your files and you can never recover them).

The advantage of Tresorit over other popular cloud services is that you do not have to create a special sync folder for it, you just right-click any folder and "tresor it" to sync it.

To use Tresorit, you have to download the desktop application. Their support page [4] has straightforward instructions to guide you on how to install and use Tresorit.

**SpiderOak** is free for the first 2GB of storage space but after that you have to pay for more storage. You can store anything from documents and photos to video and audio files.

With SpiderOak, everything is password-secured and only you (or those who have your password or who you share the folders or files with) can access them. Even the SpiderOak servers cannot read your files.

Their "zero-knowledge" policy means they know neither your password nor the content of your folders. In their own words, "In technical terms, 'zero-knowledge' means that the server has 'zero-knowledge' of your data. In non-technical terms it means that your data is 100% private and only readable to you. No plaintext data is stored on our servers, ensuring absolute confidentiality between you and your data."

**Caution:** When using zero-knowledge cloud services, ensure that you can always remember your password since they cannot reset it even in times of emergency. If you cannot remember your password, you will completely lose access to your folders. You can use **KeePass** to keep your passwords in one secure place.

You need a desktop application to be able to use SpiderOak. The website has a detailed User Manual [5]that shows how to install and use SpiderOak.

## LINKS


[1] *https://securityinabox.org/chapter-3*
[2] *https://securityinabox.org/chapter-4*
[3] *https://securityinabox.org/chapter_7_1*
[4] *https://support.tresorit.com/forums/22959678-How-to-*
[5] *https://spideroak.com/user-manual/*

# 6
# How to use your smartphone more securely

## 6. How to use your smartphone more securely

In much of Sub-Saharan Africa, the national telecoms landline networks – initially inadequate and unreliable anyway – have all but collapsed. As a result, the mobile phone has found a natural home among people in Africa, as mobile networks have expanded to fill the void left by landlines. Many Africans now depend on the mobile phone for almost all of their communication, from making phone calls to texting and even mobile banking. The proliferation of smart phones in the region has seen many people using additional functionalities found in apps to perform many of their official functions.

**Human Rights Defender Testimo**

***"The mobile phone is the only means of communication in Liberia. The landline network collapsed a long time ago. We use our phones for everything from email, accessing the web, social media, phone calls and SMS."***

Anonymous Environmental Rights Defender, Liberia.

Many ERDs spend a lot of time away from the office, and as such use smart phones to carry out a variety of information gathering and sharing tasks, such as audio and video recording of testimonies, photography, email, web surfing and file storage, in addition to the traditional phone functions - voice calls and SMS.

This exposes ERDs to vulnerabilities inherent in the use of smart phones, such as access to sensitive information stored in the phones, or that which is available online via the phone's apps. Such information can include emails, stored evidence, photos of self, co-workers & family members, text messages, chat records (e.g. on WhatsApp, Facebook, Gmail and Twitter), contacts and financial information.

Mobile phone security is a developing field and precaution is the best approach for ERDs at this time. There are, however tools that have been developed especially for the Android phone platform that can add a layer of protection for smart phones. Generally, however, smart phone security is to be considered as a combination of computer and mobile phone security.

There are some basic security precautions you can take to protect information stored in your phone, as well as your communication using these devices.

- Ensure that you have activated auto-lock on your phone and that

you need a 4 digit pin/code to activate the SIM Card, as well as a code or password to unlock the screen. You can add more security by requiring entry of your SIM PIN whenever the phone is turned on. Some phones offer the option of deleting all your private information after a certain number of unsuccessful phone pin attempts. You should consider this option if you store sensitive information in your phone.

- Install security apps on your phone. Install apps that protect your phone from malware and hackers, and also apps that you can use to protect your sensitive information from unauthorized access. Remember to always download your apps from approved sources, depending on your phone operating system.
- Always keep your phone's operating system up to date, to the level permitted by your hardware. Before you attempt an upgrade of your phone software, ensure that your hardware meets the minimum requirements for the upgrade, otherwise it will not work.
- Always back up all the information you can from your phone. Use encryption on your phone for all sensitive information. On phones with Andriod version 4.0 or later, you can encrypt the entire contents of the phone.
- Turn off your data, WiFi, Bluetooth and other remote connection features on your phone when not in use or when you are in risky locations.

In **Security in-a-box**, ***Chapter 11: How to use your smart ones as securely as possible***, gives a detailed explanation on how to stay safe when using your smart phone. [1]

## LINKS

[1] *https://securityinabox.org/chapter-11*

# 7
# How to make a distress call in emergencies

## 7. How to make a distress call in emergencies

Often, ERDs work in risky situations and locations. You may be gathering evidence in a location where ecological or community rights violations have taken place, or you may be holding demonstrations or consultative meetings with affected communities. Security forces are likely to disrupt these activities and sometimes arrest the defenders. Company security personnel or hired goons may also attack and abduct defenders.

**Human Rights Defender Testimonies**

***"We are trying to negotiate for the release of a local pastor from Bahi District in Dodoma, who was arrested and jailed for 6 months for opposing uranium prospecting in Bahi. The pastor was accused of inciting the local population and the District Commissioner ordered his arrest. In a country where court cases can take months or even years, the pastor was jailed within two weeks of his arrest which makes this action very unusual."***

Anonymous Human Rights Defender, Tanzania

In the event of such incidences, defenders need a discreet and rapid means of alerting their peers and family that they are under attack or they have been arrested. Mobile phone based solutions are the best for these situations, since virtually all ERDs have phones which they carry with them to these locations. A solution like the Panic Button, developed by a collective led by Amnesty International, would be an important addition to the digital security measures that ERDs should consider.

### SENDING DISTRESS CALLS USING PANIC BUTTON

**Panic Button** sends selected partners, friends or family a message informing them that you are in danger. Panic Button can also be set up such that when it is activated, it will send periodic location maps to the people you have selected as long as your phone is on, thereby allowing them to track you. Here are some tips on using Panic Button. Remember Panic Button is a useful tool to alert your network quickly and discretely in an emergency. It is not a fail-safe security tool!

- To use panic button effectively, you need to select an emergency response team of 3 of your most trusted partners. Panic Button aims to send your emergency message/s to your trusted contacts when you need help. However, the app is not able to guarantee a response.

Think carefully when choosing your trusted contacts and always talk to them first to ensure you have a response plan in place.

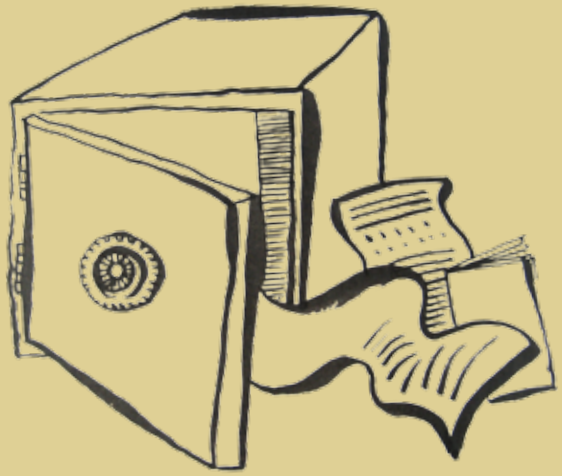
- Panic Button works only with Android phones. You should be able to use Panic Button on Android versions 2.3.3 to 4.4.2.
- To send an emergency alert, you only need to tap rapidly on your power button. For the alert to be sent, you must have battery and phone credit/units.
- Only use Panic Button if you have independent access to your phone. This prevents false alarms and also misuse, such as partners or family members using the app to track you without your knowledge. So make sure that you are the only one who has access to your phone.
- When using Panic Button, you have to be careful not to put yourself and your emergency response partners in danger. If your country is known to practise mass telecommunications monitoring and interception, then you should think seriously about whether using Panic Button will reveal information about your location and trusted contacts that could put you or them at increased risk.

You can download the app from the Panic Button website [1], where you will also find more information about how you can use it.

**LINK**

[1] *https://panicbutton.io/*

# 8
# How to protect your evidence



## 8. How to protect your evidence

Environmental Rights defenders depend on evidence gathered from sites of ecological and community violations to advocate for favourable public opinion, policy change and government action against these offences. As a result, the security and integrity of evidence is of utmost importance.

Evidence such as interviews, photos, videos and documents stored in computers, phones and other devices can be compromised, stolen or destroyed by adversaries who want to disrupt the work and destroy the credibility of ERDs, if such evidence remains unsecured. Inside informants can also be exposed and action taken against them.

### PROTECTING EVIDENCE FILES STORED IN YOUR COMPUTER

You should consider all evidence collected and saved in your computer or phone as sensitive information. As such, you should always protect this information and make it impossible for it to be used against you, your partners or your informers. Security in-a-box has several chapters that can show you how to protect your information. Specifically, you should read and understand these three chapters:

- *How to protect the sensitive files in your computer* [1], which explains how you can encrypt and hide your sensitive information.
- *How to recover from information loss* [2], which explains how to backup your information and how you can recover your files from accidental deletion
- *How to destroy sensitive information* [3], which deals with completely obliterate files stored in your computer in case you no longer need them.

### LINKS

[1] *https://securityinabox.org/chapter-4*
[2] *https://securityinabox.org/chapter-5*
[3] *https://securityinabox.org/chapter-6*

# Glossary

## Glossary

Some of the technical terms that you will encounter as you read through these chapters are defined below:

**Android** - A Linux-based open-source operating system for smartphones and tablet devices, developed by Google

**APG** - Android Privacy Guard: FOSS app for Android smartphones which facilitates OpenPGP encryption. It can be integrated with K9 Mail

**.apk file** - The file extension used for Android apps

**App Store** - The default repository from which iPhone applications can be found and downloaded

**Avast** - A freeware anti-virus tool

**BIOS (Basic Input/Output System)** - The first and deepest level of software on a computer. The BIOS allows you to set many advanced preferences related to the computer's hardware, including a start-up password

**BlackBerry** - A brand of smartphones which run the BlackBerry operating system developed by Research In Motion (RIM)

**Blacklist** - A list of blocked websites and other Internet services that can not be accessed due to a restrictive filtering policy

**Bluetooth** - A physical wireless communications standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short wavelength radio transmissions

**Booting** - The act of starting up a computer

**CCleaner** - A freeware tool that removes temporary files and potentially sensitive traces left on your hard drive by programs that you have used recently and by the Windows operating system itself

**CD Burner** - A computer CD-ROM drive that can write data on blank CDs. DVD burners can do the same with blank DVDs. CD-RW and DVD-RW drives can delete and rewrite information more than once on the same CD or DVD.

**Circumvention** - The act of bypassing Internet filters to access blocked websites and other Internet services

**Clam Win** - A FOSS Anti-virus program for Windows

**Cobian Backup** - A FOSS backup tool. At any given time, the most recent version of Cobian is closed-source freeware, but prior versions are released as FOSS

**Comodo Firewall** - A freeware firewall tool

**Cookie** - A small file, saved on your computer by your browser, that can be used to store information for, or identify you to, a particular website

**Cryptonite** - A FOSS app for file encryption on Android smartphones

**Digital signature** - A way of using encryption to prove that a particular file or message was truly sent by the person who claims to have sent it

**Domain name** - The address, in words, of a website or Internet service; for example: https://securityinabox.org

**EDGE, GPRS, UMTS** - Enhanced Data Rates for GSM Evolution, General Packet Radio Service, and Universal Mobile Telecommunications System – technologies which allow mobile devices to connect to the internet

**Encryption** - A way of using clever mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key

**Enigmail** - An add-on for the Thunderbird email program that allows it to send and receive encrypted and digitally signed email

**Eraser** - A tool that securely and permanently deletes information from your computer or removable storage device

**F-Droid** - An alternative repository from which many FOSS Android applications can be found and downloaded

**Firefox** - A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer

**Firewall** - A tool that protects your computer from untrusted connections to or from local networks and the Internet

**FOSS (Free and Open Source Software)** - This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it

**Freeware** - Includes software that is free of charge but subject to legal or technical restrictions that prevent users from accessing the source code used to create it

**Gibberbot** - A FOSS app for Android which facilitates secure chats over XMPP protocol (used also by Google Talk). It is compatible with Off-the-Record and, when used in conjunction with Orbot, can route chats through the Tor network

**Global Positioning System (GPS)** - A space-based global navigation satellite system that provides location and time information in all weather, anywhere on or near the Earth, where there is an (almost) unobstructed sky view

**GNU/Linux** - A FOSS operating system that provides an alternative to Microsoft Windows

**Google Play** - The default repository from which Android applications can be found and downloaded

**Guardian Project** - An organisation which creates smartphone apps, mobile devices operating system enhancements and customisations with privacy and security in mind

**Hacker** - In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely

**HTTPS** - When you are connected to a website through SSL, the address of the website will begin with HTTPS rather than HTTP

**Infrared Data Association (IrDA)** - A physical wireless communications standard for the short-range exchange of data using infrared spectrum light. IrDA is replaced by Bluetooth in modern devices

**IP address (Internet Protocol address)** – A unique identifier assigned to your computer when it is connected to the Internet

**iPhone** – A brand of smartphones designed by Apple which run the Apple's iOS operating system

**ISP (Internet Service Provider)** - The company or organisation that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries

**Jailbreaking** - The process of unlocking features on an iPhone which are otherwise blocked by the manufacturer or mobile carrier in order to gain full access to the operating system

**K9 Mail** - A FOSS e-mail client for Android smartphones, which enables OpenPGP encryption when used with the APG app

**Keylogger** - A type of spyware that records which keys you have typed on your computer's keyboard and sends this information to a third party. Keyloggers are frequently used to steal email and other passwords

**KeePass** - A freeware secure password database

**LiveCD** - A CD that allows your computer to run a different operating system temporarily

**Malware** - A general term for all malicious software, including viruses, spyware, trojans, and other such threats

**Mnemonic device** - A simple trick that can help you remember complex passwords

**NoScript** - A security add-on for the Firefox browser that protects you from malicious programs that might be present in unfamiliar webpages

**Obscuracam** - A FOSS app for Android smartphones, which protects identity of people by facilitating editions such as face-blurring to photographs

**OpenVPN** - An open source software application that implements virtual private network (VPN) techniques for creating secure point-to-

point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

**Orbot** - A FOSS app for Android smartphones which enables apps such as Orweb and Gibberbot to connect to the Tor network

**Orweb** - A FOSS web browser for Android smartphones which, when used in conjunction with Orbot, facilitates browsing over the Tor network

**OTR (Off the Record)** - An encryption plugin for the Pidgin instant messaging program

**Peacefire** - Subscribers to this free service receive periodical emails containing an updated list of circumvention proxies, which can be used to bypass Internet censorship

**Physical threat** - In this context, any threat to your sensitive information that results from other people having direct physical access your computer hardware or from other physical risks, such as breakage, accidents or natural disasters

**Pidgin** - A FOSS instant messaging tool that supports an encryption plugin called Off the Record (OTR)

**Proxy** - An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy

**Proprietary software** - The opposite of Free and Open-Source Software (FOSS). These applications are usually commercial, but can also be freeware with restrictive license requirements

**Recuva** - A freeware tool that can sometimes restore information that you may have deleted accidentally

**Riseup** - An email service run by and for activists that can be accessed securely either through webmail or using an email client such as Mozilla Thunderbird

**Rooting** - The process of unlocking features on an Android Phone which are otherwise blocked by the manufacturer or mobile carrier in order to gain full access to the operating system

**Router** - A piece of networking equipment through which computers connect to their local networks and through which various local networks access the Internet. Switches, gateways and hubs perform similar tasks, as do wireless access points for computers that are properly equipped to use them



**Secure password database** - A tool that can encrypt and store your passwords using a single master password

**SSL (Secure Sockets Layer)** – The technology that permits you to maintain a secure, encrypted connection between your computer and some of the websites and Internet services that you visit

**Security certificate** - A way for secure websites and other Internet services to prove, using encryption, that they are who they claim to be. In order for your browser to accept a security certificate as valid, however, the service must pay for a digital signature from a trusted organization. Because this costs money that some service operators are unwilling or unable to spend, however, you will occasionally see a security certificate error even when visiting a valid service

**Security policy** - A written document that describes how your organization can best protect itself from various threats, including a list of steps to be taken should certain security-related events take place

**Security cable** - A locking cable that can be used to secure a laptop or other piece of hardware, including external hard drives and some desktop computers, to a wall or a desk in order to prevent it from being physically removed

**Server** - A computer that remains on and connected to the Internet in order to provide some service, such as hosting a webpage or sending and receiving email, to other computers

**SIM card** - A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM cards can also store phone numbers and text messages.

**Skype** - A freeware Voice over IP (VoIP) tool that allows you to speak with other Skype users for free and to call telephones for a fee. The company that maintains Skype claims that conversations with other Skype users are encrypted. Because it is a closed-source tool, there is no way to verify this claim. ***www.skype.com***

**Source code** - The underlying code, written by computer programmers, that allows software to be created. The source code for a given tool will reveal how it works and whether it may be insecure or malicious

**Spybot** - A freeware anti-malware tool that scans for, removes and helps protect your computer from spyware

**Steganography** - Any method of disguising sensitive information so that it appears to be something else, in order to avoid drawing unwanted attention to it

**Swap file** - A file on your computer to which information, some of which may be sensitive, is occasionally saved in order to improve performance

**Textsecure** - A FOSS app for Android which facilitates encrypted sending and storage of text messages

**Thunderbird** - A FOSS email program with a number of security features, including support for the Enigmail encryption add-on

**Tor** - An anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you vist from anyone who may be monitoring your Internet connection, while also disguising your own location from those websites

**TrueCrypt** - A FOSS file encryption tool that allows you to store sensitive information securely

**Uninterruptable Power Supply (UPS)** - A piece of equipment that allows your critical computing hardware to continue operating, or to shut down gracefully, in the event of a brief loss of power

**VautletSuite 2 Go** - A Freeware encrypted email program

**Voice over IP (VoIP)** – The technology that allows you to use the Internet for voice communication with other VoIP users and telephones

**Whitelist** - A list of websites or Internet services to which some form of access is permitted, when other sites are automatically blocked

**Windows Phone** - A smartphone operating system developed by Microsoft

**Wiping** - The process of deleting information securely and permanently

**Your-Freedom** - A freeware circumvention tool that allows you to bypass filtering by connecting to the Internet through a private proxy. If Your-Freedom is configured properly, your connection to these proxies will be encrypted in order to protect the privacy of your communication

Software and documentation in this **Security in-a-box** toolkit is provided “as is” and we exclude and expressly disclaim all express and implied warranties or conditions of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose so far as such disclaimer is permitted. In no event shall Front Line, Tactical Technology Collective or any agent or representatives thereof be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption), however caused under any theory of liability, arising in any way out of the use of or inability to make use of this software, even if advised of the possibility of such damage. Nothing in this disclaimer affects your statutory rights.