STAND UP!

Security guide for human rights defenders in Africa

DEFENDDEFENDERS.ORG

DEFENDDEFENDERS

East and Horn of Africa Human Rights Defenders Project

Stand Up!

Security guide for human rights defenders in Africa

Published April 2017

East and Horn of Africa Human Rights Defenders Project

Human Rights House | Plot 1853 | Lulume Road | Nsambya | P.O. Box 70356 | Kampala | Uganda |

Phone: +256 (0)393 265 820 | +256 (0)414 510 263
E-mail: program@defenddefenders.org | executive@defenddefenders.org
Web: www.defenddefenders.org

This publication is available online in PDF-format at:
www.defenddefenders.org/our-publications

Made possible by the generous support of Open Society Initiative for Eastern Africa (OSIEA), the Swedish International Development Cooperation Agency (Sida) and Soleterre - Strategie die pace ONLUS.

Stand up! The rights of our families, communities, and fellow citizens must be protected. And YOU are the one to defend them! They have the right to live in peace, to enjoy liberty, to speak freely, to live in healthy environments, to enjoy democratic process... in short to enjoy the promises of states made in the Universal Declaration of Human Rights.

But these rights are not claimed easily in Africa. Human rights defence is not "a walk in the park". Human rights defenders across the continent are threatened, harassed, imprisoned, displaced, and even killed because of their convictions and the work they do challenging the status quo.

Have you read the news? From Algeria to Zimbabwe we see an A-Z of repressive and heavy-handed measures restricting civic space to associate, assemble, or express opinions for the common good. While there are differences in severity, even in the most advanced, open, and stable of democracies you will find pushback when your work threatens the interest of the powerful.

You hold in your hands a tool to reduce your exposure to the risks inherent in your goals. Use it to better understand the opposing and supporting factors in your environment, identify your vulnerabilities, and create new capabilities to stand up to adversity.

This tool is composed of two books written to meet the range of security concerns you may face in your personal life, in the life of your organisation or social movement, and in your digital life.

Book One covers personal, physical, and organisational security planning. Learn the essential framework for security analysis and planning as well as the support mechanisms available at the regional and international level for human rights defenders.

Book Two covers digital security for your devices, accounts, and communications. Extend the lessons of security management into the digital realm with risk assessment of your electronic workspace and learn the essential steps to lock down your human rights work as you do it from your phone, computer, email, websites, social media accounts and more.

Turn the recommendations in these two books into action in your life and support your colleagues and communities to do the same and you will see tangible results in the form of more safety consciousness, better communication and planning within communities of human rights defenders, and robustness of response when threats do manifest themselves.

Stand up! Let's do it together, and let's do it safely.

FOREWORD

Threatening phone calls, physical attacks, vicious intimidation of family members all have one common purpose: to prevent those who stand up for human rights from continuing their work. However, there are many ways human rights defenders can attempt to mitigate and protect themselves from these threats, and therefore build their capacity to do their work safely and effectively.

Across the East and Horn of Africa sub-region, we have documented worrying patterns affecting the work of human rights defenders. These include increasing online surveillance, judicial harassment and spurious prosecutions, physical attacks and threats against defenders and their families, targeting of non-governmental organisations' information through break-ins or confiscation of documents, the list goes on.

In our every day work with the human rights defenders community, we have found that in their passion to defend others, it is not uncommon for human rights defenders to forget or neglect their own safety. However, as a fellow defender and friend of mine once pointed out, "you cannot help others if you're dead." Sound security management has unfortunately become a key component of human rights work in the East and Horn of Africa and as human rights defenders we have a responsibility, both to ourselves and to those we serve, to consider this.

The rapid expansion of the Internet has only compounded this problem. Human rights defenders have made clever and creative use of new technologies to shine a light on abuses and violations that may otherwise have gone unreported and undocumented. However, these new possibilities also expose us to new vulnerabilities. As information travels over complex and unprotected digital networks, we can now have our data and safety compromised by state and non-state actors half a world away.

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

This manual contains key strategies and concrete measures that any human rights defender working in the East and Horn of Africa can and should implement immediately to improve their own safety was well as their organisation's, and their constituents'. I encourage all my fellow human rights defenders to take these lessons at heart.

Yours in solidarity,

Hassan Shire

- *Executive Director of DefendDefenders (the East and Horn of Africa Human Rights Defenders Project)*
- *Chairperson of the Pan-African Human Rights Defenders Network.*

BOOK I

PROTECTION AND SECURITY MANAGEMENT

BOOK I

Table of contents

INTRODUCTION

Physical and organisational security management

The adoption of the United Nations Declaration on Human Rights Defenders in 1998 and the establishment of the mandate of the UN Special Rapporteur on the situation of human rights defenders in 2000 constitute major milestones in the protection of human rights defenders around the world. However, defenders continue to face threats and risks despite the existence of these mechanisms.

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

To ensure their security and the continuity of their work, defenders 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 security is intended to serve as a tool for human rights defenders in the East and Horn of Africa sub-region to equip them with necessary strategies and responses to tackle the often volatile environment they operate in.

This manual reflects DefendDefenders' experiences over the past 11 years, focused on ensuring defenders' safety, security and protection through trainings on security management, technical support, security guidelines for defenders most at risk and organisational support.

It was developed by the Security Management team within the Protection Department of DefendDefenders, with support from colleagues, national human rights defenders coalitions and HRDs in the sub-region.

This manual adds to the existing materials on security management as it contextualises security management knowledge and tools for defenders in the region of East and Horn of Africa sub-region and the entire the continent.

CONCEPT DEFINITIONS

WHO IS A HUMAN RIGHTS DEFENDER?

Human rights defenders are people who, individually or with others, act to promote or protect human rights enshrined in the United Nations Universal Declaration of Human Rights 1948 (UDHR). The 1998 United Nations Declaration on Human Rights Defenders refers to "individuals, groups and associations contributing to the effective elimination of all violations of human rights and fundamental freedoms of people and individuals."[5]

Anyone can be an HRD regardless of educational background, professional qualifications, gender, age, race, social group, or nationality. If a street vendor or a banana seller denounces the mistreatment of fellow sellers by local tax authorities, s/he is considered an HRD. In some cases, HRDs can be found in both private and government sectors. All actions taken by HRDs must be peaceful.

DEFINITION OF SECURITY, SAFETY, AND PROTECTION

Understanding the concepts of security, safety and protection, and the similarities and differences between these concepts, will help HRDs conduct risk assessments and develop and implement effective security strategies and measures.

For the purpose of this manual, **security** is defined as "the state of being free from intentional harmful acts" while **safety** is defined as "the state of being free from unintentional harmful acts" both security and safety include the element of danger. **Protection** are measures taken by HRDs or other actors to enhance security[6] and safety.

Examples of protection measures:

- Visitors access procedure;
- Closed-circuit television (CCTV) surveillance and alarm;
- Electric fencing;
- Fire extinguisher;
- First aid kit.

"During the September 2013 demonstrations in my country, HRDs were killed, detained, and tortured by police and national security because we did not think about our security, we did not do risk assessments and never thought about security strategies to mitigate imminent risks."

WHY IS SECURITY MANAGEMENT IMPORTANT FOR HUMAN RIGHTS DEFENDERS?

HRDs, as people who stand up to protect the rights of others, are subjected to risks and their fundamental human rights are regularly violated.

In the East and Horn of Africa,

5 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

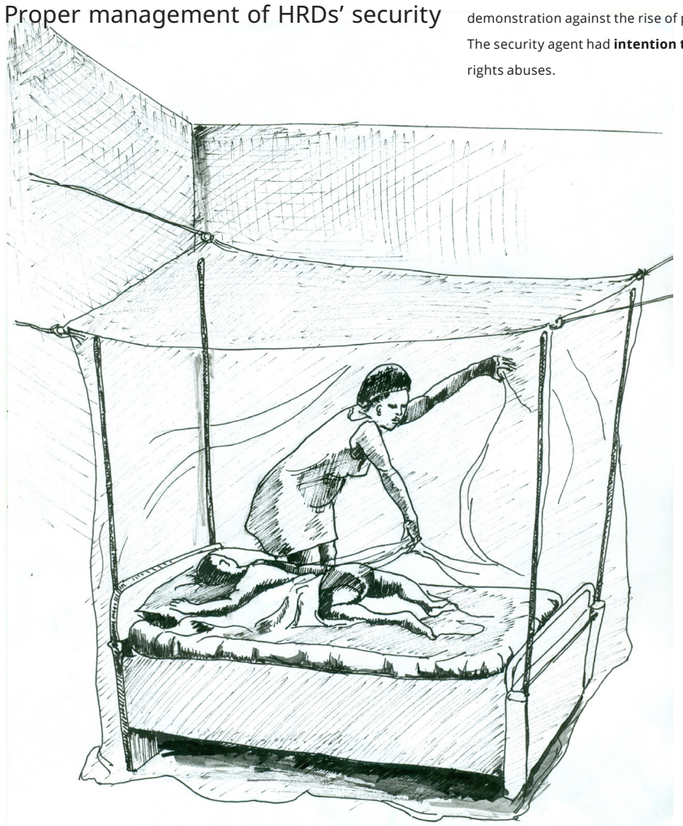
6 Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk, Accessed 23 June 2016.

DefendDefenders has seen HRDs targeted through executions, torture, beatings, arbitrary arrests and detention, death threats, harassment, defamation and smear campaigns, as well as restrictions on their rights to freedom of movement, expression, association and peaceful assembly.

HRDs have also been victims of false accusations, and unfair trials and convictions. Additionally those who challenge existing stereotypes, for example while working on women's rights and Sexual Orientation and Gender Identity (SOGI) rights are regularly confronted with specific challenges compounding existing risks.

SECURITY: Three security agents attacked and arrested a prominent journalist while he was covering a demonstration against the rise of prices of public transport and basic commodities.
The security agent had **intention to harm** the journalist in order to stop him from documenting human rights abuses.

Proper management of HRDs' security is of critical importance in Africa, where political contexts are often volatile and civic space continues to shrink. The existing legal mechanisms for the protection of HRDs are often not fully effective or accessible. Finally, threats to HRDs can often be directed to their families and colleagues. Therefore, more comprehensive security management strategies must be developed.



SAFETY: A woman using a mosquito net to protect her child against mosquito bites which could lead to the baby falling sick with malaria. A mosquito **does not have intention** to cause malaria: it only carries the parasite.

COMMON OBSTACLES AND IMPEDIMENTS TO HRDS' SAFETY AND SECURITY

Despite facing risks and threats in relation to their work, some HRDs are reluctant to take steps to manage their security. Some cite their lack of knowledge or skills as the reason, while others do not feel like their busy schedules allow them to devote time to security management. Lack of awareness of the risks they face, limited financial resources, and unwillingness to take responsibility for managing their security are all common reasons for inadequate security management.

SECURITY MANAGEMENT STEPS

Security management is a process which involves analysing HRDs' context, evaluating and reacting to security incidents and threats, assessing risks, and preparing security plans. These steps are interdependent and they build on each other. Risk assessment is based on context analysis and it constitutes the foundation for security plans. HRDs are encouraged to regularly review the aforementioned process, as security management is always an ongoing practice.

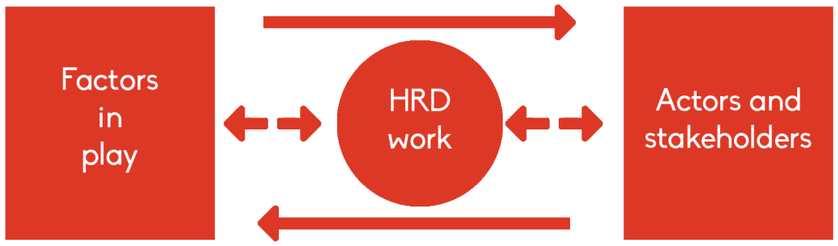
Protection: Measures taken by HRDs or other actors to enhance security and safety.

CONTEXT ANALYSIS

In order to take charge of their security HRDs must carefully seek to understand factors at play, present actors and stakeholders that could have a direct or indirect impact on their work and expose them to risk, or shield them from it. As they carry out their work, HRDs are likely to find themselves in the crosshairs of powerful actors. It is therefore important that a number of key aspects in their daily work are considered and then related to how these may affect their work.

unwanted attention towards an HRD if they have not been under any kind of threat before.

HRDs cannot fully understand the risks they face unless they have a proper appreciation of the environment in which they work. In order to do a proper security assessment, they have to relate their security experiences with what is happening around them, whether directly or indirectly, and their final assessment should be made in relation to their unique context.



WHY IT IS IMPORTANT TO UNDERTAKE A CONTEXT ANALYSIS

Context is the basis for every security decision to be made. The security risks that HRDs face vary according to the context. Risk in itself is dynamic, and changes according to factors in a person's environment. Ultimately, the choice of protection measures is also influenced by the prevailing circumstances in a given context. For instance, while surveillance cameras may deter some risks in a highly sensitive case, they can also attract

A good understanding of the context should also inform an organisation's programs and activities, and influence its methodology, timing, and resource allocation and planning. For example, in some countries in the sub-region, such as Somalia, it is more secure to conduct activities in small groups of no more than five individuals and in closed venues.

Key factors to consider when carrying out a context analysis:

- **Political environment:** ask questions about who the key political players are; what are their declared and underlying interests; is there a conflict and, if so, what the nature of the conflict is; how do political powers interact with and respond to HRD activities, etc;
- **Social-cultural environment:** issues around traditional norms, religion, crime, and social perceptions of the community in which the HRD operates, particularly regarding issues such as women's rights and SOGI rights;
- **Technological aspects:** means of communication, particularly digital communication (for more on this, please refer to Book II of this manual on digital security), and transport within the geographical region in which the HRD is working or intends to work;
- **Legal frameworks:** the laws and constitutional provisions of a certain country and how they apply; how cases of HRDs have been handled in the past; what legal structures are available that affect the area of the HRD's focus; is the judiciary is impartial;
- **Other environmental factors:** public health concerns, weather, geographical terrain which could translate into risk should also be examined.

In carrying out context analysis, HRDs also need to ask themselves the following questions:

SECURITY INCIDENTS

A **security incident** is any event that can expose HRDs and/or their organisations to danger.
Security incidents provide lessons to HRDs and their organisations on the impact of their work and how various people's interests are affected. They also give opportunity to HRDs and their organisations to re-assess their security and protection mechanisms.

Examples of security incidents:

- In some cases, people are sent to the offices of HRDs to find out when HRDs come and leave their office, the means of transport they use, the colour of their car, etc.
- Leakage of information on sensitive cases can cause security threats such as detention, stalking and intimidation from anyone implicated in the human rights violations;
- If visitors are not well screened and their identities documented, anyone can enter the offices of HRDs and commit a crime or compromise their security. They can go even unpunished because there is no record of their visits.

HOW TO REACT TO SECURITY INCIDENTS

The impact of an HRD's work can often be gauged by the reaction HRDs receive from their community. When a security incident occurs, an HRD should take a number of steps to ensure the incident is properly addressed. These steps may vary on a case-by-case basis.

"I received messages stating you are helping westerners, we know your name, where you live and where you work."

Step 1: Incident Reporting

When an HRD experiences or observes a security incident, an immediate report should be sent to the designated security contact person at his/her organisation or organisation's managing director. Key information in this report should include[7]:

- Who is reporting?
- What happened? Where did it happen? When did it happen, as precisely as possible);
- Who was involved, what are the 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;
- Summary of the current situation and whether there are problems or not;
- If yes, what are the decisions that the rapporteur proposes to take/ has taken and what actions are requested?

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

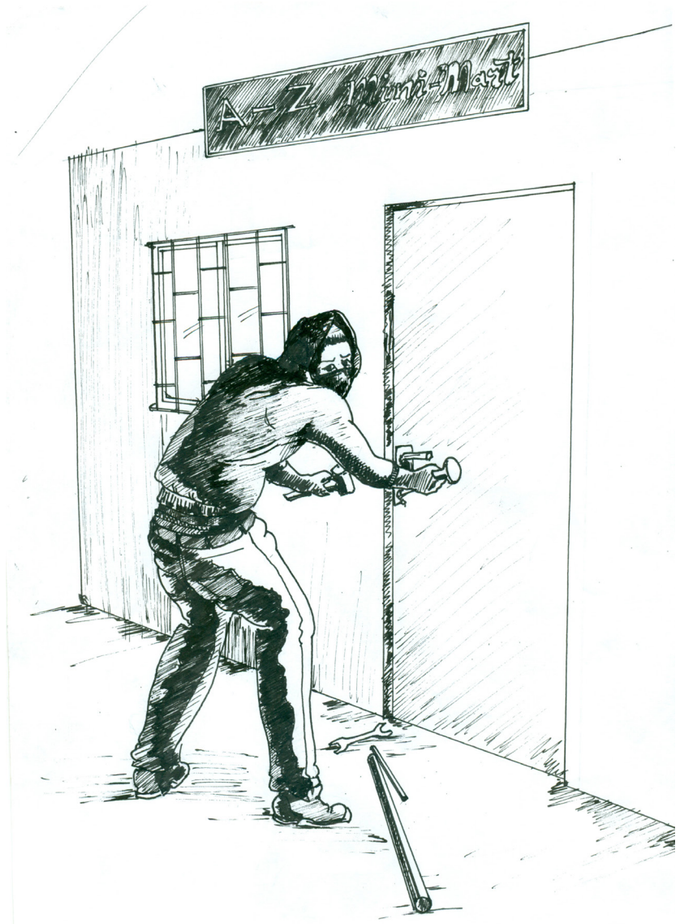
Incident reporting can be written or verbal. However a record of the incident should be kept in written form to prevent the loss of reported facts. HRDs are advised to use secure means of communications (for more on this, please refer to Book II of this manual on digital security).

Step 2: Analyse the facts

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

Step 3: To react or not to react

When the analysis shows that the security incident is serious, HRDs should take necessary actions. The actions depend on the nature of the security incident. In case of an office break-in, new locks and security systems should be put in place. If a security incident is considered as minor, HRDs may not react but they are required to document the incident for future reference.



"My office was broken into, my laptop and medical reports for victims were taken away."

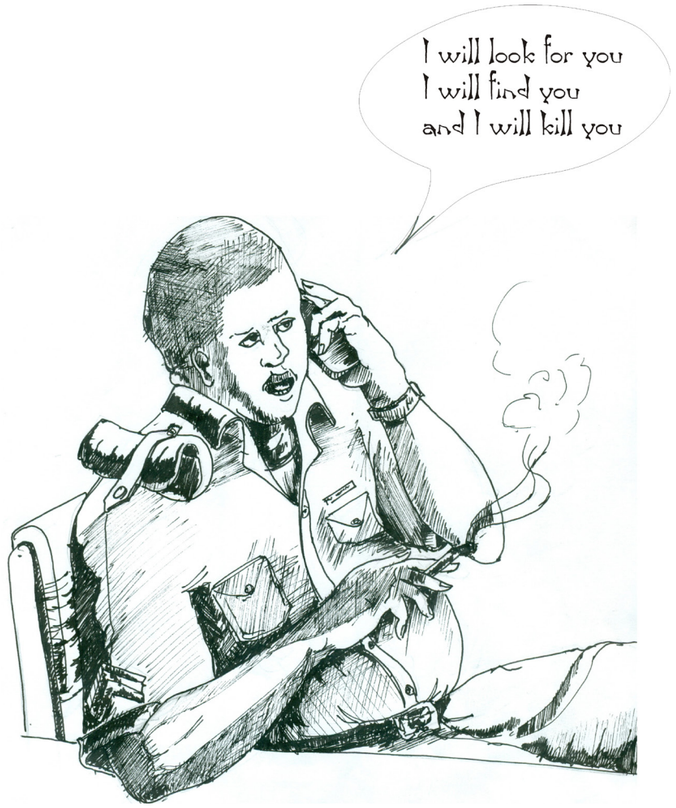
THREAT ANALYSIS

A **threat** can be defined as a "declaration or indication of an intention to inflict damage, punish or hurt."[8]

WHY ARE HUMAN RIGHTS DEFENDERS THREATENED?

HRDs are threatened because their work touches the interests of various actors. These actors may use threats as tools to achieve their goals without paying the cost. Ordinarily threats are not taken seriously until someone is harmed. In security management, understanding how these threats come about will help HRDs to come up with strategies to mitigate them.

The following case studies show HRDs experience and react to threats.



Ngugi is a journalist working with a renowned media forum that advocates for the right to freedom of expression. He started to receive anonymous phone calls from a man telling him to stop the work he was doing. The next month, as Ngugi was heading home from work, he noticed six men following him on his usual route. They overtook him and ordered him to stop, but he declined and instead raised an alarm, which attracted onlookers. The men fled.

What are the threats?
- Anonymous phone calls;
- The trailing by unknown men;
- The actual act of trying to arrest/ kidnap/harm or kill Ngugi.

Objective of the threats?
- To stop Ngugi's work on freedom of expression.

What could have been done differently?
- Report the matter to police so in case he is targeted, the police can begin their search with details of the phone calls received;
- Avoid using the same route;
- Deploy police or security guard at Ngugi's office.

8 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.

Kigozi, a prominent HRD, was due to present on the human rights situation in his country at the UN Human Rights Council (UNHRC). He started to receive phone calls from an individual claiming to be a journalist seeking Kigozi's opinion on the recommendations he would make. The gentleman later identified himself as an official from the national security and told him that they were aware of the advocacy that Kigozi and his colleagues were carrying out. Within days of the call, Kigozi received a death threat from an individual who claimed to have information about his intention to travel to the UNHRC.

Towards the time of his travel, he was called by one of his office staff to urgently attend a meeting with one of their donors. At the office Kigozi was met by national security officials who pulled him into a tinted car and at gunpoint told him not to travel. His attempts to ask who they were and who sent them met with beatings using the back of their pistols. Kigozi was forced to abandon the trip and changed residence thereafter.

What are the threats?
- Anonymous phone calls threatening Kigozi to stop advocacy;
- Death threat from unknown person;
- Death and physical assault threat from security officers who pulled Kigozi into the car and pointed gun at him;
- Travel impeded by national security officials.

Objective of the threat?
- To stop Kigozi' advocacy mission on the human rights situation in his country.

What could have been done differently?
- Alert the police to the phone call especially since it concerned national security;
- Try to find partners that could present on his behalf;
- Cross check with fellow colleagues before rushing to respond to emergency calls;
- Change phone numbers.

In trying to avert some of the harm, which in both cases could have ended in death, it is important for HRDs to critically look at these threats and come up with some logical conclusions. From the two cases, it is important to ask ourselves why the HRDs received these threats. This will lead us to the source of the threat and, how we can avert it.

RISK ASSESSMENT

DEFINITION OF RISK

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

HRDs face risks because their work can impact negatively on the interests of powerful actors. This puts them, their families, organisations, and the people they represent in danger.

Common examples of risks in the sub-region

- The closure of human rights organisations;
- Freezing the accounts of civil society organisations and its active members;
- Assassinations of journalists and HRDs working on sensitive issues;
- Smear campaigns;
- Loss of sensitive information;
- Damage of property and physical assets;
- Travel bans;
- Assault;
- Torture;
- Forced exile;
- Arrest, illegal detention and enforced disappearance;
- Judicial and administrative harassment.

RISK ASSESSMENT

Risk assessments involve examining threats, vulnerabilities, and capacities. These three steps are interconnected and build upon each other as it is shown in the following illustration.

STEPS	EXPLANATION
1. Risk assessment	During this assessment, HRDs identify and assess indicators of potential risk. They are then able to determine the probability and impact of the risks linked to the threats.
2. Vulnerabilities analysis	HRDs look at the factors that contribute to the increased likelihood of harm occurring. It involves considering HRDs' weaknesses in the face of risks.
3. Capacities assessments	HRDs identify existing resources (strengths) to deal with potential risks and required resources to improve their security.

VULNERABILITIES

Vulnerability can be described as those weaknesses of HRDs that increase the likelihood of harm occurrence or aggravate its impact: just like the beautiful colour and sweet scent of flowers which make a flower more susceptible to insects' visits. The elements that an HRD possesses or surrounds himself with or even the actions that an HRD does or does not take could possibly expose him or her to harm.

CAPACITIES

Related to vulnerabilities, capacities are resources, abilities, and strengths that can be used to reduce harm and its impact: similar to using a sugar bowl with a tight lid to keep off black ants. There are various factors contributing to increasing risk levels for HRDs.

Political environment

The political environment in which HRDs operate has a direct influence on the levels of risk they are confronted with. For example, election periods in some countries are characteristically tense in the East and Horn of Africa, and represent periods of heightened risk for HRDs.

Technology

The 21st century has seen technology evolve exponentially, which has greatly enhanced the capacity and impact of HRDs. Communication between defenders, countries, and continents has increased, but the transfer of information through digital means has also created more vulnerabilities. These range from compromised channels of communication and hacking, surveillance, information theft, to shutting down digital infrastructures. Even in cases where measures have been taken to set up secure systems, there have been instances where hackers or intruders have been able to tamper with or bypass the systems.

Thematic issues
Human rights work is at times seen by State and non-State actors as work intended to tarnish and interfere with the status quo. There are several thematic issues that have inevitably resulted in difficulties for the HRDs. These thematic areas include minority rights, women and gender rights, civil and political rights, and extractives and environmental rights.

Common mistakes about risk management

- Focus on reactive strategies: Most HRDs only put in place security management measures after facing risks or threats. The assessment of those probable risks helps to reduce their impact on HRDs and their work. Thanks to the assessment, HRDs can devise strategies to prevent such risks and to handle them in secure way.;
- Copy and paste approach: 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;
- Heroism: Extreme bravery sometimes places HRDs at unnecessary risk. It is advisable for HRDs to measure their vulnerabilities vis-à-vis the magnitude of threats facing them;
- Misrepresentations 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;
- Tendency to ignore one's security: in some instances , HRDs tend to give more priority to their work and victims of violations. The foundation of HRDs' work is based on their security and without it, human rights work cannot be maintained.

Summary

- Risk – probable event or danger;
- Threat – external communicator of danger;
- Vulnerability – internal weakness;
- Capacities – available resources;
- Risks are inherent to HRDs' work ;
- All HRDs face unique risks which vary from one to another;
- Reduce threats and vulnerabilities while increasing capacities in order to mitigate risk.

SECURITY PLANNING

WHAT IS A SECURITY PLAN?

A **security plan** is a document that includes preventive and reactive protection measures that improve personal or organisational safety and security. It is the roadmap for safety and security of the organisation activities, staff, and primary stakeholders.

SECURITY POLICY AND SECURITY PLAN

A **security policy** is a set of general rules, principles, and guidelines within an organisation to meet the needs of proper security management. A security plan can also focuses on the implementation of those rules, principles, and guidelines to fit a specific situation during a given period or activity undertaken by the organisation.

For instance, an organisation may design a security plan for a training or conference and sets general rules or policies aimed at addressing the issue of staff travel.

HOW TO DEVELOP AND IMPLEMENT A SECURITY PLAN?

To come up with a security plan, staff members should meet to brainstorm about the organisation's potential risks. Below are practical steps to follow when developing a security plan.[5]

5 Protection International (PI), Guide for Facilitators, Page 96, http://protectioninternational.org/wp-content/uploads/2014/04/PI-FACILITATORS-GUIDE_EN.pdf , Accessed 2 August 2016.

IMPLEMENTATION OF THE SECURITY PLAN

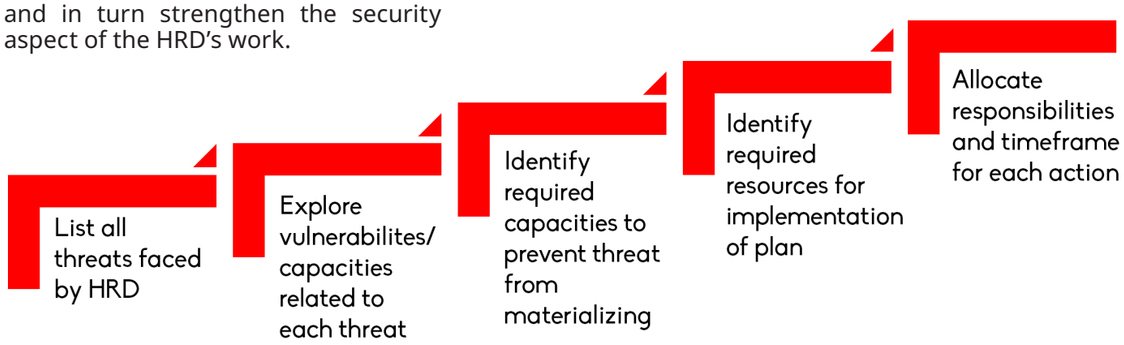
The implementation of the security plan takes into account:
- The involvement of all the staff and the support of the organisation's management;
- Clear communication among all parties involved in its development as per the content;
- Measures to ensure adherence;
- Regular updates and reviews.

PRACTICAL WAYS OF PUTTING IN PLACE SECURITY MEASURES

Come up with strategies and think about actions under each category. To ensure the acceptance of different actors, one would have to implement activities that would bring these actors to a point of positively appreciating the work they are doing. This acceptance in turn would reduce their level of risk and in turn strengthen the security aspect of the HRD's work.

What to consider?

- The security plan should be concise, precise, and available as a reference document, user friendly, and with up-to-dated information;
- It should address prioritised threats with a focus on a proper risk assessment;
- For each vulnerability, an action shall be formulated to meet the required capacity and therefore mitigate the risk.



STRATEGY	POSSIBLE STEPS
Acceptance	Sensitisation about work HRDs do; Advocacy around the work done; community involvement in the work done; lobbying, etc.
Deterrence	Wall fence; secure gate; watchmen/guards; strong, burglar proof, locks; security lights; CCTVs, etc.
Transfer	Working with other grassroots HRDs that are more welcome and have a level of immunity at the community level; networking with more prominent or high-profile entities; working in coalitions as opposed to individually; working under umbrella organisations; insurance policies, etc.

On the other hand, deterrence strategy involves putting in place barriers to prevent unwanted access and intrusion into the HRD's space. The transfer strategy suggests that to be more secure, an HRD can redirect risks that they cannot bear to other entities that have the capacity to deal with the risk. It is a way of hiding behind a more formidable force.[6]

6 Van Brabant 2000, p.57

EXISTING PROTECTION MECHANISMS FOR HUMAN RIGHTS DEFENDERS

UN SPECIAL RAPPORTEUR ON HUMAN RIGHTS DEFENDERS

In 2000, the United Nations Commission on Human Rights established the mandate of Special Rapporteur on the situation of human rights defenders to support implementation of the 1998 Declaration on Human Rights Defenders.[7] The current mandate holder is Mr. Michel Forst.[8]

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

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

Several regional mechanisms have been created following the establishment of the UN Special Rapporteur on human rights defenders with the aim of increasing the protection of HRDs, the following are the major regional mechanisms:

From left to right: Pierre Claver Mbonimpa (President of l'Association pour la Protection des Droits Humains et des Personnes détenues), Hassan Shire (Executive Director of DefendDefenders), and Michel Forst (UN Special Rapporteur on the situation of human rights defenders) during a panel discussion at the 31st session of the UN Human Rights Council.

- The Special Rapporteur on Human Rights Defenders of the African Commission on Human and Peoples' Rights (2005)[9];
- The Special Rapporteur on Human Rights Defenders of the Inter-American Commission for Human Rights[10];
- The European Union (EU) Guidelines on Human Rights Defenders adopted by EU foreign ministers in 2004[11].

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

8 OHCHR, 'Resolution 25/18. Mandate of the Special Rapporteur on the situation of human rights defenders' https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/134/52/PDF/G1413452.pdf?OpenElement, Accessed 1 August 2016.

9 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.

10 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, accessed 1 August , 2016.

11 EUR-Lex, Access to European Union Law, 'EU guidelines on

The United Nations mandate collaborates with regional mechanisms to ensure protection of HRDs. This collaboration includes sharing experiences and information, comparing and mutually reinforcing working methods, and identifying common objectives.

At national level, several states around the world followed the United Nations and regional steps, and created their own national mechanisms that help protect HRDs. These include constitutions and legislation, judiciary system, and national human rights institutions.

THE SPECIAL RAPPORTEUR ON HUMAN RIGHTS DEFENDERS OF THE AFRICAN COMMISSION ON HUMAN AND PEOPLES' RIGHTS

In 2004, the African Commission on Human and Peoples' Rights (ACHPR) established the mandate of the Special Rapporteur on human rights defenders in Africa.[12]

The current mandate holder is Reine Alapini-Gansou, a lawyer from Benin.[13] the mandate calls for the special rapporteur to:

- To seek, receive, examine and to act upon information on the situation of human rights defenders in Africa;
- To submit reports at every Ordinary Session of the African Commission;
- To cooperate and engage in dialogue with Member States, national human rights institutions, relevant intergovernmental bodies, international and regional mechanisms of protection of HRDs and other stakeholders;
- To develop and recommend effective strategies to better protect HRDs and to follow up on his/her recommendations;
- To raise awareness and promote the implementation of the UN Declaration on Human Rights Defenders in Africa.

Since the establishment of the mandate, the Special Rapporteurs have maintained regular contact with HRDs through their participation in regional forums, carried a number of country visits, including joint visits and press releases with the UN Special Rapporteur on the situation of human rights defenders.[14]

The Special Rapporteur has also encouraged individuals and NGOs 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.[15]

NATIONAL MECHANISMS FOR HUMAN RIGHTS DEFENDERS PROTECTION

The Declaration on Human Rights Defenders stresses that the primary responsibility and duty to promote and protect human rights and fundamental freedoms lie 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 is the first time an African State has enacted a law with the specific purpose of protecting HRDs.[16]

Below are examples of mechanisms for HRDs protection at the national level:

- **Administrative mechanisms:** national human rights institutions, legal institutions such as judiciary, law enforcement, police, national security, legislative bodies, and local governments.
- **Legislations:** Constitutions and specific laws such as "The Law on the Promotion and Protection of Human Rights Defenders" in Ivory Coast.

human rights defenders', http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33601, Accessed 1 August 2016.

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 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

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

15 Article 55 of the African Charter on Human and Peoples' Rights

16 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

ANNEX

Summary of the UN Declaration on Human Rights Defenders

Elaboration of the Declaration on human rights defenders[17] began in 1984 and ended with the adoption of the text by the General Assembly in 1998, on the occasion of the 50th anniversary of the Universal Declaration of Human Rights. A collective effort by a number of human rights non-governmental organisations and some State delegations helped to ensure that the final result was a strong, very useful, and pragmatic text. Perhaps most importantly, the Declaration is addressed not just to States and to HRDs, 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.

1. Legal character

The Declaration is not, in itself, 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 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 HRDs. 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 with regard to defending human rights, in addition to explaining its relationship with national law. Most of the Declaration's provisions are summarized in the following paragraphs.[18] 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:

17 OHCHR, Declaration on Human Rights Defenders, http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx Accessed 3 August 2016.

18 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 Sekaggya 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.

- 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 organisations;
- 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 organisations concerned with public affairs 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 organisations;
- To benefit from an effective remedy;
- To the lawful exercise of the occupation or profession of HRDs;
- 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;
- 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.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;
- 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 HRDs. 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 also 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 ensuring the application of the highest possible legal standards of human rights.

BOOK II
DIGITAL SAFETY

BOOK II

Table of contents

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, an iPad, and a laptop. Twenty 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 human rights defenders and society at large without necessarily having an equal opportunity to affect such developments.

The global war on terrorism has grown at the same time as 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 the fraction of the cost of home-grown capabilities. This booklet has been designed to give you a solid base of technological knowledge in order 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 human rights defenders as they encounter digital challenges and questions in their work. This booklet is organised in the following structure:

RISK ASSESSMENT

Cyber security threats face every user of digital technology, from peasants to presidents. Compared to ordinary users though, the stakes are higher for human rights defenders 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.

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 all the time, however we will link you to resources which stay updated with the newest references. Our Five Security Goals are:

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.

Security of Data on computers, flash disks, external drives, and mobile phones

Data is stored on your laptop, desktop, mobile phone, iPads, 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.

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.

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.

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.

HOW TO USE THIS MANUAL

Think of this manual as a companion on your journey to improved digital security practices. We have included many resources to online information in footnotes and in most cases you will need to follow these links to obtain a fuller explanation on each subject. Yet even these links may not be sufficient and you will need to use online search engines to search for information and solutions to challenges that come up.

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. To become more secure, you must determine what you need to protect, and whom you need to protect it from. Threats can change depending on where you arelocated, what you are doing, and whom you are working with. Therefore, in order to determine what solutions will be best for you, you should conduct a threat modeling assessment.

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 in order 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.

In order 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.

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.

Make a list of who might want to get 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 actually 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 neighbors as opposed to an 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 do not view the threat as a problem.

Now, let's practice threat modeling

If your office stores whistleblower'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 whistleblowers?
  - They can steal the files and destroy evidence that can be used against them

Once you have asked yourself these questions, you are in a position 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'll want to get the best locks on the market, and perhaps even add a security system.

BASIC DEVICE SECURITY

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.

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

Nearly all aspects of life now revolve around technology and the Internet to create, store and share information. All users tap into these opportunities using devices. These can be desktops, laptops, smartphones or other gadgets. The list has exponentially increased with the so-called 'Internet of things' where literally everything (including your phone, your car, watch, and refrigerator!) 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 as a result of device compromise or attack.

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

HOW DO I PROTECT MYSELF AGAINST MALWARE?

Malware, short for "malicious software," is software 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 in 2015 it was revealed that malware developers Hacking Team was selling its product to Ethiopia, Sudan, Egypt, Morocco, and (pre-revolutionary) Tunisia.[19] Malware has wide-range capabilities; it may allow an attacker to record from a webcam and microphone, disable the notification setting for certain antivirus programs, record keyboard strokes, copy emails and other documents, steal passwords and more.

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 Hacking Team.

19 Karsperksy ,What is malware and how to defend against it, http://usa.kaspersky.com/internet-security-center/internet-safety/what-is-malware-and-how-to-protect-against-it#.WJwGtX_3Mo9, Accessed 8 February 2017

Kuma is a 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.

She 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.

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. If you have the ability to monitor your network traffic, the timing and volume of that traffic might indicate a compromise. 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.

Security in a Box maintains a step-by-step guide on Avast! a popular free anti-virus software for Windows. Find it at https://securityinabox.org/en/guide/avast/windows

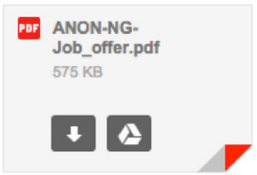
How can attackers use malware to target me?

The best way to deal with a malware attack is to avoid getting infected in the first place. This can be a difficult feat if your adversary has access to zero day attacks—attacks that exploit a previously-unknown vulnerability in a computer 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. But zero day exploits are expensive to buy and costly to re-use (once you use the secret tunnel to break into the fortress, it increases the chances that other people may find it). It is much more common for an attacker to trick you into installing the malware yourself.

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 colleague 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) 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 malware delivery tricks, but will not protect against the most sophisticated adversaries.

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.



If you are using Gmail you can view the attached document by clicking on this square (not the download arrow). 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.

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

If you do find malware on your computer, unplug 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've found the malware, removing it does not guarantee the security of your computer. Some malware gives the attacker the ability to execute arbitrary code on the infected computer—and there is no guarantee that the attacker has not installed additional malicious software while in control of your machine.

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 considered to be compromised. You may wish to reinstall the operating system on your computer in order to remove the malware. This will remove most malware, but some especially 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 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.

The first step of updates is to ensure that your operating system itself is receiving automatic updates. Next check that your software is up to date. You should try to update everything but some of the most important software to keep updated is your web browser (Chrome, Firefox, etc.), Adobe Reader, Adobe Flash, and Java.

There is a free application which helps centralize the search for out-of-date programs on your computer. Flexera PSI[20] checks your installed software and version numbers against an online database of current version numbers and links you to download new versions of your programs. Your antivirus program may offer a similar functionality under a different name such as 'Smart Scan' or 'Vulnerability Scan'.

SAFE SOFTWARE PRACTICES

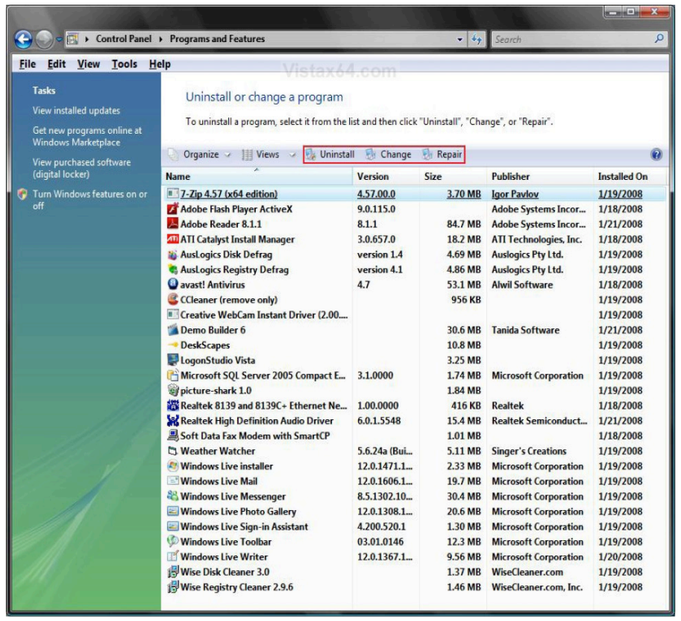
Since software unfortunately becomes vulnerable and needs to be updated all the time, one of the simplest ways to keep secure is to avoid installing unnecessary programs.

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.[21] Go to your list of

20 Flexera, "Stay secure by updating insecure programs on your computer", http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/personal-software-inspector/, Accessed 8 February 2017

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

installed programs (In Windows: 'Add/ Remove Programs' or 'Uninstall or change a program') and review what is installed. Are there programs you do not recognize 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 up your browser 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.

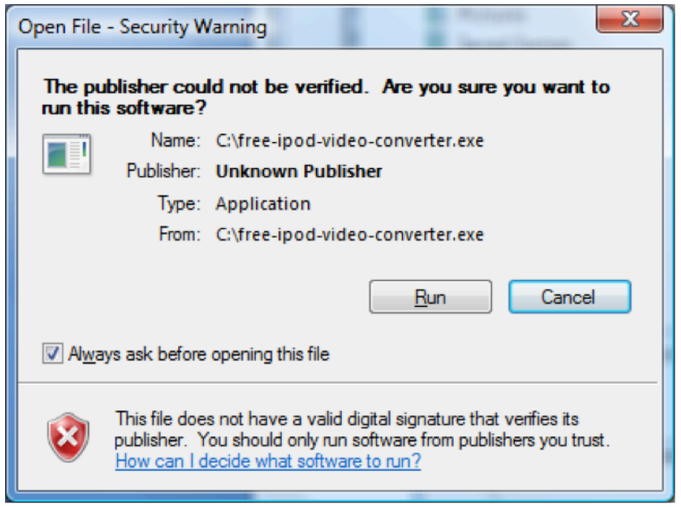
Browser extensions are sensitive because they may be able to read and change information appearing on your browser and being typed in such as passwords, banking information, and social media shares.

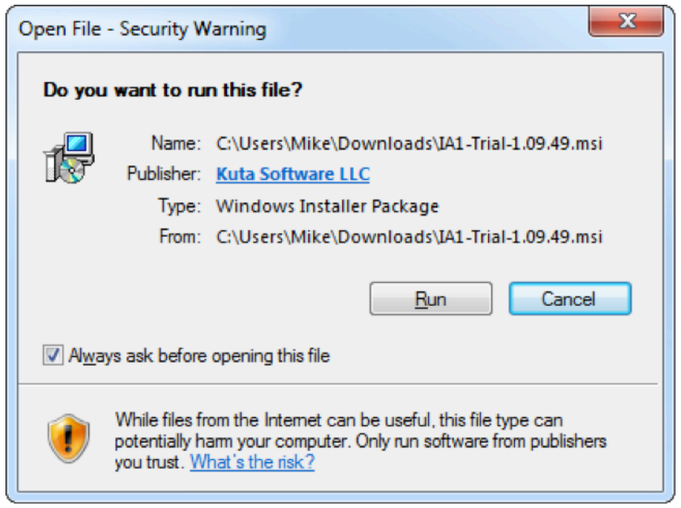
Safe Sources

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 www.adobe.com rather than from 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.

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, do not 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





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[22] 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 are able to '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 publishers 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.

22 How-To Geek,Here's what happens when you install the top 10 download.com apps http://www.howtogeek.com/198622/here-what-happens-when-you-install-the-top-10-download.com-apps/, Accessed 8 February 2017

SECURITY OF DATA ON DEVICES

Digital security in five parts

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 phone, laptop, iPad, or flash drive 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. All an attacker needs to do is to access the storage directly (for example by attaching a computer's hard drive to a new computer), and the data can be copied or examined without knowing your password.

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 the encrypted data—there's 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 of 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 usable. This protects computers and phones in case they are stolen or confiscated.

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.

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 authorization.

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.

Cryptography is the mathematical science of codes, ciphers, and secret messages. Encryption is an application of this science used to scramble information such that anyone without a password will be unable to access that information. Throughout history, people have used encryption to send messages to each other that (hopefully) could not be read by anyone besides the intended recipient.

Today, we have computers that are capable of performing 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.

Under some circumstances, encryption can be automatic and simple. But there are times when you will need to take extra steps to secure your data. The more you understand it, the safer you will be.

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 DiskCryptor 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 of your files will be vulnerable. A more robust solution is to combine full-device encryption with file and folder encryption in order 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, an independent branch of the now-abandoned Truecrypt project. 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 Axcrypt, 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. Do not 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 and 8, and on most versions of Windows 8.1 and above. An easy to use guide is available at HowToGeek[23] plus another at Windows Central specifically for Windows 10.[24] 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.[25]

DiskCryptor (Windows)[26] - Read the guide from the Electronic Frontier Foundation on the DiskCryptor full-device encryption software for Windows.[27]

Veracrypt[28] (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.[29]

Phone Encryption

Android Phone Encryption - Read the guide from HowToGeek.[30]

iPhone and iPad Encryption - Simply activating a passcode lock on your device will enable device encryption. Learn more at the Electronic Frontier Foundation guide.[31]

External Drives

BitLocker To Go (Windows) - Encrypt external hard drives and flash drives with BitLocker To Go.[32]

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.[33]

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.

23 How-To Geek, How to set ste up bitlocker encryption on windows http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/,Accessed 8 February 2017

24 Windows Central, How to use bitlocker encryption on windows 10, http://www.windowscentral.com/how-use-bitlocker-encryption-windows-10, Accessed 8 February 2017

25 Apple, Use FileVault to encrypt the startup disk on your mac, https://support.apple.com/en-us/HT204837, Accessed 8 February 2017

26 https://diskcryptor.net/

27 Electronic Frontier Foundation,How to: Encrypt your windows device, https://ssd.eff.org/en/module/how-encrypt-your-windows-device, Accessed 8 February 2017

28 VeraCrypt,Project description,https://veracrypt.codeplex.com/, Accessed 8 February 2017

29 Security in a box,Veracrypt:Secure file storage, https://securityinabox.org/en/guide/veracrypt/windows, Accessed 8 Februaury 2017

30 How-To Geek, How to encrypt your android phone http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/, Accessed 8 February 2017

31 Apple, How to encrypt your iphone, https://ssd.eff.org/en/module/how-encrypt-your-iphone, Accessed 28 April 2016

32 Microsoft, Enable bitlocker on a USB Flash drive to protect data, https://technet.microsoft.com/en-us/magazine/ff404223.aspx,

33 Apple, OS X El Capitan: Encrypt removable disks or media, https://support.apple.com/kb/PH21791?locale=en_US, Accessed 8 February 2017

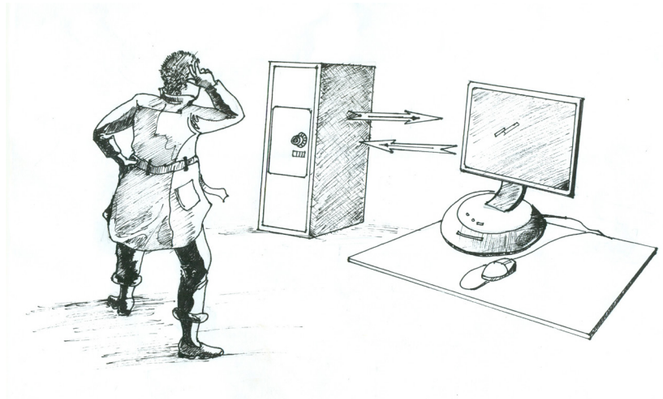
BACKING UP YOUR DATA

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. Remember that 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 and Restore*[34]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*[35] which will retain versions of documents as they change over time. You can use either of these systems or even both at the same time. Mac OS X also has a built-in backup system called Time Machine[36] 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,[37] Duplicati,[38] and Viivo.[39]

34 Microsoft, Back and Restore yout PC, https://support.microsoft.com/en-us/help/17127/windows-back-up-restore, Accessed 8 February 2017

35 Microsoft, File history in Windows, https://support.microsoft.com/en-us/help/17128/windows-8-file-history, Accessed 9 February, 2017

36 Apple, Time Machine, Time Machine https://support.apple.com/en-us/HT201250, Accessed 9th February 2017

37 Boxcryptor, Highest security for files in the cloud, https://www.boxcryptor.com/, Accessed 9 February 2017

38 Duplicati,Free backup software to store encrypted backups online For Windows, macOS and Linux, www.duplicati.com, Accessed 9 February 2017

39 Viivo,Encrypt your files before they sync to Dropbox, Box, Google Drive, https://viivo.com/, Accessed 9 February 2017

SECURITY OF DATA MOVING THROUGH NETWORKS

Digital security in five parts

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; 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.

As you can see, on the image on page 45, 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.

COMMUNICATIONS 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.

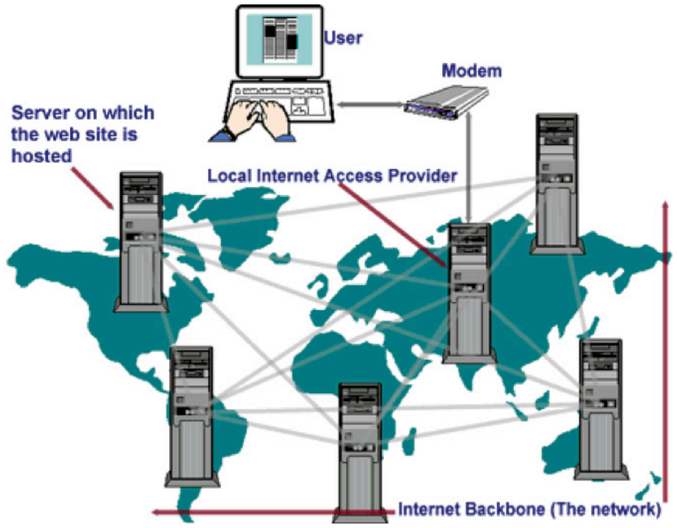
Often the safest way to communicate with others is in person, without computers or phones being involved at all. Because this is not always possible, the next best thing is to use end-to-end encryption while communicating over a network if you need to protect the content of your communications.

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 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.



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

encryption while communicating over a network if you need to protect the content of your communications.

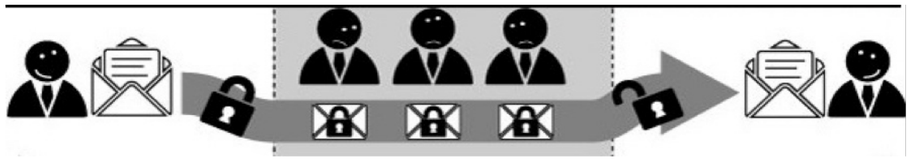
How does end-to-end encryption work?

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.

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 read the message. When Abuya receives it, she must use his key to decrypt it into a readable message.

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[40] 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.

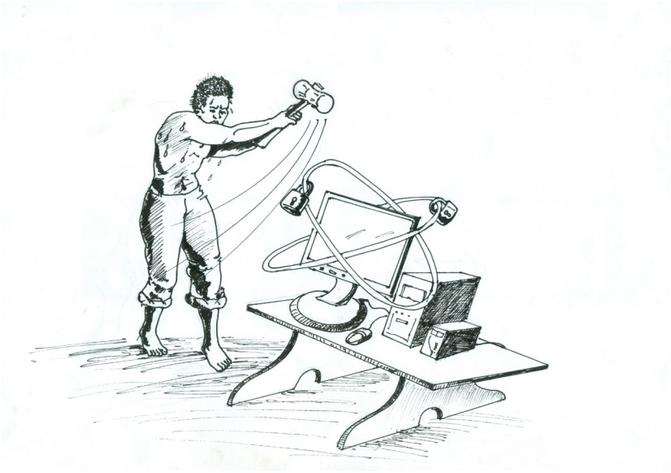
Voice Calls

When you make a call from a landline or a mobile phone, your call is not end-to-end encrypted. If you're 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 organisations 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 Hangouts, 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.

40 Skype, What is the cloud, https://support.skype.com/en/faq/fa10983/what-are-p2p-communications, Accessed 9 February 2017

41 Electronic Frontier Foundation, Secure messaging scorecard, https://www.eff.org/secure-messaging-scorecard, Accessed 9 February 2017



A very useful resource to help you decide if your messaging application gives you security and privacy is the Electronic Frontier Foundation's Secure Messaging Scorecard.[41]

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

- Ostel
- Silent Phone[42]
- Signal[43]

Among these Signal is the most widely adopted and we do recommend its usage. 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 app[44] for Android, formerly SMS Secure.

42 Silent Circle, Silent mananger, https://www.silentcircle.com/services#mobile, Accessed 9 February 2017

43 Electronic Frontier Foundation, How to use Signal on IOS, https://ssd.eff.org/en/module/how-use-signal-ios, Accessed 9 February 2017

44 Silence, Need some Privacy, https://silence.im/, Accessed 9 February 2017

Other secure messaging options work over the Internet. So, for instance, users of Android and iOS[45] can chat securely using Signal.[46]

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.

Some tools that incorporate OTR with instant messaging include:

- Pidgin[47] (for Windows or Linux)
- Adium[48] (for OS X)
- ChatSecure[49] (for iPhone and Android)
- Jitsi[50] (for Windows, Linux, and OS X)
- Jitsi Meet[51] (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 or Chrome. 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 (for example: https://mail.google.com).

45 Open Whispers systems, Privacy that fits in your pocket, https://whispersystems.org/#privacy, Accessed 9 February 2017

46 Electronic Frontier Foundation, How to: use Signal on IOS, https://ssd.eff.org/en/node/61/,Accessed 9 February 2017

47 Electronic Frontier Foundation,How to: Use OTR for windows https://ssd.eff.org/en/module/how-use-otr-windows, Accessed 9 February 2017

48 Electronic Frontier Foundation, How to: Use the OTR for MAC, https://ssd.eff.org/en/module/how-use-otr-mac, Accessed 9 February 2017

49 Electronic Frontier Foundation, How to: Install and use Chat Secure, https://ssd.eff.org/en/module/how-install-and-use-chatsecure, Accessed 9 February 2017

50 Jitsi, Open source video calls, https://jitsi.org/, Accessed 9 February 2017

51 Jitsi, Jitsi meet, https://jitsi.org/Projects/JitsiMeet, Accessed 9 February 2017

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 would like to make sure that you are always using HTTPS on sites where it is available, download the HTTPS Everywhere[52] browser add-on for Firefox or Chrome.

Some webmail providers that use HTTPS by default include:

- Gmail
- Riseup
- Yahoo

Some webmail providers that 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.

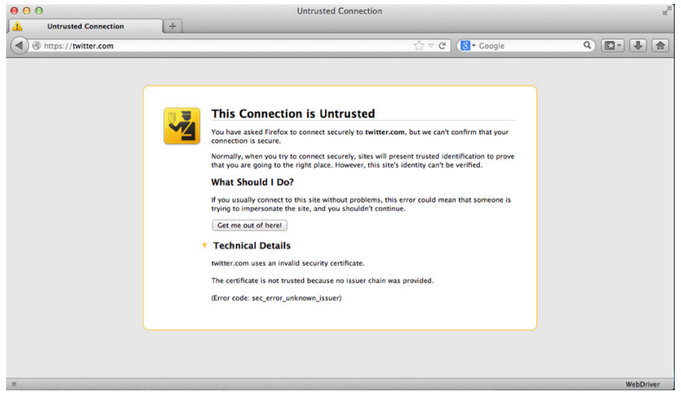
What does transport-layer encryption do and why might you need it?

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.

HTTPS is the most basic level of encryption for your web browsing that we recommend for everybody. It is as basic as putting on your seat belt when you drive.

52 Electronic Frontier Foundation, https everywhere, https://www.eff.org/https-everywhere, Accessed 9 February 2017

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 the whole session and information exchanges between your computer and the server, it 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 at a later time if you are presented with the warning shown in the image above.



Advanced Email Security (GPG/PGP)

There are some things that HTTPS does not do. When you send an 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, most email providers have a policy that says they will tell you when you 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[53], Yahoo[54], and Microsoft[55], 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).

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[56], and Linux[57].

To use PGP/GPG in your web browser using webmail, look at using the Mailvelope[58] browser plugin or watch out for the fully featured webmail clients like ProtonMail.[59]

53 Google, Transparency report to information,https://www.google.com/transparencyreport/ , Accessed 9 February 2017

54 Yahoo, Transparency Report overview, https://transparency.yahoo.com/ , Accessed 9 February 2017

55 Microsoft, Our commitment to transparency, https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/, Accessed 9 February 2017

56 Electronic Frontier Foundation, How to: Use PGP for MAC OS X, https://ssd.eff.org/en/module/how-use-pgp-mac-os-x, Accessed 9 February 2017

57 Electronic Frontier Foundation,How to: Use PGP for Linux https://ssd.eff.org/en/module/how-use-pgp-linux, Accessed 9 February 2017

58 Mailvelope, https://www.mailvelope.com/ ,Accessed 9 February 2017

59 ProtonMail, Secure Email, https://protonmail.com/, Accessed 9 February 2017

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.[60]

What end-to-end encryption does not do

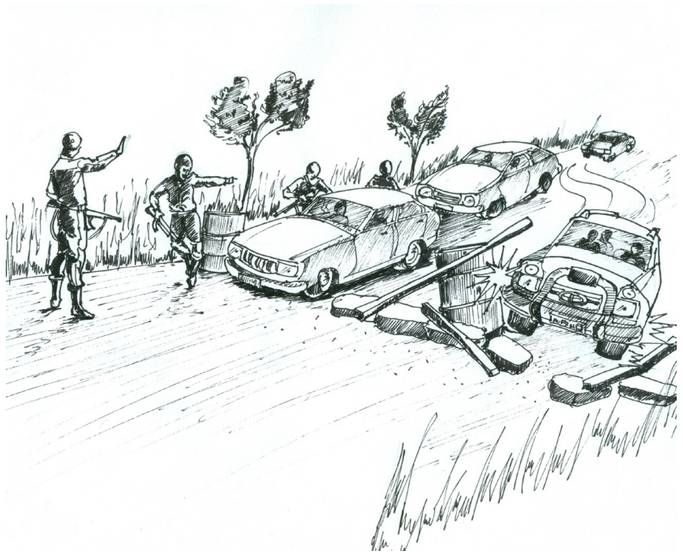
End-to-end encryption only protects the content of your communication, not the fact of the communication itself. It does not protect your metadata—which is everything else, including the subject line of your email, or who you are communicating with and when.

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 do not 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 remains 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 do not 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. 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[61] showed a detailed history of Spitz's movements. Spitz gave an inspiring TED speech about this case which is available online.[62]



60 Tactical Technology Collective, Decrypting Encryption, https://tacticaltech.org/projects/decrypting-encryption, Accessed 9 February 2017

61 Zeit Online, Tell- on Telephone, http://www.zeit.de/datenschutz/malte-spitz-data-retention,Accessed 9 February 2017

62 Ted, Your phone company is watching, http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=en, Accessed 9 February 2017

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 words "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 are 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**[63] 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[64], you might visit http://m.twitter.com[65], 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.

Web-based Proxies

A web-based proxy (such as http://proxy.org/)[66] is a good way of circumventing censorship. In order 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 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, 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[67] at 8.8.8.8 and 8.8.4.4. OpenDN[68]S 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.[69]

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[70], Psiphon[71], BitMask[72], and Opera[73].

For some recommendations about paid VPN services, check here[74]. Some VPNs with exemplary privacy policies could still be run by devious people.

63 Electronic Frontier Foundation, Https everywhere, https://www.eff.org/https-everywhere, Accessed 9 February 2017

64 Twitter, https://twitter.com/, Accessed 9 February 2017

65 Twitter, Login https://mobile.twitter.com/home, 9 February 2017

66 Proxy, Proxify, http://proxy.org/, Accessed 9 February 2017

67 Google, Public DNS, https://developers.google.com/speed/public-dns/?hl=en, Accessed 9 February 2017

68 Open DNS, https://use.opendns.com/, Accessed 9 February 2017

69 Open DNS, https://use.opendns.com/, Accessed 9 February 2017

70 Betternet, Online security and privacy for all devices and Platform, https://www.betternet.co , Accessed 9 February 2017

71 Psiphon, Beyond borders, https://www.psiphon3.com/ ,Accessed 9 February 2017

72 Bitmask, Encrypted communication for mere mortals (superheroes welcome, too) https://bitmask.net , Accessed 9 February 2017

73 Opera, Unblock the web for free, https://www.opera.com/apps/vpn , Accessed 9 February 2017

74 Torrentfreak, What Are The Best Anonymous VPN Services? https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/ Accessed on 12 December 2014

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 are communicating will never see your IP address, but instead will see the IP address of the last Tor router through which your traffic traveled.

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 the guide from the Electronic Frontier Foundation.[75]

75 Electronic Frontier Foundation, How to: Use Tor for Windows https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/ Accessed 9 February 2017

ACCOUNT SECURITY

Digital security in five parts

CREATING STRONG PASSWORDS

Because remembering many different passwords is difficult, people find it hard to effectively and efficiently work with passwords. 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 a large number of passwords safely. This makes it practical to avoid using the same password in multiple contexts. The password manager protects all of 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, KeePassX is an open source, free password safe that you keep on your desktop. it is important to note that if you are using KeePassX, it will not automatically save changes and additions. This means that if it crashes after you've 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

Seseko is the executive director of a sexual minorities organization. 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 in order 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 organization 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.

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 memorized 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.

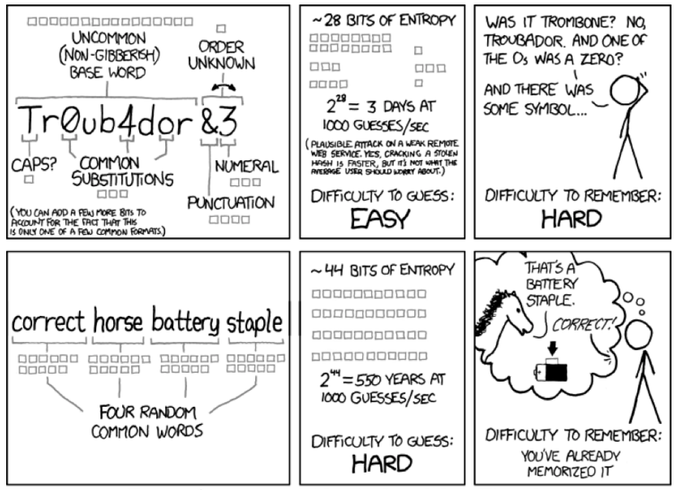
There are several ways to create a strong and memorable passphrase; the most straightforward and sure-fire method is Arnold Reinhold's "Diceware."[76]

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.

76 Diceware, What is a passphrase, http://world.std.com/~reinhold/diceware.html , Accessed 9 February 2017

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'[77]



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.

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 in order 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.

77 Electronic Frontier Foundation, How to: Use Tor for Windows, https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/ , Accessed 9 February 2017

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're 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.

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 memorize 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.

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 [78], Yahoo[79], Facebook [81], and Twitter [81] accounts!

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 very serious 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.

78 Google, 2-step verification, https://www.google.com/landing/2step/ , Accessed 9 February 2017

79 Yahoo, Signin, https://login.yahoo.com/account , Accessed 9 February 2017

80 Faccebook, Introducing login approvals, https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920, Accessed 9 February 2017

81 Twitter,Get started with login aprovals, https://blog.twitter.com/2013/getting-started-with-login-verification ,Accessed, 9 February 2017

MOBILE SECURITY

Digital security in five parts

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, 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 canot. 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.

Fayed is an activist working on transparency, accountability and freedom of expression. He has many friends who have run away from 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 arrested him at his home and took him to court accusing him of planning to overthrow the government and communicating with terrorists. In the court 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.

Mobile Signal Tracking

Network operator can calculate where a particular subscriber's phone is located whenever the phone is powered on and connected with the network. The ability to do this results from the way the mobile network is built, and is commonly called triangulation.

One way the 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 as long as 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[82] 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.

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 of 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 of 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 in order to monitor the area. There is currently no reliable defense 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.

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.[83]

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

82 Zeit Online, Betrayed by your own data, http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz , Accessed 9 February 2017

83 Zeit online, Tell-all telephone, http://www.zeit.de/datenschutz/malte-spitz-data-retention , Accessed 9 February 2017

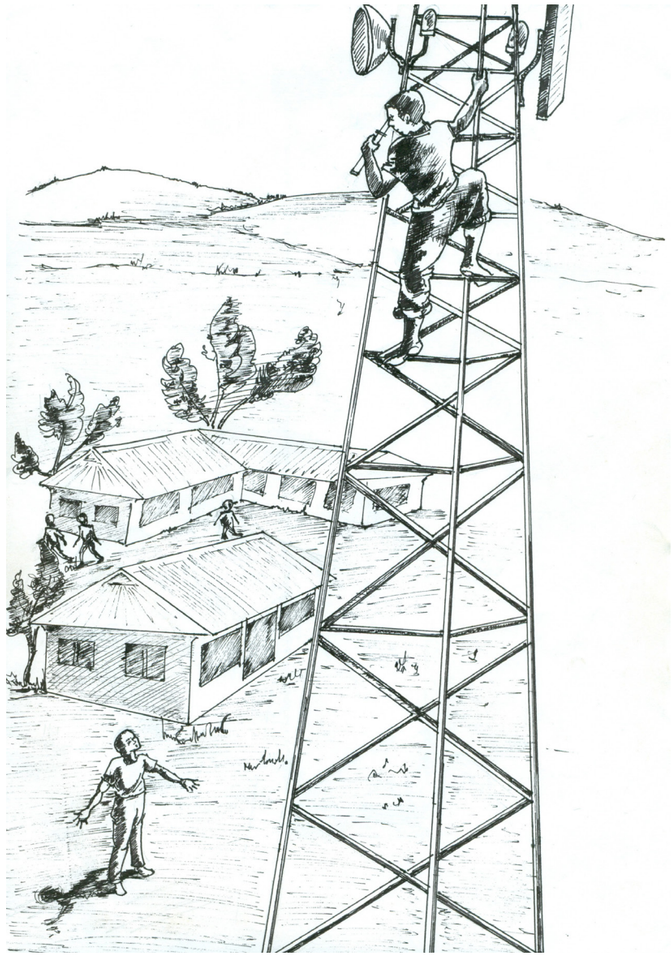
about their users to governments or hackers.) Some smartphones will give you some kind of control over whether apps can find out your physical location; a good privacy practice is to try to restrict which apps can see this information, and at a minimum to make sure that your location is only shared with apps that you trust and that have a good reason to know where you are.

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 also 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 theater, 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 subscribers' 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[84] (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're 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 have the ability to 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.

84 Aftenposten, Sources: We were pressured to weaken the mobile security in the 80's, http://www.aftenposten.no/verden/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-98459b.html , Accessed 9 February 2017

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's any way for the app developer to undo or bypass the encryption.

Infecting 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.

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.

SMARTPHONES: APPS AND PRACTICES FOR MOBILE SECURITY

Security recommendations for desktops and laptops equally apply to mobile phones . The steps needed here usually involve changing some phone settings, following best practices and using security-focused applications. Below we will review again our Five Security Goals as they relate to smartphones. In addition, mobile phones are useful tools to improve your operational security and effectiveness and we will look at some of the tools available for those goals. For more information about the security goals listed here, refer back to the main sections earlier in this booklet.

Most security-focused apps have been developed for Google's mobile operating system Android, however there are increasingly options available for Apple's iOS, while the Windows Phone system has largely been bypassed by the security developers community. All of the apps mentioned below are available for Android, and where there are iOS versions they will be mentioned.

Basic mobile device Security

Basic device security on a phone can be summarized over several action points:

Use a screen Lock

Activate a screen lock on your phone so that when it is picked up an attacker cannot access your applications, data, and accounts on your phone. Several varieties of screen locks can be activated: It may be a password, a numeric PIN, or a swipe-pattern. On newer phones it may even use your camera to look at your face or use your fingerprint to unlock it. Swipe pattern-unlocks are not recommended as your fingers tend to leave a trail of natural oils on the screen which can easily be read by someone trying to access your phone.

Additionally your phone will have settings that set the amount of time that needs to pass (a) before your screen blacks out, and (b) before the screen lock is activated. You should consider these settings and set them according to your own preferences of convenience and security.

Note that screen locks are a good first step but they cannot ultimately protect the contents of your phone. For that you should encrypt your smartphone hard drive, see below for more information.

Keep your phone up to date

Software on phones contain security flaws just like any other software. In order to keep up to date with the latest security patches, it is important that you are in the habit of installing updates for your phone's operating system and installed applications. Operating system updates can be done by checking for the appropriate section in your phone's Settings pages, while updates are usually controlled by the App Market you use. Whenever possible, activate automatic updating.

Unfortunately many Android phones lose official support and cease to receive security updates within a short period of time. In this case the only option to keep the device secure may be to purchase a newer model.

Do not install Apps from unofficial markets

Apps can contain malicious code and can steal data off your phone. While it is still possible for malicious apps to be approved on Google Play store or the Apple App store, you should still restrict yourself to official app stores such as those two and a few others such as Amazon Store, Samsung Store, and F-Droid.[85] Unofficial markets may help you to download free apps which cost money on other markets, but remember that you could still be paying the price of malware and loss of personal information.

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

Disable Bluetooth Discovery Mode

Depending on your phone's model, Bluetooth may remain in discovery mode at all times. This may make your phone vulnerable to various Bluetooth-based attacks. Most modern phones however require you to turn on discovery mode for only short periods and verify device pairing by entering a shared code.

85 F-Droid is an alternative app market which only hosts free and open source apps. Learn more and download the market app at www.f-droid.org , Accessed 9 February 2017

Security of data on your phone

Newer models of smartphones permit full disk encryption. Review the security section of your phone's settings to see if this is possible. Remember that without drive encryption, an attacker could bypass your screen lock by simply reading your smartphone's hard drive using specialized hardware.

With full disk encryption on your phone, your screen lock password becomes the only way to access its contents. Your phone may have additional settings that lock out an attacker after a certain number of access attempts. You may even be able to set the phone to erase the hard drive after a maximum number of attempts.

If your phone does not have an option for full disk encryption, you may still be able to encrypt data using apps. Some security-focused apps encrypt app data, such as Silence[86] (encrypts SMS) and CameraV[87] (encrypts photos).

Security of data traversing the Internet
A phone is obviously used for communication, yet as discussed above, mobile phone calls and SMS text messages are susceptible to interception. Instead you should use Internet-based applications on your phone for communications. While apps like Skype and Facebook Messenger will protect your communications from local attackers, your messages can still be stored and read on the servers of the service provider. Apps which are designed for security include Signal by Open Whisper Systems[88] (for Android and iPhone) which provide secure phone calls and instant messaging.

86 Silence, Need some privacy, https://silence.im/ , Accessed 9 February 2017

87 Google, CameraV: secure visual proof, https://play.google.com/store/apps/details?id=org.witness.informacam.app , Accessed 9 February 2017

88 Open whisper systems, https://whispersystems.org/ , Accessed 9 February 2017

To protect all of your Internet traffic and hide your location or identity from websites you can use a VPN for your smartphone. Psiphon[89] is a popular VPN application developed for activists needing to protect their Internet traffic. Another alternative is Betternet.[90] Opera also offers a free VPN app for Android and iPhones.[91] You may also subscribe to a paid VPN which often provides higher speeds.

Tor is like a VPN but also anonymises you to the circumvention network. Tor is available on your smartphone through two apps called Orbot[92] and Orweb.[93]

Security of Accounts

A mobile phone can help you keep your accounts secure too. By activating Two Factor Authentication on your online accounts, you will receive a text message every time a new device accesses one of your accounts. This way, even if an attacker steals your password, they still will not be able to log in with the password alone. If you travel often and know that you will not be able to connect to your home mobile network by roaming, you should install an Authenticator App. Google Authenticator is available for Android[94] and iOS.[95] This app will generate codes for you no matter where you are in the world, and you do not even need to be connected to the Internet for it to work. Facebook allows you to generate codes from within its own app.

A very useful resource to help you decide if your messaging application gives you security and privacy is the Electronic Frontier Foundation's Secure Messaging Scorecard.[96]

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:

Panic Button[97] is an application which can be triggered by tapping repeatedly on the power button. When triggered, the application will send SMS text messages to pre-selected contacts containing a pre-written message as well as your current GPS location. It is designed as an anti-disappearance application and is available for Android.

CameraV[98] is a photo and video application which uses cryptographic signing functions to combine media data with metadata such as location, surrounding wifi and bluetooth signals, and celltown data, to create non-repudiable evidence out of photographs. It is designed to reinforce the validity of cellphone photos and videos such that they could be presented and accepted in courts of law. It is available for Android.

Mobile Martus[99] is a data collector app which connects to the secure documentation database Martus.[100] It permits the user the send field reports securely into an existing documentation project then the report is securely erased from the phone immediately after sending. It is available for Android.

Umbrella[101] 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.[102]

89 Psiphon, keeping the web world wide, https://psiphon.ca , Accessed 9 February 2017

90 Betternet, Online security and privacy for all devices and platforms, https://www.betternet.co/ , Accessed 9 February 2017

91 Opera, Unblock the web for free, https://www.opera.com/apps/vpn , Accessed 9 February 2017

92 Guardian Project, Orbot, Tor for Android https://guardianproject.info/apps/orbot/ , Accessed 9 February 2017

93 Guardian Project, Orbot, Tor for Android https://guardianproject.info/apps/orbot/ , Accessed 9 February 2017

94 Google, Play, Google authenticator, https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en , Accessed 9 February 2017

95 https://itunes.apple.com/en/app/google-authenticator/id388497605?mt=8

96 Electronic Frontier Foundation, Secure messaging scorecard https://www.eff.org/secure-messaging-scorecard , Accessed on the 9 February 2017

97 Panic Button, Turns your mobile into a secret alarm, https://panicbutton.io/, Accessed 9 February 2017

98 Google play, CameraV secure visual proof https://play.google.com/store/apps/details?id=org.witness.informacam.app&hl=en , Accessed 9 February 2017

99 Google play, Mobile Martus, https://play.google.com/store/apps/details?id=org.martus.android&hl=en , Accessed 9 February 2017

100 Martus,Information is power, https://www.martus.org/ , Accessed on the 9th February 2017

101 Google play, Umbrella security made easy https://play.google.com/store/apps/details?id=org.secfirst.umbrella , Accessed 9 February 2017

102 https://secfirst.org/

RESOURCES

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

- **ACT Alliance Security Risk Assessment Tool**[103] - A tool to identify, evaluate, rate, and reduce or mitigate risks.
- **Front Line Defenders: Workbook on Security**[104] - Practical steps for HRDs at risk.
- **Protection International: guide for facilitators**[105] - Tool for people interested in facilitating training processes to develop protection capacities in HRDs.
- **Protection International: New protection manual for HRDs**[106] - Manual with additional knowledge and tools for HRDs to help them improve their understanding of security and protection.
- **Security in a Box**[107] - Tactics chapters and step-by-step guides on how to use many of the softwares discussed in this booklet. See also their Community Guides for African Environmental Rights Defenders[108] and Sexual Minorities.[109]
- **Surveillance Self-Defense**[110] - Chapters on protection against surveillance and how-to guides on software.
- **Digital First Aid Kit**[111] - A how-to guide to responding to various types of digital attacks.
- **SaferJourno**[112] - Digital security training manual specifically for teaching journalists.
- **Level-Up**[113] - Digital security training curriculum for trainers.
- **SAFETAG**[114] - Digital security auditing framework for security professionals.
- **VirusTotal**[115] - Scan file or URL link for malware.
- **The Digital First Aid Kit**[116] - Digital Defenders Partnership.
- **Umbrella**[117] - A free self-guided learning app available for Android.

103 ActAlliance, Security Risk Assesment Tool, http://actalliance.org/documents/act-alliance-security-risk-assessment-tool/, Accessed 18 April 2017

104 Frontline Defenders, Workbook on Security, https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk, Accessed 18 April 2017

105 Protection International, GUIDE FOR FACILITATORS, http://protectioninternational.org/publication/guide-for-facilitators/, Accessed 18 April 2017

106 Protection International, NEW PROTECTION MANUAL FOR HUMAN RIGHTS DEFENDERS, http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/, Accessed 18 April 2017

107 Security in a box, Digital security tools and tactics, https://securityinabox.org/en , Accessed 9 February 2017

108 Security in a box, Tools and tactics for environmental rights defenders in Sub-Saharan Africa, https://securityinabox.org/en/eco-rights-africa , Accessed 9 February 2017

109 Security in a box,Tools and tactics for the LGBTI community in Sub-Saharan Africa, https://securityinabox.org/en/lgbti-africa , Accessed 9 February 2017

110 Electronic Frontier Foundation, Surveillance self defense, https://ssd.eff.org/ , Accessed 9 February 2017

111 Digital Defenders Partnership,The digital first aid kit, https://www.digitaldefenders.org/digitalfirstaid/ , Accessed 9 February 2017

112 SaferJourno, Digital security resources for media trainers, https://saferjourno.internews.org/ , Accessed 9 February 2017

113 LevelUp, Resources for the global digital safety training community, https://www.level-up.cc/ , Accessed 9 February 2017

114 Safetag, A security audit frame work,Project of Internew, https://safetag.org/ , Accessed 9 February 2017

115 Virus total, Analyzes suspicious files and URLs, https://www.virustotal.com/ , Accessed 9 February 2017

116 Digital Defenders Partnership,The digital first aid kit, https://www.digitaldefenders.org/digitalfirstaid/, Accessed 9 February 2017

117 Google play, Umbrella security made easy https://play.google.com/store/apps/details?id=org.secfirst.umbrella , Accessed 9 February 2017

DefendDefenders (the East and Horn of Africa Human RIghts Defenders Project) seeks to strengthen the work of human rights defenders throughout the sub-region by reducing their vulnerability to riks of persecution and by enhancing their capacity to effectively defend human rights.

DefendDefenders is the secretariat of EHAHRD-Net, a network of 78 human rights organisations in the eleven countries of the East and Horn of Africa sub-region: Burundi, Djibouti, Eritrea, Ethiopia, Kenya, Rwanda, Somalia (together with Somaliland), South Sudan, Sudan, Tanzania, and Uganda.

www.defenddefenders.org

+256 393 265 820

info@defenddefenders.org

@ehahrdp

/defenddefenders