

# STAND UP MANUAL



**DEFENDEFENDERS**

East and Horn of Africa Human Rights Defenders Project



# CONTENT

Acronyms	4
Acknowledgement	5
Foreword	6
<b>INTRODUCTION</b>	<b>7</b>
<b>CHAPTER 1: DEFINING CONCEPTS</b>	<b>8</b>
<b>CHAPTER 2: CONTEXT ANALYSIS</b>	<b>9</b>
<b>CHAPTER 3: SAFETY AND SECURITY INCIDENTS</b>	<b>11</b>
<b>CHAPTER 4: UNDERSTANDING THREATS</b>	<b>13</b>
<b>CHAPTER 5: RISK ASSESSMENT</b>	<b>16</b>
<b>CHAPTER 6: SAFETY AND SECURITY PLANNING</b>	<b>18</b>
<b>CHAPTER 7: EXISTING PROTECTION MECHANISMS FOR HRDs</b>	<b>20</b>
<b>CHAPTER 8: SELF- CARE AND RESOURCING RESILIENCE</b>	<b>23</b>

# ACRONYMS

<b>AU</b>	African Union
<b>ACHPR</b>	African Commission on Human and Peoples' Rights
<b>CBO</b>	Community-Based organisation
<b>EU</b>	European Union
<b>HRD</b>	Human Rights Defender
<b>WHRD</b>	Woman Human Rights Defender
<b>NHRI</b>	National Human Rights Institution
<b>NGO</b>	Non-Governmental Organisation
<b>SOGI</b>	Sexual Orientation and Gender Identity
<b>UN</b>	United Nations
<b>UDHR</b>	Universal Declaration of Human Rights

# ACKNOWLEDGEMENT

**O**n May 5<sup>th</sup> 2017, DefendDefenders launched the STAND UP! Manual for African human rights defenders (HRDs). The manual is aimed at enhancing the physical and digital security of individual HRDs and organisations by contextualising the existing knowledge in Protection International's New Protection Manual for HRDs and Front Line Defenders Workbook on Security. In December 2019, DefendDefenders launched the STAND UP! Manual in five Ugandan local languages, namely Acholi, Ateso, Luganda, Luo, Runyakitara. In 2020, DefendDefenders decided to review the manual to accommodate feedback from HRDs and new emerging concepts in safety, security, and wellbeing of HRDs in Africa. The present edition is a result of DefendDefenders experience and defenders feedback from trainings, research missions and various engagements with stakeholders, and emerging aspects in safety and security.

Protection and Security Management team composed of Janvier Hakizimana, Majid Maali, Karis Moses Oteba, Anne Nakiyingi, Mariam Nakibuuka (RIP), Brian Bamutaze, Leon Nsiku and Denise Kwizera revised Book One on physical safety and security. Book Two on digital safety and security was reviewed by Defenders Tech team made up of Daniel Byekwaso, Samuel Eibu, Joshua Ssengonzi, Donatien Niyongendako, Immaculate Nabwire, Abdikani Hassan.

The review process would not have been successful without the guidance and supervision of DefendDefenders' management team. The Executive Director of DefendDefenders – Hassan Shire, Director of Programs and Administration– Memory Bandera and Senior Manager Protection & Security Management– Tabitha Netuwa provided invaluable contributions from the strategic guidance to the editing and publication of this edition.

# FOREWORD

**T**he need for safety and security management for human rights defenders (HRDs) was arrived at when violence suffered by HRDs due to their work surpassed the protection capacity of rights duty bearers. Thus, as early as during the fall of the Berlin Wall, it was evident there was need for HRDs to have contextualized security and safety management tools and strategies. This need has now been answered through the StandUp Manual: Security and Safety Management for African Human Rights Defenders. It expands and strengthens knowledge in preventive protection for HRDs in Africa.

The manual focuses on safety and security threats and mitigation measures. It also delves into practical illustrations gleaned from training experience and interactions with grassroots African HRDs involved in daily human rights work in hard-to-reach zones of Africa, particularly in the East and Horn of Africa. These valuable experiences informed the choice of style, themes, and organisation of the manual, which makes its content easily understandable and practical for HRDs and their networks across Africa. The Manual's special characteristic is its holistic approach to security management that encompasses physical security and safety management, self-care, resourcing resilience, digital security.

HRDs sometimes forget or neglect their own safety in the course of their duties. It should not be the case. Sound security management has unfortunately become a key component of human rights work in the East and Horn of Africa, as HRDs, we have a responsibility, both to ourselves and to those we serve, to consider this.

While the use of internet and information technology in the process of promoting or protecting human rights has in many respects been a game-changer, it exposes HRDs to higher risks that require adapted solutions specified in this manual.

DefendDefenders was founded to protect HRDs facing immediate risks. However, more than a decade of experience has taught us that much can be done to prevent HRDs from reaching this critical point. By carefully considering their safety, developing strong security plans, rigidly adhering to them, even HRDs working in extreme conditions can mitigate the risk they face as individuals or organizations.

This manual contains key strategies and concrete measures that any HRDs working in the East and Horn of Africa can and should implement immediately to improve their own safety as well as that of their organizations and constituents. I encourage all my fellow HRDs to take these lessons to heart.



Hassan Shire,  
Executive Director,  
DefendDefenders

# INTRODUCTION

**T**he adoption of the United Nations Declaration on HRDs in 1998 and the establishment of the mandate of the United Nations Special Rapporteur on the situation of HRDs in 2000 are major milestones in the protection of HRDs at a global level. However, defenders continue to face threats and risks despite the existence of these mechanisms.

Across Africa, HRDs working to promote and protect human rights in volatile political contexts face major risks, such as killings, physical attacks and assaults, arrests, intimidation, shrinking civic space. States constantly fail to investigate violations against defenders.

To ensure their security and the continuity of their work, HRDs have taken steps to manage individual and organisational security by assessing risks and putting in place effective strategies to mitigate potential threats. Dedicating time and resources to managing security helps HRDs to continue their human rights activities and ensure their safety and security.

DefendDefenders contextualised manual on safety, security and resourcing resilience is intended to serve as a tool for HRDs in Africa to equip them with necessary strategies and responses to the often-volatile environment they operate in. Despite the available protection mechanisms, HRDs continue to face risks and threats which have an undeniable effect in the long run on their mental health. HRDs need to take steps to manage their safety and security.

This manual reflects DefendDefenders experiences over the past 17 years, focused on ensuring defenders safety, security, protection and self-care through trainings, advocacy & research, technical support, organisational support. The second edition is based on recommendations, feedback and interactions with HRDs, protection partners, national, regional and international mechanisms for the protection of HRDs.

This manual adds to the existing materials on safety, security and self-care of HRDs. It contextualises knowledge and tools for defenders in Africa.

This chapter defines basic concepts that are used throughout the manual. Understanding these concepts, their similarities, differences and complementarities is useful for HRDs when conducting risk assessments and developing effective safety and security strategies and measures.

# 1

## CHAPTER

# DEFINING CONCEPTS

## Human Rights Defender

Human rights defenders (HRDs) are people who individually or with others, act, in a peaceful manner to promote or protect human rights enshrined in the Universal Declaration of Human Rights (1948). The 1998 United Nations Declaration on Human Rights Defenders<sup>1</sup> refers to individuals, groups and associations contributing to the effective elimination of all violations of human rights and fundamental freedoms of people and individuals.

Anyone can be a HRD regardless of their educational background, professional qualifications, gender, age, race, social group and nationality. For example, if a street vendor or a banana seller denounces the mistreatment of their fellow sellers by local tax authorities, they can be considered HRDs. In some cases, HRDs can be found in both private and public sectors.

**Security** is defined as the state of being free from intentional harmful events

**Safety** is defined as the state of being free from unintentional harmful events.

**Both Safety and security include the element of danger.**

**Protection** is defined as measures taken by HRDs or other actors to enhance safety and security<sup>2</sup>. Safety and security incidents are events that can expose HRDs and/or their organisations to danger.

**Threat** can be defined as a declaration or indication of an intention to inflict damage, punish or hurt.

**Risk** can be defined as the possibility of an event that results in harm.

**Wellbeing** is taking care of one's physical, mental, and emotional health.

The context of HRDs, also known as working environment, is the basis for every safety and security decision. The safety and security risks that HRDs face vary according to the context. HRDs work in a dynamic environment that impacts their safety and security. The HRDs context is made up of factors and actors. Factors include politics, economy, culture, gender, religion, environment and other aspects such as health whereas actors include supporters and opposers of HRDs work. Context analysis intends to help HRDs make informed decisions about their safety and security.

1 The Declaration's full name is the "Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms" though commonly referred to as "The Declaration on Human Rights Defenders" <http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Translation.aspx>

2 Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, <https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk>, Accessed 23 June 2016.



# 2

## CHAPTER

# CONTEXT ANALYSIS

## Factor Analysis Method (FAM)

- 1. Political factors:** Politics can have positive and negative impacts on HRDs and their work. HRDs are not necessarily politicians, but the knowledge of political underpinnings in each setting is crucial in the adoption of safety, security and mechanisms for effective human rights work. HRDs should ask questions about who the key political factors are in their context and how they affect their safety and security. For instance, in some countries, elections mean heightened attacks against HRDs. In armed conflict areas, Women Human Rights Defenders (WHRDs) are particularly exposed to sexual violence and assassinations. Political instability forces HRDs to adjust safety and security mechanisms on a regular basis. HRDs need to actively monitor the dynamics of the political context and its impact on their safety and security.
- 2. Economic factors:** Economic regulations, necessities, facilities and opportunities are key to HRDs work. The defenders need to know the existing economic laws, regulations, and practices that affect their work. There is often the need for economic resources to implement certain safety and security measures. HRDs should analyse the global economic trends coupled with geopolitics for proper strategic programming and security planning.
- 3. Socio-cultural factors:** HRDs should appreciate the socio-cultural norms when conducting their work bearing in mind that some of these norms contradict the universality, inalienability and indivisibility of human rights. It is important to study the issues around traditional norms, religion and social perceptions of the community in which the HRD operates. Particularly regarding issues such as women's rights and sexual orientation, and gender identity and expression (SOGI). HRDs should monitor the socio-cultural factors and their impact on their safety and security.
- 4. Technological factors:** The use of technology has grown rapidly in the past decades. HRDs use various technology aspects in their human rights work including advocacy, networking and human rights monitoring, documenting and reporting (MDR). Technological factors look at the use of digital tools and support gadgets in the process of achieving human rights goals. Even though technology advances HRDs work, it has become one of the main sources of threats and risks. Most of today's threats and risks are executed via digital platforms. Therefore, HRDs need to manage the risks of the digital platforms.
  - Refer to Book II of this manual for more information on digital safety and security.

**5. Ecological and geographical factors:** Weather and landscape inform HRDs about safety and security risks arising from working in specific areas. In addition, they also inform of the period and timing to conduct certain activities. For example, terrain and weather conditions dictate the means of transport, clothing and protective gear to use. Depending on topography and available infrastructures, HRDs may be required to use all-terrain vehicles and boats to reach far-off areas. Biking, walking and/or canoeing are some of the options that can be utilised to access unreachable places.

**6. Legal frameworks:** In principle, national laws and constitutions provide legal protection of HRDs. But some legal provisions have been misapplied to violate HRDs rights. HRDs are increasingly faced with restricted civic space due to the adoption of repressive legislations. After the terrorist attacks of September 11 2011, most African countries have since passed and used anti-terror laws to limit the work of HRDs.

Furthermore, certain legislations governing freedoms of assembly and associations have been misused to justify the violation of HRDs rights. When HRDs acquaint themselves with legislations and ordinances of certain areas, they put in place measures to work securely and in addition, through advocacy, they call for repeal or amendment of certain laws. Past violations of HRDs rights are helpful in predicting what could happen to HRDs and their organisations.

**7. Other factors:** Public health concerns and hazards put the lives of HRDs in danger. HRDs need to consider preventive and reactive measures to care for medical eventualities. HRDs working on environment pollution and human rights violations in medical facilities are prone to contracting certain infections and diseases. For example, HRDs in zones prone to infectious diseases like Ebola have high chances of getting the disease. For best practices, HRDs are advised to receive prophylaxis, use personal protection equipment (PPE), and acquire medical insurance.

## Actor Analysis Method (AAM)

An actor is any person or institution that has interests in HRDs' work. HRDs must map out supporting actors, opposing actors and actors with unknown intentions. HRDs context is dynamic because actors shift their positions according to their interests and prevailing environments. Therefore, HRDs should monitor changes in their working context to re-assess whether the actors' position has changed or not.

### Types of actors

This table can be used by HRDs to categorise actors according to their interests and position.

Supporting actors	Opposing actors	Actors with unknown intentions
Donors	Human Rights Violators	Politicians
Fellow HRDs	Law Enforcement Agencies in some contexts	Religious Leaders in some contexts
International NGOs	Multi-National Companies in some contexts	Academia in some contexts

- Please avoid generalisation in Actor analysis.
- Where possible, HRDs need to mention individual names within a unit or an institution. For example, whereas some HRDs may assume that security services are against them, there may be some agents within the security services who support their cause.

# 3

CHAPTER

# SAFETY AND SECURITY INCIDENTS

A safety and security incident can be any event that exposes HRDs and/or their organisations to danger. It provides lessons to HRDs and their organisations on the impact of their work by giving them the opportunities to re-assess their programming and protection mechanisms.

## Examples of Safety Incidents

1. Fire outbreak or electrocution.
2. Office flooding; and
3. Disease outbreaks.

## Examples of Security Incidents

1. People monitoring HRDs' improvements.
2. Leakage of confidential information of HRDs; and
3. Search of HRDs' homes and offices.

## STEP 1:

### Recording Incident

HRDs use various formats to capture details of incidents including bullet-point and paragraph. Whichever format is preferred, they are guided by the six question pillars made up of 5 Ws and 1 H as illustrated in table below:

5 Ws and 1 H		
Who?	What?	Where?
When?	Why?	How?

Incident recorders endeavor to ask as many questions as possible under each question pillar which are relevant to incidents being captured. They should avoid complicated words, jargons and buzzwords while recording. They also must make sure that names, addresses, figures, and facts are correct for a proper guidance in next steps of Safety and security incident assessment.

## STEP 2:

### Reporting Incident

When an incident is experienced or observed, the incident must be captured in a report format. Incident reporting can be written or verbal. However, a record of the incident should be kept in written form to prevent the loss of reported facts. For HRDs working in an organisation, the incident report should be sent to the management. For individual HRDs, the incident report can be shared with trusted colleagues and stakeholders. In reference to the six question pillars, key information in this report should include:<sup>3</sup> Who is reporting;

- What happened? Where has it happened? When it happened, as precisely as possible;
- Who was involved, with details of the victims of the incident;
- What the impact is on those affected, with details of their current condition;
- Who perpetrated the incident, with brief details of numbers, weaponry, apparent affiliation, post-incident actions;
- Why the incident took place at that time? How did the incident happen (means used by the perpetrator);
- Summary of the current situation and whether there are problems or not; and
- If yes, what decisions and actions that the incident reporter proposes to take/have taken and what actions are requested.

HRDs can use different secure means of communication to report incidents. They can also convene meetings where the reporter provides oral accounts on the incidents.

## STEP 3:

### Analysing Incident Facts

While carrying out an analysis on the facts, certain issues need to be taken into consideration such as: who might be involved, where did the incident occur, was there any physical injury or property damaged, and what was the probable goal of the perpetrators? This will dictate the next step on whether and when to react. At this point, one should determine the gravity of the incident in order to know whether the incident is minor or serious.

## STEP 4:

### To React or not to React

When the analysis shows that the incident is serious, HRDs should take necessary actions. The actions depend on the nature of the incident. In case of an office break-in, new locks/ security system should be put in place. If an HRD is arrested, the immediate reaction would be to secure his or her release. If an HRD is injured, there is a need to provide first aid support and seek further medical attention.

If an incident is considered as minor, HRDs may not react but they are required to document the incident for future reference. An incident is deemed serious when it is related to HRDs' work and their general physical health and mental wellbeing. Therefore, the incident becomes a threat and an in-depth analysis is required.

3 Koenraad Van Brabant 'Operational Security Management in Violent Environments' June 2000, Page 240, <https://sites.google.com/site/ngosecurity/GPR8.pdf?attredirects=0>

# 4

## CHAPTER

# UNDERSTANDING THREATS

## What is a Threat?

A threat can be defined as a declaration or indication of an intention to inflict damage, punish, or hurt.<sup>4</sup> Threats are triggers that communicate the dangers ahead. They could be verbal or non-verbal.

## Examples of Threats to HRDs

Some of the most common threats to defenders include the following:

1. We will close your organisation if you do not stop your work.
2. You are the next.
3. You will not live to see your children; and
4. I will kill you.

Threats are the most common strategies used against HRDs by stakeholders whose interests are affected negatively by the work of HRDs. Threats are preferred to attacks/aggressions because they are the cheapest tactics to stop the work of HRDs.

Threats are signs that harm could occur to HRDs. Aggressors gather information about HRDs and their work which they use to threaten them if HRDs continue to ignore threats and the aggressors may implement the threats resulting into harm. Therefore, HRDs should analyse threats to identify the potential dangers and put in place mitigation mechanisms.

<sup>4</sup> Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, <https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk>, Accessed 23 June 2016.

## Making Threats Versus Posing Threats

HRDs ought to know whether threateners are so serious to commit any act of aggression/ attacks. Some people may threaten, but they do not actually execute their threats whereas others implement warnings against HRDs. But it all depends on the socio-political environment where HRDs operate. There is also a need to refer to the execution and non-execution of past threats and the credibility<sup>5</sup> of the source of the threats.

Most people who **make** threats ultimately **pose** a threat: These people will threaten HRDs and will avail all necessary means to execute their plans.



Some people who **make** threats **do not pose** a threat: In many cases, threats are not implemented because threateners want to achieve their objectives without paying costs. Although the threats may not be executed, HRDs are urged to keep monitoring a series of similar threats and security incidents.



Some people who **rarely make** threats **do pose** a threat: Unlike the first two examples, this category of people does not declare their intentions to harm. Instead, they lurk in silence. They pose danger without warning. HRDs ought to interpret how and when the silence can bite.

*Adapted from Front Line Defenders manual: Workbook on Security*

## Threateners Versus Threat Implementers

In threat analysis, HRDs tend to focus more on the person who issues threats. For various reasons, the real threatener hires other people to deliver or execute the warnings. HRDs need to make more efforts to identify the real sources of the threats. The case below shows that sources of the threats can hire people to execute their threats:

The case of a Nigerian Land Rights Activist, late Ken-Saro Wiwa, shows that the people who communicate and execute threats are not the real threateners. This activist was hanged at the order of the president. However, an in-depth analysis shows that the presidential order was motivated and facilitated by a Multi-National Corporation (MNC) called Shell .

## How to Analyse Threats

A proper assessment of threats is necessary to identify the sources and objectives of the threats and examine the probability of threat execution. Threat analysis can be done individually or at an organisational level. Individual HRDs can involve their colleagues to get a non-biased conclusion about threats.

When HRDs are analysing threats, they must consider the facts, patterns, sources, and objectives of the threats. This helps to come up with a conclusion on whether threats can be executed or not<sup>6</sup>. Below are five steps for threat analysis:

- 1. Establishing facts surrounding threats:** HRDs look at the nature of the threats, what kind of threats, who communicated the threats and how the threats were communicated. The acts may be threatening messages, phone calls, pieces of advice on human rights activities at stake, summons, pronouncements by government on the activities of HRDs, visits of government and multi-national company officials or visits of security services, etc.
- 2. Determining the patterns of threats over time:** HRDs point out a series of acts that have taken place in a certain period. HRDs look at the time, the frequency and the gravity of the threats. Threatening messages may be sent using abnormal means such as red ink, blood, skull and bones images and the like. Extreme threat tools such as empty coffins or coffins having dead animals may be used as well.
- 3. Examining the objective of threats:** HRDs are to assess the intention of the threateners. It may not be easy to know the exact intention of the threateners, but HRDs should endeavor to conduct an in-depth analysis of their probable intentions. It is important to look at how HRDs activities impact negatively on stakeholders interests and the types of threats they receive;
- 4. Examining the source of threats:** It is hard to know the exact source of the threats because real threateners may use proxies to conduct businesses and to execute threats. HRDs need to dig deep in their analysis to find out who or where the threat is coming from. Knowing the source of the threats enables HRDs to know the ability to execute the posed threats.
- 5. Make conclusion on threat execution:** This final step helps HRDs to decide whether the threats will materialise into dangers or not.

**Please note:** The threat facts and patterns are based on actual occurrences whereas the source and the objective of threats are based on assumption and informed guesswork. The conclusion is based on the probability and considers the outcomes of the first four steps.

6 <https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf>

# 5

## CHAPTER

# RISK ASSESSMENT

HRDs work towards achieving the full respect, protection and realisation of human rights enshrined in the UDHR and other human rights instruments. Defenders working towards the incorporation of these instruments in domestic laws of various countries with different systems of governance puts them in great danger from different stakeholders including state authorities, private sectors and local communities. These dangers are inherited in the HRDs work and cannot be eliminated. This chapter looks at how HRDs effectively manage and mitigate the dangers from taking place.

## What is Risk?

Risk can be defined as the possibility of an event that results in harm. Risks can be the dangers HRDs face in their daily work.

## Examples of Risks

HRDs face risks such as arrest, detention, imprisonment, murder, verbal and non-verbal assaults, abduction/kidnap, character assassination, smear campaign, rejection by society and fellow professionals, summons, blackmails, closure of the office, police raids, office break-ins, interception and tapping of HRDs communications and trailing. In other words, risks are uncertain dangers that HRDs face because of their human rights activities.

## Components of Risk

Risk is composed of three variables namely vulnerability, capacity and threat. The three components are interdependent and determine the probability and impact of a risk.

- 1. Vulnerabilities:** Vulnerabilities can be described as internal weaknesses of HRDs which increase the likelihood of harm occurrence or aggravate its impact.
- 2. Capacities:** Capacities are internal resources/abilities/strengths that can be used to reduce harm and its impact.
- 3. Threats:** Threats are external factors signalling the risks that can possibly affect the HRDs work.



## Nature of Risks

Risks differ according to HRDs context including profile, location, resources and approaches and activities/ issues undertaken by HRDs.

## How to Assess Risks?

HRDs should analyse risks properly to put in place appropriate risk mitigation measures. They should identify risks and their sources and measure the probability and impact. They should consider whether they can withstand the identified risks.

Risks can be assessed using the following steps:

### 1. Risk identification

Risk identification is an initial but critical stage in risk assessment. It involves listing potential dangers that HRDs can face. An HRD should catalogue risks in a checklist so that each risk is thoroughly analysed. Risks can be identified through brainstorming or interviews. An HRD should catalogue risks in a checklist so that each risk is thoroughly analysed. While analysing the risks, HRDs should look at the security incidents and threats, the reaction of stakeholders and risks faced by other HRDs.

### 2. Risk sources

HRDs need to point out both obvious and underlying causes of a risk. Risk causes can be institutions or individuals whose interests are affected by HRDs work. HRDs also need to look at the link between two or more risk causes and possible interactions of causes to implement risks;

### 3. Risk Probability

Various factors influence risk implementation. HRDs consider the chance for a risk to occur by looking at the abilities of risk causes to execute risks, the nature of work in terms of sensitivity and the context in terms of factors and actors influencing HRDs work. It is important to study probability rates of risks faced by HRDs in the past to gauge the likelihood of the present risks to be executed. Risk probability is gauged according to the threshold of high, medium, or low;

### 4. Risk Impact

The risk impact is estimated in terms of damage associated with identified risks. HRDs vulnerabilities and capacities can make the damage high, medium or low;

## 5. Risk Tolerance

Risk tolerance is measured in capacities and vulnerabilities of HRDs to withstand identified risks. HRDs are required to increase their capacities to measure up to identified risks and reduce risk impacts; and

## 6. Conclusion

HRDs need to come up with a conclusion whether identified risks can occur or not. The conclusion looks at HRDs abilities to withstand a risk. If HRDs can withstand the risk, they must put in place measures to reduce its impact. This step enables HRDs to also think of possible scenarios of risk execution and adopt effective strategies.

## Common misconceptions about Risk management

**1. Focus on reactive strategies:** Most HRDs only put in place security management measures after facing risks or threats. However, it is important to consider all probable risks that may have an impact on HRDs and put in place preventive strategies;

**2. Copy and paste syndrome:** Some HRDs apply security management measures that work well for other defenders. HRDs work on different themes and operate in different contexts, hence the contextualisation of security measures. For example, the installation of CCTV cameras may attract attention and suspicion to HRDs working in rural areas;

**3. Heroism syndrome:** Extreme bravery sometimes places HRDs at unnecessary risks. It is advisable for HRDs to measure their vulnerabilities vis-à-vis the magnitude of threats or risks facing them as they are more valuable alive than dead;

**4. Misunderstanding of HRDs work:** In some cases, HRDs confuse political activism and human rights work, which can hinder the dialogue between authorities and civil society. Limited constructive dialogues create mutual suspicion yet governments and HRDs should work in complementarity; and

**5. Tendency to ignore one's safety and security:** HRDs tend to give more priority to their work and victims of violations rather than their own safety and security. The foundation of HRDs work is based on their safety and security and without it, human rights work cannot be sustained.

# 6

## CHAPTER

# SAFETY & SECURITY PLANNING

Risks are inherent to HRDs work and they cannot be eliminated. However, they can be mitigated, transformed, and/ or transferred. Therefore, HRDs need to regularly conduct risk assessment to devise effective safety and security plans.

Safety and security planning is the process of putting in place and implementing preventive and reactive measures to enhance HRDs capacities to reduce the impact of risks. It applies to individual HRDs as well as groups and organisations. Safety and security planning involves developing policies, plans and protocols.

A policy consists of general rules, principles and guidelines whereas a plan focuses on the policy implementation. A protocol consists of standard operating procedures to deal with a specific event.

## Components of a Safety and Security Policy

A policy describes the overall management of organisational safety and security. It should be tailored to the safety and security needs of an organisation.

Below are standard components of a safety and security policy:

- Principles: The primacy of life over assets, individual and collective responsibilities, do no harm, etc;
- Approach and framework for safety and security management;
- Attitude to risks – how much is acceptable;

Assessment of the threats against the organisation, at a general level

- Who should assess this, how often?
- How should this be communicated?
- Safety and security roles and responsibilities: A policy should clearly spell out roles and responsibilities at all levels; and
  - Requirements for monitoring the effectiveness of security management: For instance, how often the policy should be revised.
  - For further suggestions on the creation of a security policy, see People in Aids Policy Pot on Safety and Security, May 2003<sup>8</sup>.

# Components of a Safety and Security plan

Safety and security plans are meant to address the risks and threats related to HRDs in specific situations or events. To come up with a plan, HRDs should brainstorm about the potential risks/threats, vulnerabilities, and capacities. A good plan must identify risks and have preventive and reactive measures to mitigate the risks. For example, HRDs working on Female Genital Mutilation (FGM) can develop a specific plan to address risks related to their work.

## What to consider in developing a plan?

- A plan should be concise, precise and available as a reference document, user friendly and with up-to-date information;
- It should address potential risks/threats through a proper assessment; and
- For each vulnerability, an action should be formulated to meet the required capacity and therefore mitigate the risk.

## Implementation of a Safety and Security plan

For effective implementation, a detailed plan should be communicated to all parties involved in a clear language. It should spell out precise and specific roles/responsibilities of each party and include disciplinary measures to ensure adherence to the plan. In addition, the implementation of the plan requires resources, time, knowledge and awareness. The plan needs to be reviewed regularly to address emerging risks/threats.

## Security Strategies

There are three main security strategies/ approaches that HRDs and their organisations apply in their day-to-day human rights work.

- 1. Acceptance strategy:** an approach which involves negotiating with all actors – the local community, the authorities etc, to gain acceptance and ultimately support for the organisation's presence and work. Although this requires careful planning and can be labour-intensive, it may be the most effective strategy in the longer term to reduce threats. This approach usually entails high visibility, so in times of great threat, it is sometimes more difficult to adapt to being more low profile;
- 2. Protection strategy:** an approach which emphasises security procedures and protective elements. Impact is mainly on reducing vulnerabilities and can be used in conjunction with the other two strategies to strengthen protection; and
- 3. Deterrence strategy:** an approach which relies on counterthreats for protection. For example, if threatened, an organisation might react by taking a legal case out against the person issuing the threat, or by publicising the threat, or responding to the perpetrator by explaining the consequences of carrying out the threat – such as international condemnation. This approach should only be used if you have accurate information and powerful allies. When you are developing your security plans, consider how elements of acceptance, protection, and deterrence can expand the menu of options you have at your disposal.<sup>9</sup>

# 7

## CHAPTER

# EXISTING PROTECTION MECHANISMS FOR HRDs

Recognition of the vital role of HRDs and the violations that many of them face convinced the United Nations (UN) that special efforts were needed to protect both defenders and their activities. The first major step was formally to define the defence of human rights as a right in itself and to recognise persons who undertake human rights work as HRDs.

## United Nations Special Rapporteur on HRDs

On 9 December 1998, by its resolution 53/144, the General Assembly of the United Nations adopted the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms (commonly known as the Declaration on HRDs).

The second step was taken in April 2000, when the United Nations Commission on Human Rights (now the United Nations Human Rights Council) asked the Secretary-General to appoint a special representative on HRDs to monitor and support the implementation of the Declaration.<sup>10</sup>

In 2000, the Commission on Human Rights established the mandate of Special Representative on HRDs (as a Special Procedure) to support implementation of the 1998 Declaration on Human Rights Defenders.<sup>11</sup>

The mandate stipulates that the Special Rapporteur's main roles are to:

- Seek, receive, examine, and respond to information on the situation of human rights defenders;
- Establish cooperation and conduct dialogue with governments and other interested actors on the promotion and effective implementation of the declaration;
- Recommend effective strategies to better protect HRDs and follow up on these recommendations; and
- Integrate a gender perspective throughout his/her work.

10 Fact Sheet 29 - Human Rights Defenders: Protecting the Right to Defend Human Rights <https://www.ohchr.org/Documents/Publications/Fact-Sheet29en.pdf>

11 OHCHR, 'resolution 2000/61 establishing the mandate' <http://ohchr.org/EN/Issues/SRHRDefenders/Pages/Mandate.aspx>, accessed 1 August 2016.

Several regional mechanisms have been created following the establishment of the UN special rapporteur on HRDs with the aim of increasing the protection of HRDs. The following are the major regional mechanisms:

- i. The Special Rapporteur on HRDs of the African Commission on Human and Peoples Rights (2005)<sup>12</sup>;
- ii. The Special Rapporteur on HRDs of the Inter-American Commission for Human Rights<sup>13</sup>;
- iii. The European Union Guidelines on HRDs adopted by EU foreign ministers in 2004.<sup>14</sup>; and

The European Union has also appointed a Special Representative for Human Rights, who has a mandate to enhance the effectiveness and visibility of EU human rights policy.<sup>15</sup>

In 2004, the African Commission on Human and Peoples' Rights (ACHPR) established the mandate of the Special Rapporteur on HRDs in Africa to address the situation of HRDs in the Africa<sup>16</sup> with the following mandate<sup>17</sup>:

- 1.** To seek, receive, examine and to act upon information on the situation of HRDs in Africa;
- 2.** To submit reports at every Ordinary Session of the African Commission;
- 3.** To cooperate and engage in dialogue with Member States, National Human Rights Institutions, relevant intergovernmental bodies, international and regional mechanisms of protection of human rights defenders, HRDs and other stake holders;

- 4.** To develop and recommend effective strategies to better protect HRDs and to follow up on his/her recommendations; and
- 5.** To raise awareness and promote the implementation of the UN Declaration on HRDs in Africa.

Since the establishment of the mandate, the Special Rapporteurs have maintained regular contact with HRDs through their participation in regional forums and carried a number of country visits, including joint visits and press releases with the UN Special Rapporteur.<sup>18</sup>

The Special Rapporteur has also encouraged individuals and non-governmental organisations to submit cases concerning HRDs to the ACHPR. Under the African Charter on Human and Peoples' Rights, the ACHPR is empowered to receive and consider communications from individuals and organisations<sup>19</sup>.

## European Union Guidelines on HRDs

The European Union (EU) has undertaken to promote the implementation of the UN Declaration on HRDs through their foreign policies. In 2004, the EU adopted guidelines on how its members contribute to promoting, supporting and protecting HRDs. While these guidelines are not legally binding, they represent political commitments by the EU and individual governments concerned.

The implementation of these guidelines has been identified as a priority within the EU's human rights foreign policy.

12 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, <http://www.achpr.org/sessions/35th/resolutions/69/> accessed 1 August 2016.

13 Inter-American Commission on Human Rights, AG/RES. 1842 (XXXII-O/02), 'Human Rights Defenders: Support for Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas' [http://www.oas.org/juridico/english/ga02/agres\\_1842.htm](http://www.oas.org/juridico/english/ga02/agres_1842.htm), accessed 1 August, 2016.

14 EUR-Lex, Access to European Union Law, 'EU guidelines on human rights defenders' 8 December 2008, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3A133601>, accessed 1 August 2016.

15 European Union, "EU Special Representatives," [https://eeas.europa.eu/headquarters/headquarters-homepage\\_en/3606/EU%20Special%20Representatives](https://eeas.europa.eu/headquarters/headquarters-homepage_en/3606/EU%20Special%20Representatives) (accessed 11 May 2020).

16 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, <http://www.achpr.org/sessions/35th/resolutions/69/> accessed 1 August 2016.

17 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, <http://www.achpr.org/sessions/35th/resolutions/69/> accessed 1 August 2016

18 DefendDefenders, 'Defending Human Rights, A Resource Book for Human Rights Defenders, East and Horn of Africa Human Rights Defenders Project, 2nd edition, page 8

19 Article 55 of the African Charter on Human and People' Rights

The UN mandate collaborates with the regional mechanisms to ensure protection of HRDs. Collaboration includes sharing experiences and information, comparing and mutually reinforcing working methods and identifying common objectives.

States around the world have created mechanisms at national level for the protection of HRDs these include inclusion of the rights of HRDs in national constitutions and legislations, and inclusion in national human rights institutions.

In some instances, they have enacted specific legislation for the protection of HRDs.

The Special Rapporteur on HRDs of the African Commission on Human and Peoples' Rights

## Diplomatic Guidelines

In addition to the EU, some countries adopted guidelines on the protection of HRDs:<sup>20</sup>

- Canada: *Voices at Risk;*
- Netherlands: *Action plan for HRDs;*
- Finland: *Finnish Guidelines on HRDs;*
- Norway: *Guide for the foreign service;*
- Switzerland: *2019 revised Swiss Guidelines on HRDs (replacing 2014 version of Swiss Guidelines on HRDs);*
- United Kingdom: *UK support to HRDs; and*
- United States: *Archived fact sheet on HRDs.*

## National Mechanisms for HRDs Protection

The Declaration on HRDs stresses that the primary responsibility and duty to promote and protect human rights and fundamental freedoms lies with the state. Therefore, states are required to ensure HRDs safety and protection by implementing the Declaration on HRDs.

In June 2016, Ivory Coast adopted The Law on the Promotion and Protection of Human Rights Defenders. It was the first time an African State enacted a law with the specific purpose of protecting HRDs.<sup>21</sup>

- 1. Administrative mechanisms-** National Human Rights Institutions, legal institutions such as judiciary, law enforcement, police, national security, legislative bodies and local governments;
- 2. Legislations-** Constitutions and specific laws such as. The Law on the Promotion and Protection of Human Rights Defenders' in Ivory Coast; and
- 3. Civil society institutions-** Networking among Civil Society Organizations (CSOs) and National Coalitions for HRDs .

The work of HRDs is inherently stressful. Risks and threats that HRDs face are not only physical and digital but most often psychological too. HRDs suffer rejection, discrimination and often sacrifice too much as a result of their work.

Security interventions focus on physical and digital components. However, HRDs' safety and security ought to be holistic and include mental wellbeing. The state of mind determines what kind of security decisions and choices HRDs make.

20 ISHR 'strengthening diplomatic initiatives for the protection of human rights' <https://www.ishr.ch/diplomatic-support>

21 Download the Côte d'Ivoire Law on human rights defenders here (French only), [http://www.ishr.ch/sites/default/files/documents/jo\\_loi\\_defenseurs.pdf](http://www.ishr.ch/sites/default/files/documents/jo_loi_defenseurs.pdf)

# 8

## CHAPTER

# SELF-CARE & RESOURCING RESILIENCE

## Understanding Stress in HRDs' Context

### What is stress?

Stress can be defined as a reaction to a stimulus that disturbs our physical or mental balance. It is a person's physical and emotional reaction to change. Stress is frustrating and draining because of the imbalance between the HRDs' capacities and the challenges that the situation presents. Stress is not the same for everyone - what might be stressful to one HRD may not be stressful to another. Similarly, stress has different levels from low to high.

### Types of Stress.

There are various ways of describing stress. According to [Healthline: Medical information and health advice you can trust](#), Stress can be categorised according to its nature over a period of time as follows.

#### i) Acute stress

This is the most common form of stress. It comes from demands and pressures of the recent past and anticipated demands and pressures of the near future. Acute stress hits at once and causes the level of anxiety to rise rapidly. For example, being called for a job interview, missing a flight and receiving bad news can cause panic.


#### i) Episodic acute stress

When acute stress happens regularly, it is called episodic acute stress. This kind of stress is repetitive and usually takes a regular pattern. It can be likened to a wave that has peaks and lows. Examples of acute episodic stress could include rent stress, school fees stress and loan repayment stress.

#### i) Chronic stress

This is a permanent type of stress people live with. It is the grinding stress that wears people away day after day, year after year. Chronic stress destroys bodies, minds and lives. It wreaks havoc through long-term attrition. It is the kind of stress lined to permanent situations such as dysfunctional families, incurable diseases, of being trapped in an unhappy marriage or in a despised job or career.

## Common causes of stress in HRDs context

-  Wars and conflict
-  Shrinking political space for civil society engagement
-  Corruption and economic malpractice
-  Electoral strife
-  Harassment
-  Arbitrary arrest and detention
-  Defamation and stigmatisation
-  Discrimination
-  Torture
-  High poverty levels

## Symptoms of Stress

Stress has behavioural, physiological and psychological symptoms. It can be observed through a change in behaviour patterns and in biological body functions. It could also manifest through a change in emotions and mental processes.


Some of the behavioural symptoms include self-negligence, change in eating habits, change in dressing habits, change in sleeping patterns, withdrawal tendencies, aggressiveness, irritability etc.

Physiological symptoms include bodily fatigue, excessive sweating, ulcers, headaches, diarrhoea and change of menstrual cycle.

Mental/psychological symptoms include forgetfulness, speech disorder, memory loss, sadness, anger, low work performance.

## Managing Stress

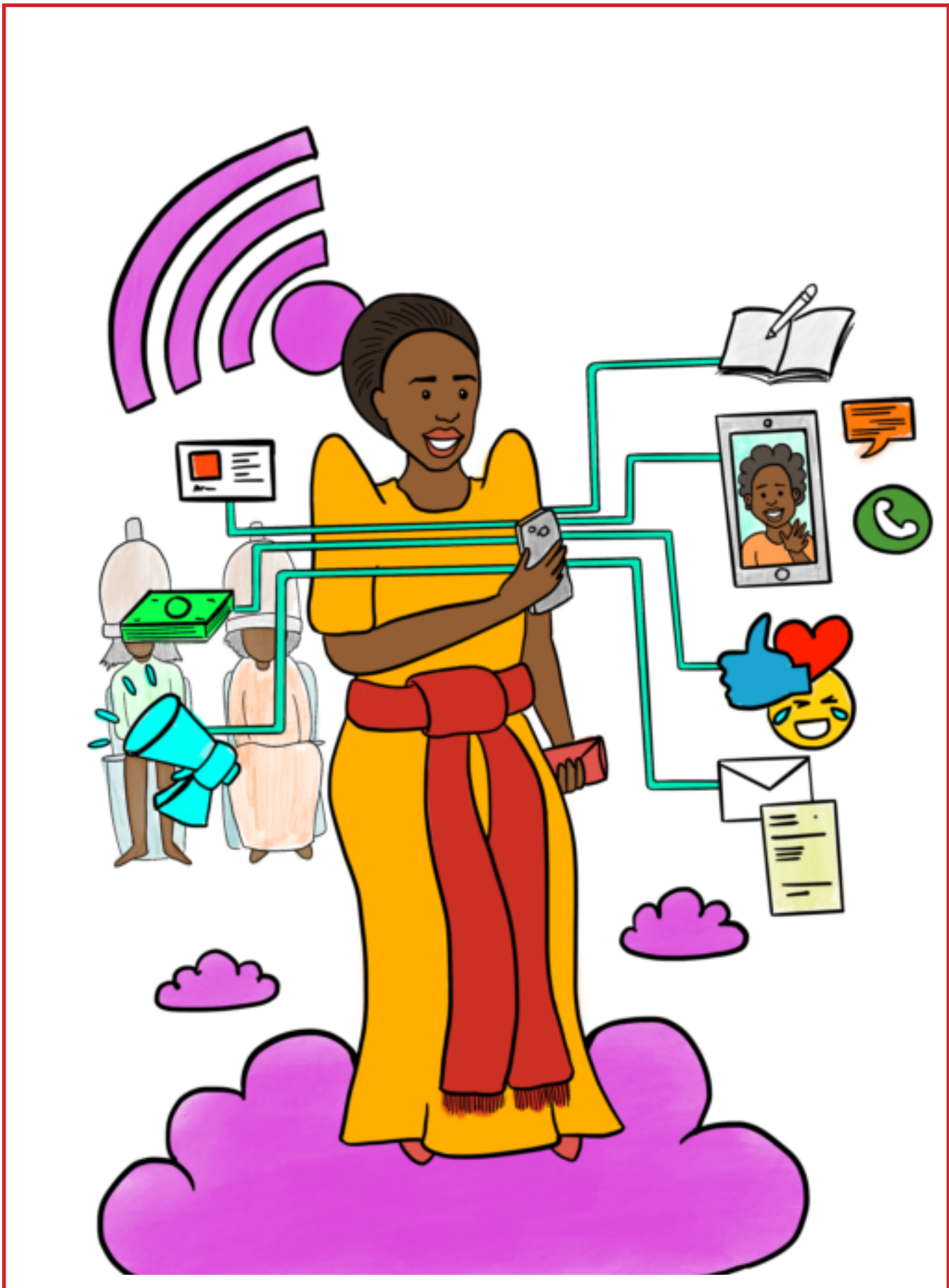
Stress by nature cannot be completely eliminated. In stress management, the aim is to point out what the stressors are – the main problems and demands that are causing stress. By so doing, one can explore options that will help to overcome the negative impact brought by these stressors. There are various ways of stress management that can be applied including talk therapy, environmental therapy, body works and massage therapy, artistic therapy and many others. HRDs are encouraged to use simple self-care practices that do not require any scientific expertise. Some of the practices are listed in the image below.

Slow Down	Keep Calm	Be Positive	Take it EASY
UNPLUG	Enjoy LIFE	Have FUN	BREATHE
	Go OUTSIDE		MEDITATE

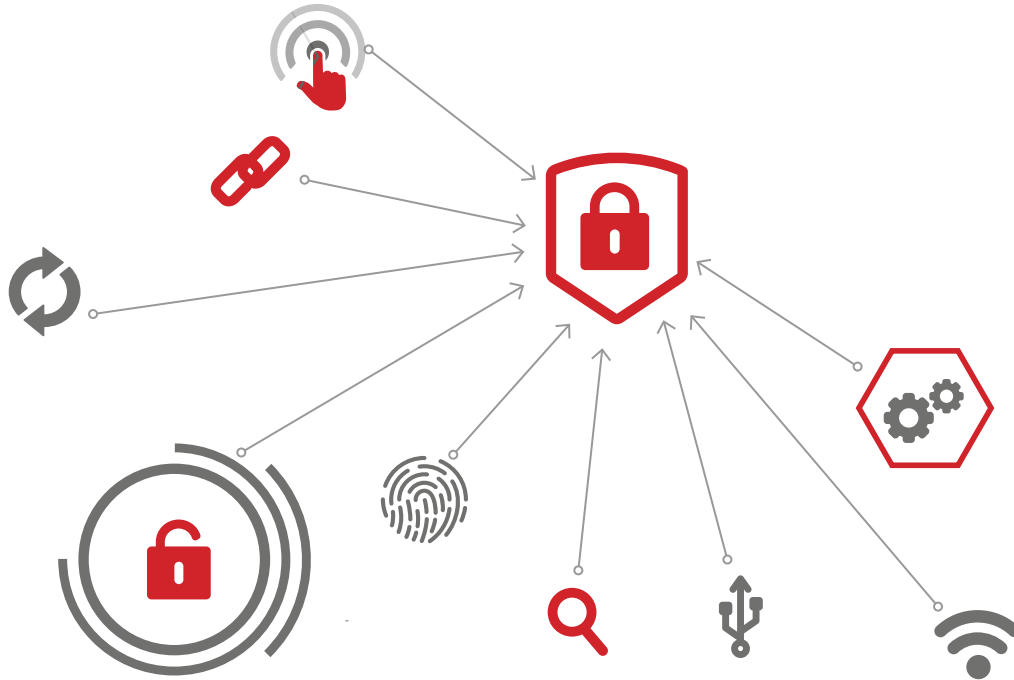


Other recommended ways of coping with stress are listed below: <sup>22</sup>

- ✓ Take care of yourself, by eating healthy, exercising and getting plenty of sleep;
- ✓ Find support by talking to other people to get your problems off your chest;
- ✓ Connect socially, as it is easy to isolate yourself after a stressful event;
- ✓ Take a break from whatever is causing you stress;
- ✓ Avoid drugs and alcohol, which may seem to help with stress in the short term, but can cause more problems in the long term;
- ✓ Learn to say NO and take No as a response.
- ✓ Take the time to relax;
- ✓ Do the things that you like e.g., singing, dancing, playing a game;
- ✓ Manage your agenda (work, home, leisure); and
- ✓ Ultimately drop the activity if it hurts more than it excites and if other solutions for the stress have not worked. It is important to note that it is not the load that breaks you, it is how you carry it. Stress itself can bring about positive outcomes. For instance, stress can push someone to work harder/better. However, if stress is not well managed, it can be very harmful.







# DIGITAL SECURITY

A BOOKLET FOR AFRICAN  
HUMAN RIGHTS DEFENDERS

The Digital Security Booklet portion contains localised content adapted from [Surveillance Self Defense](#) produced by the Electronic Frontier Foundation and is released under the same license.

Licensed under [CC-BY-3.0](#) copyleft agreement: You are free to copy and redistribute the material in any medium or format as well as remix, transform, and build upon the material for any purpose, provided you attribute the material to its original authors.

# CONTENT

<b>HOW TO USE THIS MANUAL</b>	<b>30</b>
<b>BASIC DEVICE SECURITY</b>	<b>34</b>
<b>SECURITY OF DATA ON DEVICES</b>	<b>38</b>
<b>SECURITY OF DATA MOVING THROUGH NETWORKS</b>	<b>41</b>
<b>ACCOUNT SECURITY</b>	<b>48</b>
<b>MOBILE SECURITY</b>	<b>51</b>
<b>ANNEXES</b>	<b>58</b>

# HOW TO USE THIS MANUAL

## **Introduction: Digital Safety Manual**

You are a 21st Century African Human Rights Defender. You are armed with your keen intellect, strong sense of social justice, connections to local communities, a mobile phone and a laptop. 20 years ago, you certainly would have had the first three but the phone in your pocket and the laptop in your bag are unique to the 21st century.

Digital technology complicates our ability to assess our personal and professional risk because they are almost always unintuitive. Without specialist and technical knowledge, it is difficult to analyse where devices betray the trust put in them to store sensitive files and communicate confidential information.

Africa is often said to have leapfrogged over old technology in the case of wired landline phones as the market of mobile phones exploded across the continent at much faster rates than anywhere else in the world. Conversely, global technological, legal and human rights norms related to privacy and security have an enormous impact on the environment for African HRDs and society at large without necessarily having an equal opportunity to affect such developments.

The global war on terrorism has grown in tandem with widespread usage of personal telecommunications technology such as Email, Skype, Facebook Messenger and WhatsApp and set up a showdown between individual privacy rights and arguments for collective security. At the same time, private security firms developing offensive hacking software and hardware sold to world governments means that sophisticated digital surveillance are within reach of law enforcement agencies at substantially lower costs.

The global pandemic (COVID-19) has forced organisations to adopt online working methods. This has increased the risk associated to the work done by HRDs as this new normal has happened very fast without due regard of the underlying security risks. This booklet will avail you with technological knowledge to be able to better assess your digital risks as they affect your human rights work, and to take steps to mitigate those risks. Throughout this booklet we will refer to scenarios and stories of African HRDs as they encounter digital challenges and questions in their work. This booklet is organised in the following structure:

### **i) Risk assessment**

Every user faces cyber security threats, from peasants to presidents. Compared to ordinary users though, the stakes are higher for HRDs due to the nature of their digital activities.

In this section we will break apart the concept of risk and look at categories of technological risk in the context of real-world impacts. You will learn to identify your most at-risk assets and begin to prioritise measures to reduce vulnerabilities.

### **ii) Five security goals**

The remainder of this booklet will explore five categories of digital security which together contribute to overall security of your digital practices. These chapters are not intended to be exhaustive, and it is not possible to teach skills entirely through these pages as software changes often however we will link you to resources which stay updated with the newest references. Our five security Goals are:

#### **a) Basic device security**

We are responsible for our devices (not the other way around!), but do we know how to operate them correctly? Are we doing the best to keep them in good operating condition resistant to viruses and other vulnerabilities which may occur against them? In this section we will discuss best practices for operating system and software usage.

#### **b) Security of data on computers, flash disks, external drives and mobile phones**

Data is stored on your laptop, desktop, mobile phone, external hard drives and USB thumb drives. If someone were to physically obtain these devices or copy files off them physically or through a network, would they be able to read (and change) that data? In this section we will discuss the concept and practices of encryption, which protects data as it sits on your devices, storage or in the cloud.

Furthermore, data security is compromised if you only have one copy of important documents and that copy is lost due to corruption, theft, physical damage, or other computer catastrophes. We will look at backup solutions and consider the security of those backup practices.

#### **iii) Security of data moving through networks**

Most of the value of our computers and phones come with the fact that they communicate with other devices through the Internet and mobile networks. Communication takes place over many modes such as email, web browsing, instant messaging, voice over IP and regular phone and text messages (discussed under Mobile Security). We will look at the nature of these communication flows and understand the security implications of them, especially in the context of increasing surveillance.

#### **iv) Security of accounts**

How do we ensure that our online and offline accounts are not broken into, leading to loss of data, identity and impersonation? Best practices such as unique passwords, two factor authentication, and password managers are covered here.

#### **v) Mobile security**

Traditional mobile telephones (voice and SMS) were not built with security in mind. Smartphones introduce new capabilities and new risks and we learn about all of the above areas of security as they relate to mobile phones.

When we talk about the first question, we often refer to assets. An asset is something you value and want to protect. When we are talking about digital security, the assets in question are usually information. For example, your emails, contact lists, instant messages and files are all assets. Your devices are also assets.



## Risk Assessment

There is no single solution for keeping yourself safe online. Digital security is not about which tools you use; rather, it is about understanding the threats you face and how you can counter those threats. One should conduct a threat modelling assessment to tailor it to their needs.

When conducting an assessment, there are five main questions you should ask yourself:

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through to try to prevent those?

When we talk about the first question, we often refer to assets. An asset is something you value and want to protect. When we are talking about digital security, the assets in question are usually information. For example, your emails, contact lists, instant messages and files are all assets. Your devices are also assets.

**Write down a list of data that you keep, where it is kept, who has access to it and what stops others from accessing it.**

To answer the second question- Who do you want to protect it from? It is important to understand who might want to target you or your information, or who is your adversary. An adversary is any person or entity that poses a threat against an asset or assets. Examples of potential adversaries are corporate entities, rogue government actors, or a hacker on a public network.

**Make a list of who might want to get a hold of your data or communications. It might be an individual, a government agency or a corporation.**

A threat is something bad that can happen to an asset. There are numerous ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data. An adversary could also disable your access to your own data.

The motives of adversaries differ widely, as do their attacks. A government trying to prevent the spread of a video showing police violence may be content to simply delete or reduce the availability of that video, whereas a political opponent may wish to gain access to secret content and publish it without you knowing.



**Write down what your adversary might want to do with your private data.**

The capability of your attacker is also an important thing to think about. For example, your mobile phone provider has access to all of your phone records and therefore has the capability to use that data against you. A hacker on an open Wi-Fi network can access your unencrypted communications. Your government might have stronger capabilities.

To answer the third question, you must consider risk. Risk is the likelihood that a particular threat against a particular asset will occur and goes hand-in-hand with capability. While your mobile phone provider has the capability to access all of your data, the risk of them posting your private data online to harm your reputation is low.

It is important to distinguish between threats and risks. While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur. For instance, there is a threat that your office may be broken into, but the risk of this happening is far lesser in a location where you have guards or friendly neighbours as opposed to a location where you are viewed with hostility.

Conducting a risk analysis is both a personal and a subjective process; not everyone has the same priorities or views threats in the same way. Many people find certain threats unacceptable no matter what the risk because the mere presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.



### Now, Let's Practice Threat Modelling

If your office stores whistle-blower's accounts of corruption in public service, you might want to ask

- Should the office have 24-hour guards, CCTV cameras?
- What kind of door lock should we invest in?
- Do we need more advanced security in addition to a strong door lock?
  
- How important is what we are trying to protect?
  - Evidence that can end corruption in public service
  
- What is the threat?
  - The accused perpetrators will try to break in and access these files
  
- What is the actual risk if the accused break in? Is it likely?
  - If the perpetrators of the corruption get these testimonies, they can physically attack the whistle-blowers
  - They can steal the files and destroy evidence that can be used against them

Once you have asked yourself these questions, you are able to assess what measures to take. If your possessions are valuable, but the risk of a break-in is low, then you probably will not want to invest too much money in a lock. On the other hand, if the risk is high, you will want to get the best locks on the market, and perhaps even add a security system.

## Digital Security in Five Parts

### IMPORTANT

The actions described in the following sections are often technical and can carry degrees of risk. Making changes to your devices can cause unexpected errors or if not properly implemented can lead to data loss. It is advisable to research all the steps needed to make technical changes as appropriate to your particular device and context, take backups of important data, properly store new passwords (See Account Security for relevant advice) and enlist technical assistance when necessary.

## How Do I Protect Myself Against Malware?

Nansubuga is Ugandan land rights defender. She bought a new computer 6 months ago, but it is running slowly, she sees pop-up windows on her screen which she does not understand, and her mobile internet data seems to be running out too quickly. She was carrying project documents on a flash drive but they constantly disappear from her drive. She does not understand what is happening, it is a new computer and she installed all her software from online download sites and from good friends.

-----

Nansubuga is most likely experiencing unwanted malware infections on her computer. Malware is a threat that affects all computer users. *Malware can lead to information loss, reduced performance, theft of documents and spying.*

# BASIC DEVICE SECURITY

Furthermore, legal jurisdictions and perspectives on digital security vary and each individual should seek to understand the risks involved according to their context.

All aspects of life now revolve around technology and the Internet to reincluding your phone, your car, watch, and refrigerator!) and will have the ability to be an Internet-connected device with the ability to send and receive information.

We entrust our devices with a lot of information that defines who we are, where we are, what we do, what we plan and with whom we make our plans. These devices are obvious targets for attack, compromise and infiltration.

With this background in mind, it is very important for all users of technology and the Internet to have a basic level of knowledge and skills to protect their devices against hackers, malware and any other vulnerability that can endanger their lives because of device compromise or attack.

Basic device security entails the practices and steps that put your devices into optimum configuration to avoid compromise.

Malware, short for malicious software, is **any program or file that is** used to harm computer users. It works in many different ways including, but not limited to, disrupting computer operation, gathering sensitive information, impersonating a user to send spam or fake messages, or gaining access to private computer systems. The majority of malware is criminal and is most often used to obtain banking information or login credentials for email or social media accounts. Malware is also used by both state and non-state actors to circumvent encryption and

to spy on users. For instance,<sup>23</sup> malware has wide-range capabilities; it may allow an attacker to record from a webcam and microphone and disable the notification setting.

## Anti-virus Software

You should use anti-virus software on your computer and your smartphone. Anti-virus software can be quite effective at combatting generic 'non-targeted' malware that might be used by criminals against the general population. However anti-virus software is usually ineffective against targeted and other sophisticated attacks, such as the ones sold by Israeli based security company NSO Group.

## Indicators of Compromise

When it is not possible to detect malware using antivirus software, it is still sometimes possible to find indicators of compromise. For example, Google will sometimes give a warning to Gmail users stating that it believes your account has been targeted by state-sponsored attackers. Additionally, you may notice a light indicating that your webcam is turned on when you have not activated it yourself (though advanced malware may be able to turn this off)—this could be another indicator of compromise. Other indicators are less obvious; you may notice your email is being accessed from an unfamiliar IP address or that your settings have been altered to send copies of all of your email to an unfamiliar email address. Your computer should already have a firewall activated such as the built in Windows or OS X firewall, but it is useful to also activate commercial firewalls part of Internet Security suites.

23 <http://pastebin.com/MP8zpQ26>.

## How can attackers use malware to target me?

The easiest way for one to be targeted by malware is through phishing emails. An attacker poses as someone you know and sends you an email with an attachment laced with malware. Once you download the attachment and open it, the malware infects your computer or device.

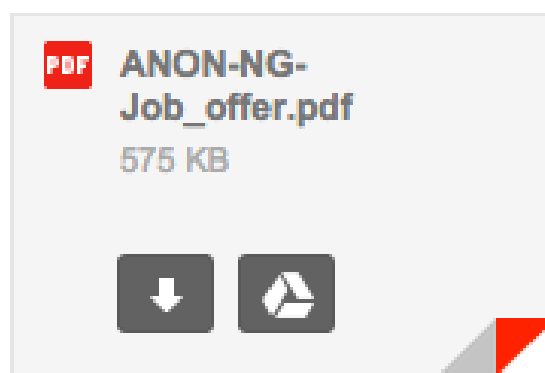
Zero-day attacks are another more sophisticated method of infecting devices with malware especially used by governments and criminals. Zero-day attacks exploit a previously unknown vulnerability in a technology device or application. Think of your computer as a fortress; a zero day would be a hidden secret entrance that you do not know about, but which an attacker has discovered. You cannot protect yourself against a secret entrance you do not even know exists. Governments and law enforcement agencies stockpile zero-day exploits for use in targeted malware attacks. Criminals and other actors may also have access to zero-day exploits that they may use to covertly install malware on your computer. Zero-day attacks are used to target very high-profile individuals because they are expensive to purchase.

There are many ways in which an attacker might try to trick you into installing malware on your computer. They may disguise the payload as a link to a website, a document, PDF, or even a program designed to help secure your computer. You may be targeted via email (which may look as if it is coming from someone you know), via a message on Skype or Twitter, or even via a link posted to your Facebook page. The more targeted the attack, the more care the attacker will take in making it tempting for you to download the malware.

For example, in December 2014, Neamin Zeleke, the managing director of Ethiopia Satellite Television (ESAT) was targeted from his office in the USA with remote monitoring software from Hacking Team that was delivered through an email claiming to have information about Ethiopian elections.

In 2013, one of Zeleke's colleagues was infected with malware after he opened what appeared to be a Microsoft word file. They later learned that it was the remote-control system Hacking Team.

The best way to avoid being infected with this kind of targeted malware is to avoid opening the documents and installing the malware in the first place. People with more computer and technical expertise will have somewhat better instincts about what might be malware and what might not be, but well-targeted attacks can be very convincing. If you are using Gmail, opening suspicious attachments in Google Drive rather than downloading them (see image for example) what would protect your computer if they are in fact infected. Using a more secure computing platform, like Ubuntu, Chrome OS, or Mac OS X significantly improves your odds against many malwares delivery tricks but will not protect against the most sophisticated adversaries.



**If you are using Gmail, you can view the attached document by clicking on this Triangle Icon inside the second square (not the download arrow) in the first square. It will appear on your browser through Google's filters rather than downloading and executing on your computer, sparing you from any risks of exploits inside of the file.**

Another thing you can do to protect your computer against malware is to always make sure you are running the latest version of your software and downloading the latest security updates. As new vulnerabilities are discovered in software, companies can fix those problems and offer that fix as a software update, but you will not reap the benefits of their work unless you install the update on your computer. It is a common belief that if you are running an unregistered copy of Windows, you cannot or should not accept security updates. This is not true. See below for more information on keeping your systems updated.

## What should I do if I find malware on my computer?

If you do find malware on your computer, disconnect your computer from the Internet and stop using it immediately. Every keystroke you make may be being sent to an attacker. You may wish to take your computer to a security expert, who may be able to discover more details about the malware. If you have found the malware, removing it does not guarantee the security of your computer.

If you suspect that your primary computer has malware, log into a computer you believe is safe and change your passwords; every password that you typed on your computer while it was infected should now be compromised.

You may wish to reinstall the operating system on your computer to remove the malware. This will remove most malware, but some sophisticated malware may persist.

## Keeping Updated

Computer hardware and software is never perfect. There will always be performance, stability, and security issues which emerge on any software: That includes your operating system (Windows, OS X, Linux), your mobile phone (Android, iOS, Windows Phone), your software (Adobe, Java, Office, Chrome, Firefox, etc.). There is a thriving market of researchers constantly looking for vulnerabilities in our systems. These researchers may be White Hats who disclose vulnerabilities publicly and encourage developers to patch software flaws, or they may be Black Hats who sell vulnerabilities to criminal and governmental buyers who plan to use these vulnerabilities against software users.

If you want to see how common vulnerabilities are, pay a visit to <https://www.exploit-db.com/> and browse how many vulnerabilities exist for the software we use. This explains why we are asked so often to update our system and software.

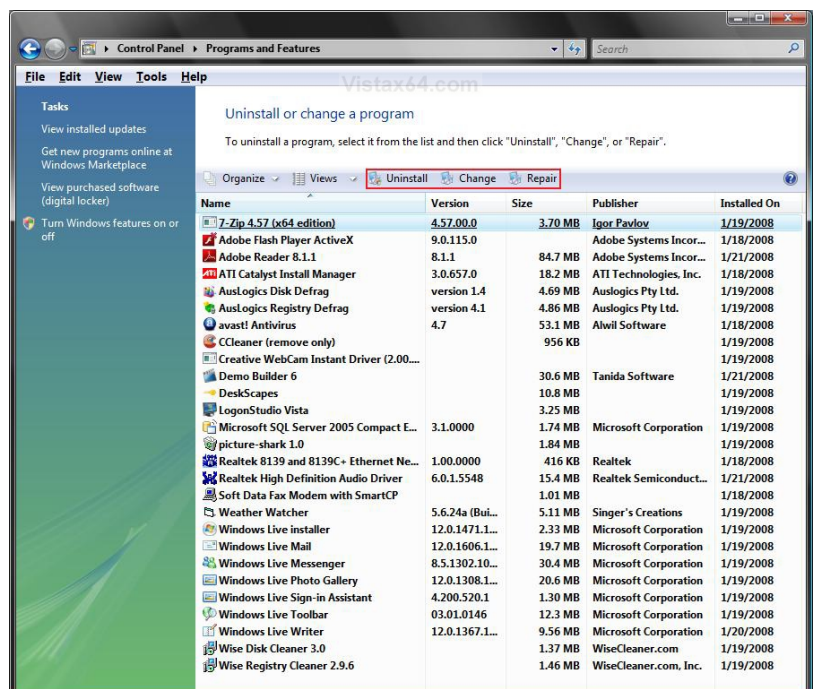
24 Google Chrome includes a secured version of Adobe Flash inside of all of its updates.

## !Do This box!

Any time you have an opportunity to update software you should do it. If you are asked to 'update now' or 'update later', always update as soon as possible, don't put it off! If you have the option to enable automatic updates, turn them on. If you are on mobile broadband and pay for Internet usage per/MB or per/GB, find a time to connect to the Internet from an unlimited source such as a university, library, office, or cafe, and begin updates. Turn on automatic updates for your operating system, update your browser and all software you use on a regular basis. Update manager applications can also help manage updates and ensure you can install available updates for your applications.

## Safe Software Practices

Since software unfortunately becomes vulnerable and needs to be updated all the time, one of the simplest ways to keep secure is to avoid installing unnecessary programs. Adobe Flash and Oracle Java are two programs which are often found to have critical flaws. You may not need either of these programs on your computer at all.<sup>24</sup> Go to your list of installed programs (In Windows: Add/Remove Programs or Uninstall or change a program) and review what is installed. Are there programs you do not recognise the name of? Some of these may be important for the functioning of your computer but if something looks suspicious you, should research what it is and decide if you can remove it. Particularly be suspicious of installed software which does not have a publisher listed in the Publisher Column. Also look out for helper browser toolbars which were installed without your knowledge.



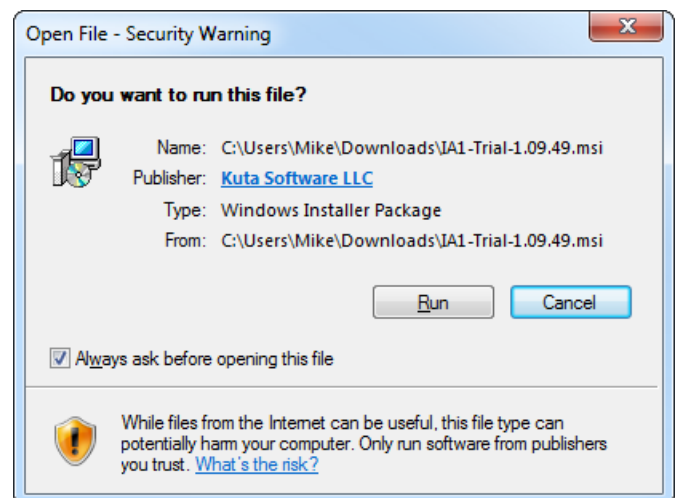
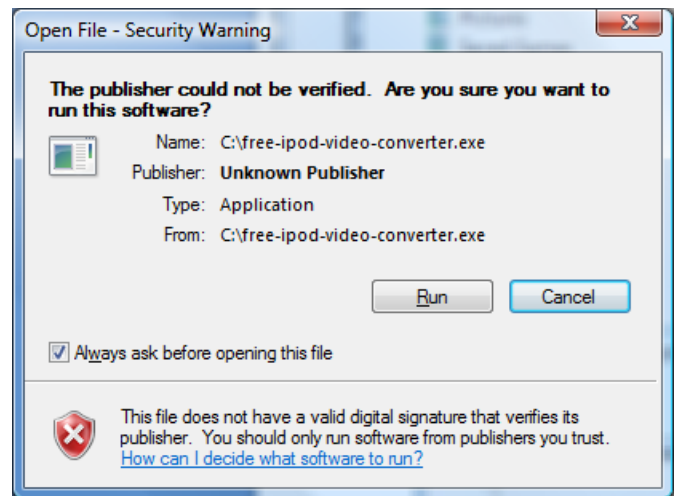
After reviewing software installed on your computer, open your browsers and look for the Extensions or Plug-ins page and similarly review extensions that you have installed. As with other software, less is more and you should keep the number of installed extensions down to a minimum of trusted and reputable extensions. Browser extensions are sensitive because they may be able to read and change information appearing on your browser and being typed in such as passwords, banking information, and social media shares.

## Safe Sources

Software should be obtained directly from the publisher of the software as much as possible. For instance, it is better to download Adobe Reader from <https://get.adobe.com/reader/> rather than from [www.download.com](http://www.download.com) or any other source. Likewise, you should avoid installing software from friends' flash drives or from EXE files sent to you by email or instant messaging. Software may be changed or may be completely bogus and will instead infect your computer.

Free download sites often bundle software downloads with unwanted extra downloads which promise additional features however are not initially desired or needed and may be downright harmful for your computer. See a story online<sup>25</sup> about a test to install all 10 of the top Download.com downloads which led to a severely damaged computer!

Whenever you install software, check the publisher of the software. Most reputable publishers can sign their software, which indicates that it comes from them and has not been modified in transit. Compare the following two Windows warning screens to see the difference between signed and unsigned software:



Remember, most software you need can be obtained for free directly from the publisher's websites. If you see an offer to get something for free which you otherwise would have to pay for, it is probably too good to be true! Take some basic precautions and you will preserve the speed, stability and security of your computer for the long-term.

25 <http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download-com-apps/>

# SECURITY OF DATA ON DEVICES

Daud works for an NGO. A few weeks ago, they experienced a break-in at their offices, where desktops, laptops, cameras, and mobile phones were stolen. The organisation's contracts, financial documents, contacts, research files, publications were all stolen. Backups had not been made of any of the computers in the office. Daud's management is concerned about motives of the thieves and worried that the confidential information they held may fall into the wrong hands.

---

Losing data is painful for any individual or organisation because it hurts you on two counts: on the one hand, you yourself lose vital information needed for your work, and on the other hand somebody else now has your information in their possession without authorisation.

**Daud should combat this risk on multiple levels. Encryption is a process of scrambling data so that only the person with the correct password can read the original data. Make backups regularly both on physical and online destinations.**

## What is Encryption?

Encryption is a way of scrambling data so that only authorised parties can understand the information.

Today, we have computers that can perform encryption for us. Digital encryption technology has expanded beyond simple secret messages; for example, encryption can be used for more elaborate purposes, such as to protect documents, verify the author of messages, or to browse the Web anonymously.

## Keeping your Data Safe with Encryption

Many of us carry our communications, information about our contacts, and sensitive working documents on laptops, removable storage devices, and even mobile phones. That data can include confidential information about your work, community, networks, and human rights monitoring. A physical device can be stolen or copied in seconds.

Computers and mobile phones can be locked by passwords, PINs or gestures, but these locks do not help protect data if the device itself is seized. It is relatively simple to bypass these locks because your data is stored in an easily readable form within the device.

By using encryption, you can make it harder for those who steal data to unlock its secrets. If you use encryption, your adversary needs not just your device, but also your password to unscramble/unlock the encrypted data—there is no shortcut. There are various applications of encryption: full-device encryption, file or folder encryption, and communication encryption (which will be discussed in the next chapter).



It is safest and easiest to encrypt all your data, not just a few folders. Most computers and smartphones offer complete, full-device (or full-disk) encryption as an option. Full device encryption ensures that contents of a computer or phone storage cannot be accessed by unauthorised people. Full device encryption will scramble all information written to the device and will need a password to unscramble the information before the device can be usable.

Android phones offer this under its Security settings, and Apple mobile devices such as the iPhone and iPad describe it as Data Protection and turn it on automatically if you set a passcode. On computer running Windows Professional it is known as BitLocker. On Macs it is called FileVault. On Linux distributions, full-disk encryption is usually offered when you first set up your system through a system called LUKS. Independent softwares like VeraCrypt and Disk Cryptor can also help you achieve the same goals.

Full disk encryption systems can also be used to encrypt portable media like external hard disks and flash drives by using BitLocker to Go (Windows), Filevault (Mac) or VeraCrypt (Windows, Mac, and Linux).

One potential weakness of full-device encryption is that it is a single point of vulnerability: in case you are forced to unlock a device, all your files will be vulnerable. A more robust solution is to combine full-device encryption with file and folder encryption to sequester your most vulnerable documents from anyone who does gain access to your main device accounts.

File and folder encryption solutions which allow you to encrypt single files or sections of your computer. An excellent cross-platform (working on Windows, Mac, and Linux computers) option is VeraCrypt. VeraCrypt allows you to create a secret volume for your files which functions like a virtual USB flash drive but which in fact exists inside an encrypted single file on your computer. Another, very easy to use, option is Ax crypt, a Windows-only software which adds file encryption to the right-click menu on your computer, allowing you to encrypt individual files easily at will.

See the following resource box for links to learn more about these options.

Remember though that encryption is only as good as your password. Don't write your password down on a post-it note attached to your monitor or keep a list of passwords in your notebook. If your attacker has your device, they could try out many different passwords until they guess your password. Cracking software can try millions of passwords a second. That means that a four number pin is unlikely to protect your data for very long at all, and even a long password may merely slow down your attacker. A really strong password under these conditions should be over fifteen characters long. See the Account Security chapter for more information on creating strong passwords.

## Encryption Software and Guides

### Computer Encryption

**BitLocker (Windows)** - Available on Professional Versions of Windows 7 & 8, and on most versions of Windows 8.<sup>26</sup> and above. Learn more from Microsoft including a step-by-step guide on its usage. An easier to use guide is available at HowToGeek1 plus, another at Windows Central specifically for Windows 10<sup>27</sup>. Note that BitLocker by default requires a device called a TPM which often is only available in higher-end business computers. Both guides linked here include directions on how to activate BitLocker in computers without a TPM.

**FileVault (Mac)** - Full-device encryption is easy to set up on most Mac computers. Follow Apple's instructions to activate FileVault from your System Preferences.<sup>28</sup>

**Disk Cryptor<sup>29</sup> (Windows)** - Read the guide from the Electronic Frontier Foundation on the Disk Cryptor full-device encryption software for Windows.<sup>30</sup>

**VeraCrypt<sup>31</sup> (Windows, Mac, Linux)** - Software which can encrypt sections of your drive or entire drive partitions and removable drives. Security In a Box has an excellent guide.<sup>32</sup>

26 <http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/>

27 <http://www.windowscentral.com/how-use-bitlocker-encryption-windows-10>

28 <https://support.apple.com/en-us/HT204837>

29 <https://diskcryptor.net/>

30 <https://ssd.eff.org/en/module/how-encrypt-your-windows-device>

31 <https://veracrypt.fr/en/Home.html>

32 <https://securityinabox.org/en/guide/veracrypt/windows>

## Phone Encryption

**Android Phone Encryption** - Read the guide from HowToGeek.<sup>33</sup>

**iPhone and iPad Encryption** - Simply activating a passcode lock on your device will enable device encryption. Learn more at the Electronic Frontier Foundation guide.<sup>34</sup>

## External Drives

**BitLocker To Go (Windows)** - Encrypt external hard drives and flash drives with BitLocker to Go.<sup>35</sup>

**Filevault (Mac)** - Encrypt external hard drives and flash drives by right-clicking the removable device in the Finder and choosing Encrypt... then choosing a password. See the guide from Apple.<sup>36</sup>

Note that the above external drive solutions will limit the encrypted drives to be used with only Macs or Windows computers. VeraCrypt alternatively offers a cross-platform external drive encryption solution.

## BACKING UP YOUR DATA

Information security also means having access to your data when you need it. What are the threats to the availability of your information? Theft of your computers from public and private places is a common risk, however things like viruses, computer crashes, fire, water damage, or hard disk failure can lead to data loss too. To address this risk, you must regularly maintain backups of your files.

Backups are traditionally done onto external hard drives, USB drives, and removable disks like CDs and DVDs. These storage media are vulnerable to theft and unwanted access, so you should also encrypt your backups. See the resource list in the previous section to learn how to encrypt external storage drives.

Making backups can be as simple as copy and pasting your working folders onto an external drive. However, many applications are available to assist with making backups. Windows has two built-in backup options (not available in all versions): Backup & Restore<sup>37</sup> will take a full system backup from which you can recover in case of data loss, furthermore you can schedule updates to that full backup; and File History<sup>38</sup> which will retain versions of documents as they change over time. You can use either of these systems or even at the same time. Mac OS X also has a built-in backup system called Time Machine<sup>39</sup> which provides incremental backups to an external hard drive, which can optionally be encrypted by activating the encryption option during setup.

It is valuable to have both a local and a remote 'cloud' backup of your files. You could use popular free cloud backup programs like **DropBox**, **Google Drive**, **Copy**, and **OneDrive**. If you are conscious of the privacy of your backups from being accessed by the cloud provider (such as Google, Microsoft, and Dropbox) you should look at backup programs that encrypt your files on your computer before they get uploaded to the cloud provider: see Mega, Sync.com, SpiderOak, and Wuala. There is even software which will encrypt your file locally then pass the resulting encrypted files into Dropbox and other Cloud backup providers: see BoxCryptor,<sup>40</sup> Duplicati,<sup>41</sup> and Viivo.<sup>42</sup>

33 <http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/>

34 <https://ssd.eff.org/en/module/how-encrypt-your-iphone>

35 <https://technet.microsoft.com/en-us/magazine/ff404223.aspx>

36 <https://www.uvm.edu/it/kb/article/encrypt-external-drive/>

37 <https://support.microsoft.com/en-us/help/17127/windows-back-up-restore>

38 <https://support.microsoft.com/en-us/help/17128/windows-8-file-history>

39 Time Machine <https://support.apple.com/en-us/HT201250>

40 <https://www.boxcryptor.com/>

41 [www.duplicati.com](http://www.duplicati.com)



# SECURITY OF DATA MOVING THROUGH NETWORKS

..... Geraldina is an environmental human rights defender. She was planning a sensitization meeting with all the people in her area to inform them about a planned government move to give a forest to foreign investors. She wrote an email to all the local leaders, telling them to inform all the people about the date and venue of the meeting. A few days to the meeting, she was shocked to learn that none of the local leaders received her email.

A few days later, she was visited by police who warned her against inciting the public and sabotaging government programs. She was left wondering what happened to her email and how the police got her communication instead of the intended recipients.

What happened to Geraldina is called Surveillance. It is where someone is able to monitor your communications because they are communicated in plain text over the Internet.

Geraldina can use encryption like HTTPS, GPG and VPNs to keep her communications secret and confidential so that they cannot be used to intimidate her as she does her work.

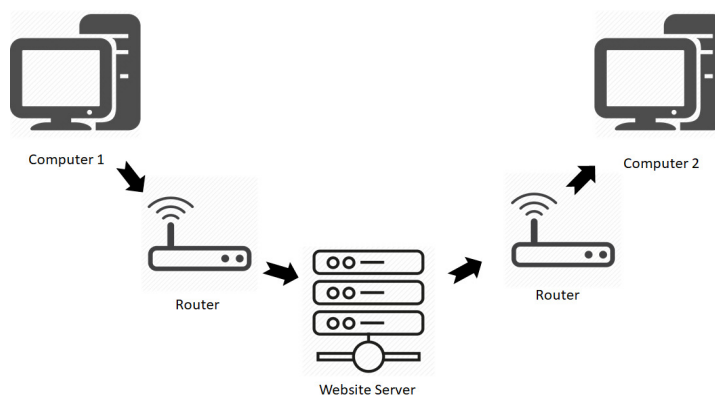
## How the Internet Works

The Internet is a network of networks that provides information exchange between client computer and servers. Client computers are the devices that you use such as your laptop, desktop PC, mobile smart phone; they request for information or services hosted or stored on server computers. The client and server computer use a variety of protocols (like a shared language both sides understand) such as Hypertext Transfer Protocol (HTTP) for the requests and responses between them. All information communicated over the HTTP protocol moves across the Internet as plain text: anyone who has a privileged position in the network (such as an Internet Service Provider, the administrator of a cyber cafe, or any one of hundreds of thousands of internet exchange points could record your communications.

A simple illustration of how the Internet works would be someone accessing a news website to read news.

As you can see, there are many other computers involved in connecting the user with the server they need. Over insecure protocols, those other computers could also read and even change the contents of the user's communication.

Fortunately, there are more secure protocols available to help secure our data and communications as it moves across the Internet. However, we must understand what they are, and which tools utilise them.



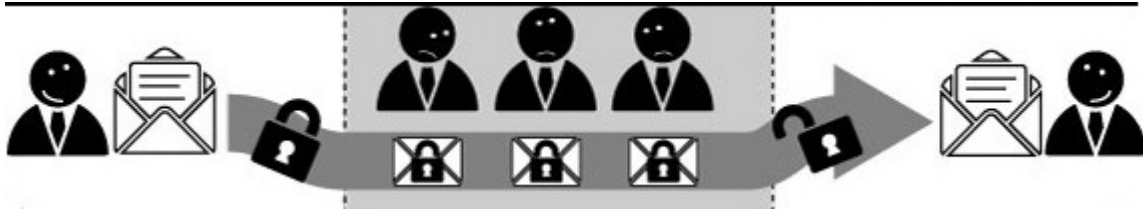
## Communicating with Others

Telecommunication networks and the Internet have made communicating with people easier than ever but have also made surveillance more prevalent than it has ever been in human history. Without taking extra steps to protect your privacy, every phone call, text message, email, instant message, voice over IP (VoIP) call, video chat and social media message may be vulnerable to eavesdroppers.

Often the safest way to communicate with others is in person, without computers or phones being involved at all. Because this is not always possible, the next best thing is to use end-to-end encryption while communicating over a network if you need to protect the content of your communications.



## How Does End-to-End Encryption Work?



When two people want to communicate securely (for example, Kamau and Abuya) they must each generate cryptographic keys. Before Kamau sends a message to Abuya he encrypts it to Abuya's key so that only Abuya can decrypt it. Then she sends the already-encrypted message across the Internet. If anyone is eavesdropping on Kamau and Abuya—even if they have access to the service that Kamau is using to send this message (such as her email account)—they will only see the encrypted data and will be unable to read the message. When Abuya receives it, she must use his key to decrypt it into a readable message. This is how end-to-end encryption works.

End-to-end encryption involves some effort, but it is the only way that users can verify the security of their communications without having to trust the platform that they are both using. Some services, such as Skype, have [claimed](#)<sup>43</sup> to offer end-to-end encryption when it appears that they actually do not. For end-to-end encryption to be secure, users must be able to verify that the crypto key they are encrypting messages to belongs to the people they believe they do. If communications software does not have this ability built-in, then any encryption that it might be using can be intercepted by the service provider itself, for instance if a government compels it to.

### Voice Calls

When you make a call from a landline or a mobile phone, your call is not end-to-end encrypted. If you are using a mobile phone, your call may be (weakly) encrypted between your handset and the cell phone towers. However, as your conversation travels through the phone network, it is vulnerable to interception by your phone company and, by extension, any governments or organizations that have power over your phone company. The easiest way to ensure you have end-to-end encryption on voice conversations is to use VoIP instead.

Beware! Most popular VoIP (Voice over Internet Protocol) providers, such as Skype and Google for Google Meet, offer transport encryption so that eavesdroppers cannot listen in, but the providers themselves are still potentially able to listen in. Depending on your threat model, this may or may not be a problem.

Some services/tools that offer end-to-end encrypted VoIP calls include:

- Wire<sup>44</sup>
- Silent Phone<sup>45</sup>
- Signal<sup>46</sup>

In order to have end-to-end encrypted VoIP conversations, both parties must be using the same (or compatible) software.

### Text Messages & Instant Messaging

Standard text (SMS) messages do not offer end-to-end encryption. If you want to send encrypted messages on your phone, consider using encrypted instant messaging software instead of text messages. Currently the only way to send encrypted SMS messages is to use the [Silence](#)<sup>47</sup> app for Android, formerly SMS Secure.

Other secure messaging options work over the Internet. So, for instance, users of<sup>48</sup> Android and iOS can chat securely using [Signal](#).<sup>49</sup>

Off-the-Record (OTR) is an end-to-end encryption protocol for real-time text conversations that can be used on top of a variety of services.

43 <https://support.skype.com/en/faq/fa10983/what-are-p2p-communications>

44 <https://wire.coma/en/>

45 <https://www.silentcircle.com/services#mobile>

46 <https://ssd.eff.org/en/module/how-use-signal-ios><https://ssd.eff.org/en/module/how-use-signal-android>

47 <https://silence.im/>

48 <https://whispersystems.org/#privacy>

49 <https://ssd.eff.org/en/module/how-use-signal-ios><https://ssd.eff.org/en/module/how-use-signal-android>


Some tools that incorporate OTR with instant messaging include:

Pidgin<sup>50</sup> (Linux)

- Adium<sup>51</sup> (For OS X)
- ChatSecure<sup>52</sup> (Android)
- Jitsi<sup>53</sup> (For Windows, Linux, and OS X)
- Jitsi Meet<sup>54</sup> (For secure video conferencing in your Web Browser)

## Email

Most email providers give you a way of accessing your email using a web browser, such as Firefox, Microsoft Edge, Chrome, etc. Of these providers, most of them provide support for HTTPS, or transport-layer encryption. You can tell that your email provider supports HTTPS if you log-into your webmail and the URL at the top of your browser begins with the letters HTTPS instead of HTTP

 <https://mail.google.com/mail/u/0/#inbox>

If your email provider supports HTTPS, but does not do so by default, try replacing HTTP with HTTPS in the URL and refresh the page. If you'd like to make sure that you are always using HTTPS on sites where it is available, download the [HTTPS Everywhere](https://www.eff.org/https-everywhere)<sup>55</sup> browser add-on for Firefox or Chrome.

Some webmail providers that use HTTPS by default include:

- Gmail
- Riseup
- Yahoo

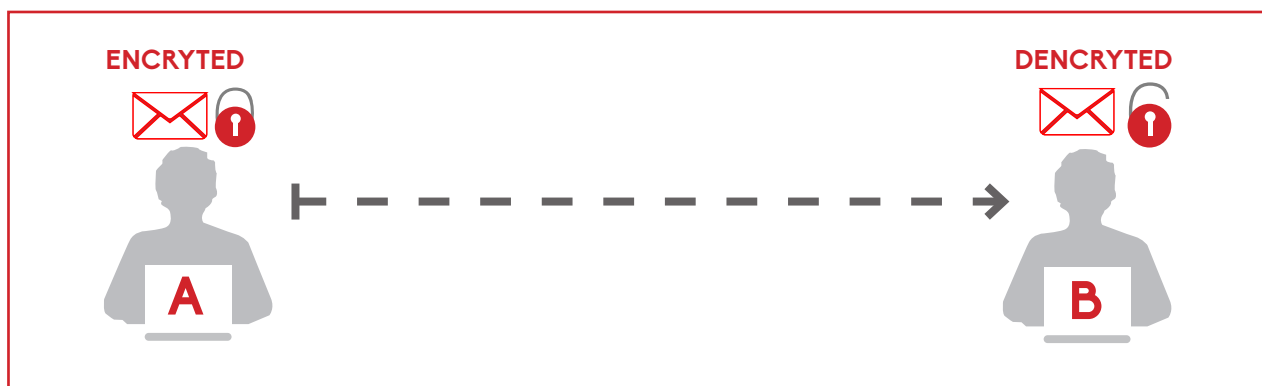
Some webmail providers give you the option of choosing to use HTTPS by default by selecting it in your settings. The most popular service that still does this is Hotmail.

## What does transport-layer encryption do and why might you need it?

HTTPS, also referred to as SSL or TLS, encrypts your communications so that it cannot be read by other people on your network. This can include the other people using the same Wi-Fi in an airport or at a café, the other people at your office or school, the administrators at your ISP, malicious hackers, governments, or law enforcement officials. Communications sent over your web browser, including the web pages that you visit and the content of your emails, blog posts and messages, using HTTP rather than HTTPS are trivial for an attacker to intercept and read.

Malicious state and non-state actors are increasingly becoming adept at hijacking HTTPS sessions between the computer and the server. In this way, they can present the browser with a fake SSL certificate of your intended server and if you ignore browser warnings then the whole session and information exchanges between your computer and the server will be compromised.

In such circumstances it very important NOT to proceed with the connection unless it is a local self-signed certificate. It is usually advisable to wait for a while and try to access the site again later if you are presented with the warning shown in the image above.



50 <https://ssd.eff.org/en/module/how-use-otr-linux>

51 <https://ssd.eff.org/en/module/how-use-otr-mac>

52 <https://guardianproject.info/howto/chatsecurely/>

53 <https://jitsi.org/>

54

55 <https://www.eff.org/https-everywhere>

## Advanced Email Security (GPG/PGP)

But there are some things that HTTPS does not do. When you send email using HTTPS, your email provider still gets an unencrypted copy of your communication. Governments and law enforcement may be able to access this data with a warrant. In the United States for example, most email providers have a policy that says they will tell you when they have received a government request for your user data as long as they are legally allowed to do so, but these policies are strictly voluntary, and in many cases, providers are legally prevented from informing their users of requests for data. Some email providers, such as Google<sup>56</sup>, Yahoo<sup>57</sup>, and Microsoft<sup>58</sup>, publish transparency reports, detailing the number of government requests for user data they receive, which countries make the requests, and how often the company has complied by turning over data.

If your threat model includes a government or law enforcement, or you have some other reason for wanting to make sure that your email provider is not able to turn over the contents of your email communications to a third party, you may want to consider using end-to-end encryption for your email communications.

PGP (or Pretty Good Privacy) is the standard for end-to-end encryption of your email. Used correctly, it offers very strong protections for your communications. PGP is also referred to as GPG (Gnu Privacy Guard). In PGP, each party creates a key in two parts: a private part and a public part. You guard the private part securely on your own devices, but you distribute the public part to any one you would like to communicate with using PGP. To help illustrate the concepts of PGP, Tactical Technology Collective has a series of explanatory videos called [Decrypting Encryption](#).<sup>59</sup>

[Resource Box]

For detailed instructions on how to install and use PGP/GPG encryption for your email using the mail clients on your computer, see these guides for [Mac OS X](#), [Windows](#),<sup>60</sup> and [Linux](#).<sup>61</sup>

To use PGP/GPG in your web browser using webmail, look at using the [Mailvelope](#)<sup>62</sup> browser plugin or watch out for the fully featured webmail clients like [ProtonMail](#).<sup>63</sup>

[/Resource Box]

56 <https://www.google.com/transparencyreport/>

57 <https://transparency.yahoo.com/>

58 <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

59 <https://tacticaltech.org/projects/decrypting-encryption>

60 <https://ssd.eff.org/en/module/how-use-gpg-mac-os-x>

61 <https://ssd.eff.org/en/module/how-use-gpg-linux>

62 <https://www.mailvelope.com/>

63 <https://protonmail.com/>

64 <http://www.zeit.de/datenschutz/malte-spitz-data-retention>

65 [http://www.ted.com/talks/malte\\_spitz\\_your\\_phone\\_company\\_is\\_watching?language=en](http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=en)

Make sure you have encryption enabled on your email client before you communicate a sensitive information or attachment to your recipient. To do so, follow how to enable PGP encryption on your email clients from the link: <https://ssd.eff.org/en/module-categories/tool-guides>

## What End-To-End Encryption Does Not Do!!!

End-to-end encryption only protects the content of your communication, not the fact of the communication itself. It does not protect your metadata—which is everything else, including the subject line of your email, or who you are communicating with and when.

Metadata can provide extremely revealing information about you even when the content of your communication remains secret.

Metadata about your phone calls can give away some very intimate and sensitive information. For example:

- They know you rang a depression counselling service at 2:24 am and spoke for 18 minutes, but they don't know what you talked about.
- They know you called a local radio station during an hour of discussion on political topics, but the exact contents of the call remain a secret.
- They know you spoke with a free HIV information centre, then your doctor, then your health insurance company in the same hour, but they don't know what was discussed.
- They know you received a call from the local opposition headquarters office while it was having a campaign against media legislation, and then called your boss immediately after, but the content of those calls remains safe from government intrusion.
- They know you called a gynaecologist, spoke for a half hour, and then called the local family planning number later that day, but nobody knows what you spoke about.

If you are calling from a cell phone, information about your location is metadata. For example, in 2009, German Green Party politician Malte Spitz sued Deutsche Telekom to force them to hand over six months of Spitz's phone data, which he made available to a German newspaper. The resulting [visualization](#)<sup>64</sup> showed a detailed history of Spitz's movements. Spitz gave an inspiring TED speech about this case which is [available online](#).<sup>65</sup>

# How to: circumvent online censorship



Many governments, companies, schools and public access points use software to prevent Internet users from accessing certain websites and Internet services. This is called Internet filtering or blocking and is a form of censorship. Content filtering comes in different forms. Sometimes entire websites are blocked, sometimes individual web pages and sometimes content is blocked based on keywords contained in it. One country might block Facebook entirely, or only block particular Facebook group pages, or it might block any page or web search with the word homosexuality in it.

Regardless of how content is filtered or blocked, you can almost always get the information you need by using a circumvention tool. Circumvention tools usually work by diverting your web or other traffic through another computer, so that it bypasses the machines conducting the censorship. An intermediary service through which you channel your communications in this process is called a proxy.

Circumvention tools do not necessarily provide additional security or anonymity, even those that promise privacy or security, even ones that have terms like anonymizer in their names.

There are different ways of circumventing Internet censorship, some of which provide additional layers of security. The tool that is most appropriate for you depends on your threat model.

## Basic Techniques

HTTPS is the secure version of the HTTP protocol used to access websites. Sometimes a censor will block the insecure version of a site only, allowing you to access that site simply by entering the version of the domain that starts with HTTPS. This is particularly useful if the filtering you're experiencing is based on keywords or only blocks individual web pages. HTTPS stops censors from reading your web traffic, so they cannot tell what keywords are being sent, or which individual web page you are visiting (censors can still see the domain names of all websites you visit).

If you suspect this type of simple blocking, try entering `https://` before the domain in place of `http://`.

Try the [HTTPS Everywhere](https://www.eff.org/https-everywhere)<sup>66</sup> plugin to automatically turn on HTTPS for those sites that support it.

Another way that you may be able to circumvent basic censorship techniques is by trying an alternate domain name or URL. For example, instead of visiting <http://twitter.com>,<sup>67</sup> you might visit <https://mobile.twitter.com>,<sup>68</sup> the mobile version of the site. Censors that block websites or web pages usually work from a blacklist of banned websites, so anything that is not on that blacklist will get through. They might not know of all the variations of a particular website's domain name—especially if the site knows it is blocked and registers more than one name.

66 <https://www.eff.org/https-everywhere>

67 <https://twitter.com/>

68 <https://mobile.twitter.com/home>



## Web-based Proxies

A web-based proxy (such as <http://proxy.org/><sup>69</sup>) is a good way of circumventing censorship. To use a web-based proxy, all you need to do is enter the filtered address that you wish to use; the proxy will then display the requested content.

Web-based proxies are a good way to quickly access blocked websites, but often do not provide any security and will be a poor choice if your threat model includes someone monitoring your Internet connection. Additionally, they will not help you to use other blocked non-webpage services such as your instant messaging program. Finally, web-based proxies themselves pose a privacy risk for many users, depending on their threat model, since the proxy will have a complete record of everything you do online.

## DNS Settings

Often governments will enforce censorship in their countries by instructing internet service providers to enact blacklists using something called Domain Name Service (DNS). DNS servers are part of the infrastructure which helps your browser identify the actual web location of web addresses you know. For instance, when you type in [www.bbc.co.uk](http://www.bbc.co.uk), a DNS server is what informs your browser that BBC is located on a server at IP address 212.58.244.20. By manipulating DNS servers your computer could be fooled into thinking that a website, such as the BBC, does not exist, or exists at a fake location.

To circumvent this type of blocking you can simply change the default DNS servers used by your computer. Google offers two [public servers](#)<sup>70</sup> at 8.8.8.8 and 8.8.4.4. [OpenDNS](#)<sup>71</sup> offers public servers at 208.67.222.222 and 208.67.220.220 which additionally block known malware and phishing sites.

You can even set these DNS settings on an office or communal router so that all users can benefit. Instructions on how to change DNS settings on various operating systems and routers can be found at <https://use.opendns.com>.

## Virtual Private Networks

A Virtual Private Network (VPN) encrypts and sends all Internet data between your computer and the VPN provider located in another country. Once a VPN service is correctly configured, you can use it to access web pages, e-mail, instant messaging, VoIP, and any other Internet service. A VPN protects your traffic from being intercepted locally, but your VPN provider can keep logs of your traffic (websites you access, and when you access them) or even provide a third party with the ability to snoop directly on your web browsing.

Some free VPNs to consider are Betternet,<sup>73</sup> Psiphon,<sup>74</sup> BitMask,<sup>75</sup> and Opera.<sup>76</sup>

For some recommendations about paid VPN services, click [here](#)<sup>77</sup>. Some VPNs with exemplary privacy policies could still be run by devious people.

## Tor

Tor is free and open-source software that is intended to provide you with anonymity, but which also allows you to circumvent censorship. When you use Tor, the information you transmit is safer because your traffic is bounced around a distributed network of servers, called onion routers. This could provide anonymity, since the computer with which you're communicating will never see your IP address, but instead will see the IP address of the last Tor router through which your traffic travelled.

When used with a couple of optional features (bridges and obfsproxy) Tor is the gold standard for secure censorship circumvention against a local state, since it will both bypass almost all national censorship, and if properly configured, protect your identity from an adversary listening in on your country's networks. It can be slow, however.

Learn how to use Tor using [this guide](#)<sup>78</sup> from the Tor Project documentation.

69 <http://proxy.org/>

70 <https://developers.google.com/speed/public-dns/?hl=en>

71 <https://use.opendns.com/>

72 <https://use.opendns.com/>

73 <https://www.betternet.co>

74 <https://www.psiphon3.com/>

75 <https://bitmask.net>

76 <https://www.opera.com/apps/vpn>

77 <https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/>

78 <https://2019.www.torproject.org/docs/documentation.html.en>

# ACCOUNT SECURITY

Seseko the executive director of a sexual minorities' organisation. Early one morning, she received an email on her phone telling her that her email would expire in four hours if she did not take action. At the end of that email, there was a link that offered to log her into her email to prevent it from being closed. Without much thought, she went through the motions and opened the link which brought her to a login page that looked exactly like the Gmail login page. She quickly entered her username and password but on submitting, nothing really happened. She went back and continued reading her other emails.

Later in the day, she got reports that the organisation website had been hacked and defaced and was not accessible anymore. This is when she was informed by the head of the organization ICT department that he had received an email from her requesting temporary access to the website backend early that morning.

What Seseko experienced that morning was a targeted password stealing phishing attack. Once the attackers got hold of her email account, they could easily compromise any part of the organisation.

**There is a very simple but powerful solution that Seseko can use to avoid that kind of attack from happening again. It is called two factor Authentication. It also helps to have strong and different passwords for each online account.**

## Creating Strong Passwords

Because remembering many different passwords is difficult, people find it hard to work with passwords effectively and efficiently. As users become overwhelmed with the requirement of creating a new password for everything, the temptation is to reuse the same password on multiple accounts, services and sites.

The practice is exceptionally bad because it can lead to compromise of all accounts on which the same password is used. That means a given password may be only as secure as the least secure service where it has been used.

Avoiding password reuse is a valuable security precaution, but you will not be able to remember all your passwords if each one is different. Fortunately, there are software tools to help with this—a [password manager](#) (also called a password safe) is a software application that helps store many passwords safely. This makes it practical to avoid using the same password in multiple contexts. The password manager protects all your passwords with a single master password (or, ideally a passphrase—see discussion below) so you only have to remember one thing. The password manager can handle the entire process of creating and remembering the passwords for the user.



For example, [KeePassXC](#) is an open source free password safe that you keep on your desktop. It is important to note that if you are using KeePassXC, it will not automatically save changes and additions. This means that if it crashes after you have added some passwords, you can lose them forever. You can change this in the settings.

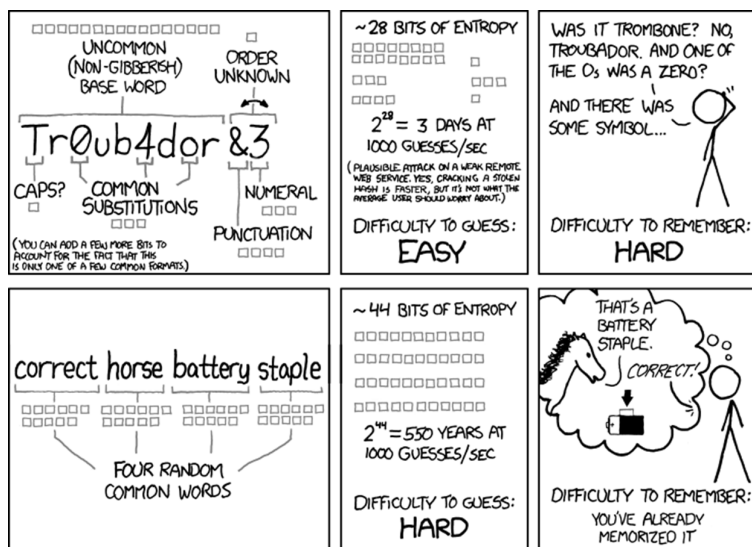
Using a password manager also helps you choose strong passwords that are hard for an attacker to guess. This is important too. Too often computer users choose short, simple passwords that an attacker can easily guess, including password1, 12345, a birthdate, or a friend's, spouse's, or pet's name. A password manager can help you create and use a random password without pattern or structure—one that will not be guessable. For example, a password manager is able to choose passwords like vAeJZ!Q3p\$Kdkz/CRHzj0v7, which a human being would be unlikely to remember—or guess. Do not worry; the password manager can remember these for you!

## Choosing Strong Passwords

There are a few passwords that do need to be memorised and that need to be particularly strong: those that ultimately lock your own data with cryptography. That includes, at least, passwords for your device, encryption like full-disk encryption, and the master password for your password manager.

Computers are now fast enough to quickly guess passwords shorter than ten or so characters. That means short passwords of any kind, even totally random ones like nQ\m=8'x or !s7e&nUY or gaG5'bG, are not strong enough for use with encryption today.

There are several ways to create a strong and memorable passphrase; the most straightforward and sure-fire method is Arnold Reinhold's [Diceware](#)<sup>79</sup>.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Source: [XKCD](#)<sup>80</sup>

Reinhold's method involves rolling physical dice to randomly choose several words from a word list; together, these words will form your passphrase. For disk encryption (and password safe), we recommend selecting a minimum of six words. A simplified version of Diceware involves simply stringing together a variety of random words yourself. See this comic for an illustration of how this method may be easier to use and more secure than complex passwords like nQ\m=8'x

When you use a password manager, the security of your passwords and your master password is only as strong as the security of the computer where the password manager is installed and used. If your computer or device is compromised and spyware is installed, the spyware can watch you type your master password and could steal the contents of the password safe. So, it is still very important to keep your computer and other devices clean of malicious software when using a password manager.

<sup>79</sup> <http://world.std.com/~reinhold/diceware.html>

<sup>80</sup> <https://xkcd.com/936/>

## Multi-factor Authentication and One-time Passwords

Many services and software tools let you use two-factor authentication, also called two-step verification or two-step login. Here the idea is that to log in, you need to be in possession of a certain physical object: usually a mobile phone, but, in some versions, a special device called a security token. Using this system ensures that even if your password for the service is hacked or stolen, the thief will not be able to log in unless they also have possession or control of a second device and the special codes that only it can create.

Typically, this means that a thief or hacker would have to control both your laptop and your phone before they have full access to your accounts.

Because this can only be set up with the cooperation of the service operator, there is no way to do this by yourself if you are using a service that does not offer it.

Two-factor authentication using a mobile phone can be done in two ways: the service can send you an SMS text message to your phone whenever you try to log in (providing an extra security code that you need to type in), or your phone can run an authenticator application that generates security codes from inside the phone itself. This will help protect your account in situations where an attacker has your password but does not have physical access to your mobile phone.

Many online services now offer two-factor authentication. An updated list of these services is available at <https://www.turnon2fa.com>. You can get started with your Google<sup>81</sup>, Yahoo<sup>82</sup>, Facebook<sup>83</sup>, and Twitter<sup>84</sup> accounts!

Some services, such as Google, also allow you to generate a list of one-time passwords, also called single-use passwords. These are meant to be printed or written down on paper and carried with you (although in some cases it might be possible to memorise a small number of them). Each of these passwords works only once, so if one is stolen by spyware when you enter it, the thief will not be able to use it for anything in the future.

## Threats of Physical Harm or Imprisonment

Finally, understand that there is always one way that attackers can obtain your password: They can directly threaten you with physical harm or detention. If you fear this may be a possibility, consider ways in which you can hide the existence of the data or device you are password-protecting, rather than trust that you will never hand over the password. One possibility is to maintain at least one account that contains largely unimportant information, whose password you can divulge quickly.

If you have good reason to believe that someone may threaten you for your passwords, it is good to make sure your devices are configured so that it will not be obvious that the account you are revealing is not the real one. Is your real account shown in your computer's login screen, or automatically displayed when you open a browser? If so, you may need to reconfigure things to make your account less obvious.

Please note that intentional destruction of evidence or obstruction of an investigation can be charged as a separate crime, often with dire consequences. In some cases, this can be easier for the government to prove and allow for more substantial punishments than the alleged crime originally being investigated.

81 <https://www.google.com/landing/2step/>

82 <https://login.yahoo.com/account>

83 <https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920>

84 <https://blog.twitter.com/2013/getting-started-with-login-verification>

# MOBILE SECURITY

Fayed is an activist working on transparency, accountability and freedom of expression. He has many friends who have run out of his country due to oppression from government. He regularly calls and texts his activist friends in the diaspora to update them on the situation in the country and to have them share stories he cannot share inside the country.

One morning, police rounded him off from his home and took him to court accusing him of planning to overthrow the government and communicating with terrorists. In the courts the prosecution presented as evidence recordings of his regular voice calls to his friends in the diaspora and text messages he has written to them talking ill about the government.

Fayed should have known that voice calls and regular SMS cannot be used to communicate sensitive information because they are easily recorded by phone companies. Fayed should learn about these vulnerabilities and about the mobile phone applications that can be used to encrypt voice calls and text messages.

## The Problem with Mobile Phones

Mobile phones have become ubiquitous and basic communications tools—now used not only for phone calls, but also for accessing the Internet, sending text messages, and documenting the world.

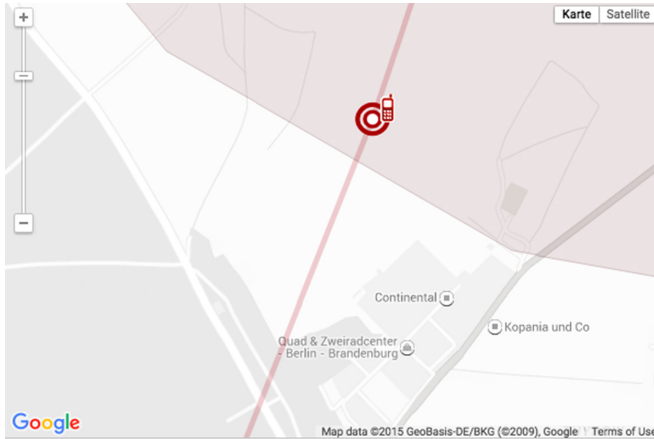
Unfortunately, mobile phones were not designed for privacy and security. Not only do they do a poor job of protecting your communications, but they also expose you to new kinds of surveillance risks. Most mobile phones give the user much less control than a personal desktop or laptop computer would; it is harder to replace the operating system, harder to investigate malware attacks, harder to remove or replace undesirable bundled software, and harder to prevent parties like the mobile operator from monitoring how you use the device.

Some of these problems can be addressed by using third-party privacy software—but some of them cannot. Here, we will describe some of the ways that phones can aid surveillance and undermine their users privacy.

## Location Tracking

One of the deepest privacy threats from mobile phones—yet one that is often completely invisible—is the way that they announce your whereabouts all day (and all night) long through the signals they broadcast. There are various ways that an individual phone's location can be tracked by others.

## Mobile Signal Tracking



A network operator can do this is to observe the signal strength that different towers observe from a particular subscriber's mobile phone, and then calculate where that phone must be located in order to account for these observations. There is no way to hide from this kind of tracking if your mobile phone is powered on and transmitting signals to an operator's network. The unequal relationship between government and telecom operators means that government could force the operator to turn over location data about a user (in real-time or as a matter of historical record). In 2010, a German privacy advocate named Malte Spitz used privacy laws to get his mobile operator to turn over the records that it had about him; he chose to publish them as an educational resource so that other people could understand how mobile operators can monitor users this way. (You can visit [here](#)<sup>85</sup> to see what the operator knew about him.) The possibility of government access to this sort of data is not theoretical: it is already being widely used by law enforcement around the world.

Data obtained by Malte Spitz from his telephone company showing his movements and phone call data. Explore 6 months of this data at Zeit Online<sup>86</sup>.

Another related kind of government request is called a tower dump; in this case, a government asks a mobile operator for a list of all the mobile devices that were present in a certain area at a certain time. This could be used to investigate a crime, or to find out who was present at a particular protest. (Reportedly, the Ukrainian government used a tower dump for this purpose in 2014, to make a list of all the people whose mobile phones were present at an anti-government protest.)

There are also devices used by law enforcement or other technically sophisticated organisations which can collect location directly called IMSI catchers (a portable fake cell phone tower that pretends to be a real one and thereby catch particular users' mobile phones, detect their presence, and intercept their communications. IMSI catchers are physical devices which need to be brought to a particular location to monitor the area. There is currently no reliable defence against all IMSI catchers though some apps detect their presence in some cases. In some cases, disabling 2G connections and roaming can protect against connecting to IMSI catchers.

## Location Information Leaks from Apps and Web Browsing

Modern smartphones provide ways for the phone to determine its own location, often using GPS and sometimes using other services provided by location companies (which usually ask the company to guess the phone's location based on a list of cell phone towers and/or Wi-Fi networks that the phone can see from where it is). Apps can ask the phone for this location information and use it to provide services that are based on location, such as maps that show you your position on the map.

Some of these apps will then transmit your location over the network to a service provider, which, in turn, provides a way for other people to track you. (The app developers might not have been motivated by the desire to track users, but they might still end up with the ability to do that, and they might end up revealing location information about their users to governments or hackers.) Some smartphones will give you control over whether apps can find out your physical location; a good privacy practice is to try to restrict which apps can see this information, and at a minimum to make sure that your location is only shared with apps that you trust and that have a good reason to know where you are.

85 <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>

86 <http://www.zeit.de/datenschutz/malte-spitz-data-retention>

In each case, location tracking is not only about finding where someone is right now, like in an exciting movie chase scene where agents are pursuing someone through the streets. It can also be about answering questions about people's historical activities and about their beliefs, participation in events, and personal relationships. For example, location tracking could be used to try to find out whether certain people are in a romantic relationship, to find out who attended a particular meeting or who was at a particular protest, or to try and identify a journalist's confidential source.

## Turning Phones off

There is a widespread concern that phones can be used to monitor people even when not actively being used to make a call. As a result, people having a sensitive conversation are sometimes told to turn their phones off entirely, or even to remove the batteries from their phones.

The recommendation to remove the battery seems to be focused mainly on the existence of malware that makes the phone appear to turn off upon request (finally showing only a blank screen), while really remaining powered on and able to monitor conversations or invisibly place or receive a call. Thus, users could be tricked into thinking they had successfully turned off their phones when they actually had not. Such malware does exist, at least for some devices, though we have little information about how well it works or how widely it has been used.

Turning phones off has its own potential disadvantage: if many people at one location all do it at the same time, it is a sign to the mobile carriers that they all thought something merited turning their phones off. (That something might be the start of a film in a movie theatre, or the departure of a plane at an airport, but it might also be a sensitive meeting or conversation.) An alternative that might give less information away is to leave everybody's phone in another room where the phones' microphones would not be able to overhear the conversations.



## Spying on Mobile Communications

Mobile phone networks were not originally designed to use technical means to protect subscriber's calls against eavesdropping. That meant that anybody with the right kind of radio receiver could listen in on the calls.

The situation is somewhat better today, but sometimes only slightly. Encryption technologies have been added to mobile communications standards to try to prevent eavesdropping. But many of these technologies have been [poorly designed](#)<sup>87</sup> (sometimes deliberately, due to government pressure not to use strong encryption!). They have been unevenly deployed, so they might be available on one carrier but not another, or in one country but not another, and have sometimes been implemented incorrectly. For example, in some countries carriers do not enable encryption at all, or they use obsolete technical standards. This means it is often still possible for someone with the right kind of radio receiver to intercept calls and text messages as they are transmitted over the air.

Even when the best industry standards are being used—as they are in some countries and on some mobile carriers—there are still people who can listen in. At a minimum, the mobile operators themselves can intercept and record all of the data about who called or texted whom, when, and what they said. This information might be available to local or foreign governments through official or informal arrangements. In some cases, foreign governments have also hacked mobile operators' systems in order to get secret access to users' data.

87 <http://www.aftenposten.no/verden/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-98459b.html>

The safest practice is to assume that traditional calls and SMS text messages have not been secured against eavesdropping or recording. Even though the technical details vary significantly from place to place and system to system, the technical protections are often weak and can be bypassed in many situations.

The situation can be different when you are using secure communications apps to communicate (whether by voice or text), because these apps can apply encryption to protect your communications. This encryption can be stronger and can provide more meaningful protections. The level of protection that you get from using secure communications apps to communicate depends significantly on which apps you use and how they work. One important question is whether a communications app uses end-to-end encryption to protect your communications and whether there is any way for the app developer to undo or bypass the encryption.

For example, malicious software on a mobile phone could read private data on the device (like stored text messages or photos). It could also activate the device's sensors (such as microphone, camera, GPS) to find where the phone is or to monitor the environment, even turning the phone into a bug.

This technique has been used by some governments to spy on people through their own phones and has created anxiety about having sensitive conversations when mobile phones are present in the room. Some people respond to this possibility by moving mobile phones into another room when having a sensitive conversation, or by powering them off. (Governments themselves often forbid people, even government employees, from bringing personal cell phones into certain sensitive facilities mainly based on the concern that the phones could be infected with software to make them record conversations.)

A further concern is that malicious software could theoretically make a phone pretend to power off, while secretly remaining turned on (and showing a black screen, so that the user wrongly believes that the phone is turned off). This concern has led to some people physically removing the batteries from their devices when having very sensitive conversations.



## Infesting Phones with Malware

Phones can get viruses and other kinds of malware (malicious software), either because the user was tricked into installing malicious software, or because someone was able to hack into the device using a security flaw in the existing device software. As with other kinds of computing device, the malicious software can then spy on the device's user.



## Recommended best safety practices for smartphones

It is impossible to imagine life without a smartphone especially if one is involved in some form of work, organising or collaboration environment. This makes the targeting of individuals, organisations and communities very easy as phones always have access to the most protected spaces in homes, organisations and communities. Some of the steps communities and individuals can take to remain secure while using smartphones are:

### Setup a screen lock on the phone

This can be Swipe, Pattern, Pin or Password. This will ensure that the contents of your phone will not be accessible to random/ unauthorised people who get access to your phone. At least one of the four will be fine but a password is the most secure option for a mobile phone. To learn how to encrypt your smartphone hard drive, look below for more information.

### Keep your phone operating system and applications updated

Phone makers and application developers always try to improve the security, efficiency and performance of their products through creating and sending out updates regularly. Downloading and installing these updates ensures that your software or device is safe from viruses but also performs efficiently. Installing updates can be done in your application store or in your device settings.

### Install applications from only trusted sources

Most smartphones have a pre-determined trusted application store where applications are downloaded. These application stores test and verify that applications in their stores are safe for use. Phone applications downloaded directly from the internet are very difficult to verify and ensure they are not malicious and might not be safe. That is why it is recommended to only download applications from a trusted application store like Google Play Store or Apple store other than from the internet. Also uninstalling applications that you no longer use frees up space on your phone making it more efficient.



On a related note, it is useful to always know which apps are installed on your phone and remove apps which you do not recognise or which you do not use any more. This can help improve system speeds, reduce the risks of loss of privacy, and reduces the number of application updates you need to download.

### Turn off phone Wi-Fi and Bluetooth if not in use

Bluetooth and Wi-Fi on a phone when switched on will always try to connect to nearby wireless networks or Bluetooth devices respectively. This happens automatically where detailed information about the device like device identifiers and data transfer capabilities is broadcast. This information can be harvested by malicious individuals and used to target the device. It is recommended to only switch on WIFI and Bluetooth when using them. Also ensure that Bluetooth discovery mode is turned off.

## Communicating securely over a smartphone

Normal phone calls and SMS are not secure because they can be intercepted by Telecom providers. Private or sensitive communications should be conducted on secure applications and platforms. Secure communication applications have encryption built in. End to end encryption is the most trusted form of encryption for communications systems. It ensures that calls and SMSs cannot be intercepted or eavesdropped on. The message or call is encrypted from the sender's device and only decrypted on the receiver's device. Applications like WhatsApp, Signal, Telegram, Wire, Slack all have this technology built in and it is advisable to use them for communication sensitive or private communications. All parties to the communication must have the application installed to a secure communication.

Mobile phones accelerate access and connectivity to the internet especially in low- and medium-income communities every year. This means that more and more people are relying on mobile phones for communicating, organising and collaborating. Unfortunately communicating over the internet using a smartphone is susceptible to surveillance and interception by governments, telecom companies. Surveillance means someone being able to monitor and track one's activities online. To protect the privacy of online activities, there are tools that can be used to not only encrypt online activities but also anonymise/ hide the identity of users on the internet.

A very useful resource to help you decide if your messaging application gives you security and privacy is the Electronic Frontier Foundations Secure Messaging Scorecard.<sup>88</sup>

Virtual Private Networks or VPNs hide user internet activities by accessing the internet through a computer network located in a different geographical location. VPNs also bypass internet censorship by accessing censored pages indirectly through a different computer using encrypted communications. The Onion Router or Tor is unique as it offers anonymity in addition to all VPN service. It provides anonymity by breaking down each step of the connection and assigning it to a different computer within the Tor network which makes it difficult to know which computer is asking for a resource over the internet. VPNs can be free or paid, paid versions usually have added functionalities and features while Tor is free.

88 <https://www.eff.org/secure-messaging-scorecard>

89 <https://play.google.com/store/apps/details?id=org.hzontal.tella&hl=en&gl=US>

90 <https://play.google.com/store/apps/details?id=org.martus.android&hl=en>

91 <https://www.martus.org/>

92 <https://play.google.com/store/apps/details?id=org.secfirst.umbrella>

## Security of Accounts

Online accounts like webmail, Facebook and Twitter have always relied on passwords for security and access control. This has been a disaster as major company hacks exposed user passwords making account takeovers and hijacking easy. This caused a rethink of online account security from a password-only based system to two-step verification system which is much more secure. Two factor authentication requires a code sent to a phone or read from an application on the user's phone in addition to the password. This system ensures that even if an account password stolen, it is almost impossible to gain access to the account without the code from the phone. All major accounts now have this feature, and it is the best option to guarantee account security.

## Operational Security

In addition to the security issues above, your phone may help you carry out your work safely and effectively. Below is a brief survey of some relevant apps:

**Tella**<sup>89</sup> is a documentation app for Android. In challenging environments--with limited or no internet connectivity or in the face of repression. Tella makes it easier and safer to document events, whether that is violence, human rights violations, corruption, or electoral fraud.

**Mobile martus**<sup>90</sup> is a data collector app which connects to the secure documentation database Martus<sup>91</sup>. It permits the user to send field reports securely into an existing documentation project and then the report is securely erased from the phone immediately after sending. It is available for Android.

**Umbrella**<sup>92</sup> is a free self-guided learning app available for Android. It covers many topics of digital, organisational, and operational security in a friendly mobile format. It includes useful checklists when planning and implementing improved security practices. Learn more from **Security First**.



## Resources

This guide is only the beginning. Learn more and obtain updated how-to guides from the below resources:

**Security in a Box**<sup>93</sup> - Tactics chapters and step-by-step guides on how to use many of the software discussed in this booklet. See also their Community Guides for African [Environmental Rights Defenders](#)<sup>94</sup> and [Sexual Minorities](#).<sup>95</sup>

**Surveillance Self-Defence**<sup>96</sup> - Chapters on protection against surveillance and how-to guides on software.

**Digital First Aid Kit**<sup>97</sup> - A how-to guide to responding to various types of digital attacks.

**SaferJourno**<sup>98</sup> - Digital security training manual specifically for teaching journalists.

**Level-Up**<sup>99</sup> - Digital security training curriculum for trainers

**SAFETA**<sup>100</sup> - Digital security auditing framework for security professionals

**VirusTotal**<sup>101</sup> - Scan file or URL link for malware

**The Digital First Aid Kit**<sup>102</sup> - Digital Defenders Partnership

**Umbrella**<sup>103</sup> - is a free self-guided learning app available for Android.

93 <https://securityinabox.org/en>

94 <https://securityinabox.org/en/eco-rights-africa>

95 <https://securityinabox.org/en/lgbti-africa>

96 <https://ssd.eff.org/>

97 <https://www.digitaldefenders.org/digitalfirstaid/>

98 <https://saferjourno.internews.org/>

99 <https://www.level-up.cc/>

100 <https://safetag.org/>

101 <https://www.virustotal.com/>

102 <https://www.digitaldefenders.org/digitalfirstaid/>

103 <https://play.google.com/store/apps/details?id=org.secfirst.umbrella>

# Annexes

## Annex 1: Summary of the UN Declaration on Human Rights Defenders

Elaboration of the Declaration on HRDs began in 1984 and ended with the adoption of the text by the General Assembly in 1998, on the 50th anniversary of the Universal Declaration of Human Rights. A collective effort by several human rights NGOs and some State delegations helped to ensure that the result was a strong, useful and pragmatic text. Perhaps most importantly, the Declaration is not just addressed to States and to human rights defenders, but to everyone. It tells us that we all have a role to fulfil as HRDs and emphasises that there is a global human rights movement that involves us all. The Declaration's full name is the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms – with this longer title is frequently abbreviated to The Declaration on human rights defenders.

### 1. Legal character

The Declaration is not a legally binding instrument however, it contains a series of principles and rights that are based on human rights standards enshrined in other international instruments that are legally binding – such as the International Covenant on Civil and Political Rights.

Moreover, the Declaration was adopted by consensus by the General Assembly and therefore represents a very strong commitment by States to its implementation. States are increasingly considering adopting the Declaration as a binding national legislation.

### 2. The Declaration's provisions

The Declaration provides for the support and protection of HRDs in the context of their work. It does not create new rights but instead articulates existing rights in a way that makes it easier to apply them to the practical role and situation of human rights defenders. It gives attention, for example, to access to funding by organisations of HRDs and to the gathering and exchange of information on human rights standards and their violation.

The Declaration outlines some specific duties of States and the responsibilities of everyone regarding defending human rights, in addition to explaining its relationship with national law. Most of the Declaration's provisions are summarised in the following paragraphs<sup>104</sup>. It is important to reiterate that HRDs have an obligation under the Declaration to conduct peaceful activities.

#### (a) Rights and protections accorded to human rights defenders

Articles 1, 5, 6, 7, 8, 9, 11, 12 and 13 of the Declaration provide specific protections to human rights defenders, including the rights:

- To seek the protection and realization of human rights at the national and international levels;
- To conduct human rights work individually and in association with others;
- To form associations and non-governmental organizations;
- To meet or assemble peacefully;
- To seek, obtain, receive and hold information relating to human rights;
- To develop and discuss new human rights ideas and principles and to advocate their acceptance;
- To submit to governmental bodies and agencies and organizations concerned with public affairs

---

<sup>104</sup> A more detailed commentary on the Declaration was provided in the report of the Secretary-General to the Commission on Human Rights at its fifty-sixth session, in 2000 (E/CN.4/2000/95). The report also contains proposals for the implementation of the Declaration. Furthermore, in July 2011, Margaret Sekagya issued a Commentary to the Declaration on human rights defenders, a key document mapping out the rights provided for in the Declaration based mostly on information received and reports produced by the mandate.

criticism and proposals for improving their functioning and to draw attention to any aspect of their work that may impede the realization of human rights;

- To make complaints about official policies and acts relating to human rights and to have such complaints reviewed;
- To offer and provide professionally qualified legal assistance or other advice and assistance in defence of human rights;
- To attend public hearings, proceedings and trials in order to assess their compliance with national law and international human rights obligations;
- To unhindered access to and communication with non-governmental and intergovernmental organizations;
- To receive help from an effective remedy;
- To the lawful exercise of the occupation or profession of human rights defender;
- To effective protection under national law in reacting against or opposing, through peaceful means, acts or omissions attributable to the State that result in violations of human rights; and
- To solicit, receive and utilize resources for the purpose of protecting human rights (including the receipt of funds from abroad).

### (b) The duties of States

States have a responsibility to implement and respect all the provisions of the Declaration. However, articles 2, 9, 12, 14 and 15 make particular reference to the role of States and indicate that each State has a responsibility and duty:

- To protect, promote and implement all human rights;
- To ensure that all persons under its jurisdiction are able to enjoy all social, economic, political and other rights and freedoms in practice;
- To adopt such legislative, administrative and other steps as may be necessary to ensure effective implementation of rights and freedoms;
- To provide an effective remedy for persons who claim to have been victims of a human rights violation;
- To conduct prompt and impartial investigations of alleged violations of human rights;
- To take all necessary measures to ensure the protection of everyone against any violence, threats, retaliation, adverse discrimination, pressure or any other arbitrary action as a consequence of his or her legitimate exercise of the rights referred to in the Declaration;
- To promote public understanding of civil, political, economic, social and cultural rights;
- To ensure and support the creation and development of independent national institutions for the promotion and protection of human rights, such as ombudsmen or human rights commissions; and
- To promote and facilitate the teaching of human rights at all levels of formal education and professional training.

### (c) The responsibilities of everyone

The Declaration emphasizes that everyone has duties towards and within the community and encourages us all to be human rights defenders. Articles 10, 11 and 18 outline responsibilities for everyone to promote human rights, to safeguard democracy and its institutions and not to violate the human rights of others. Article 11 makes a special reference to the responsibilities of persons exercising professions that can affect the human rights of others, and is especially relevant for police officers, lawyers, judges, etc.

### (d) The role of national law

Articles 3 and 4 outline the relationship of the Declaration to national and international law with a view to assuring the application of the highest possible legal standards of human rights.



**DEFENDDEFENDERS**

East and Horn of Africa Human Rights Defenders Project