security in-a-box

community focus

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

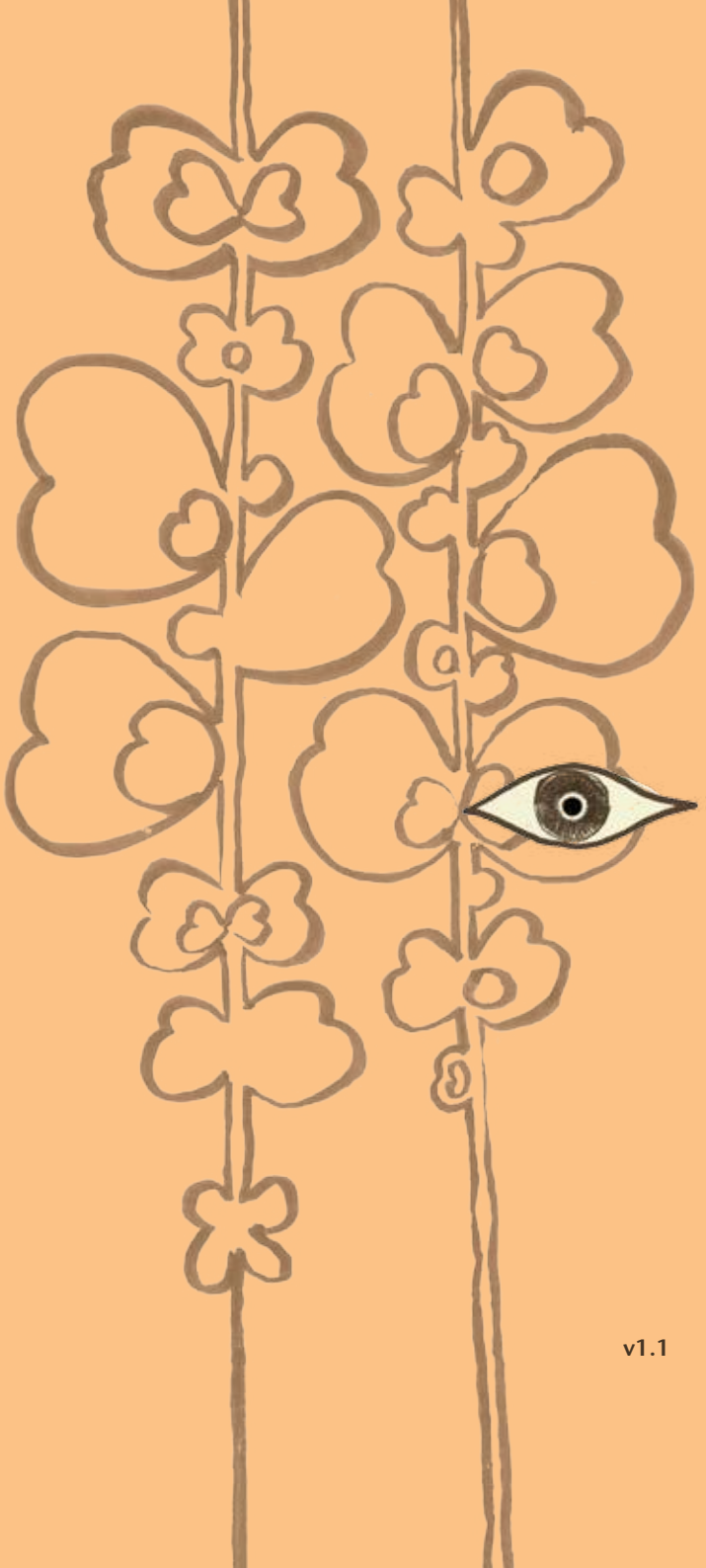
https://securityinabox.org
https://tacticaltech.org
https://frontlinedefenders.org

TACTICAL
TECHNOLOGY
COLLECTIVE

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

ISBN 978-90-81-76901-3

TOOLS AND TACTICS FOR ADVOCACY



v1.1

security in-a-box

community focus

digital security tools and tactics for the African LGBT community

TACTICAL TECHNOLOGY COLLECTIVE

TOOLS AND TACTICS FOR ADVOCACY

This guide was developed by
the Tactical Technology Collective

Coordination, writing & editing (Part I) Azeenarh Mohammed
Daniel Ó Clunaigh

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

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

Design & illustration Lynne Stuart

Funders American Jewish World Service
Swedish International Development Agency

v1.1: July 2014

CONTENTS

PART ONE: CONTEXT

PART TWO: HOW-TO BOOKLET

PART I:
Context

1
Introduction

Introduction

Welcome to **Security in-a-Box** Community Focus: digital security tools and tactics for the LGBTI community in sub-Saharan Africa.

Security in-a-box is a collaborative effort of the Tactical Technology Collective and Front Line Defenders. It was created to meet the digital security and privacy needs of advocates and human rights defenders. Security in-a-box includes a How-to Booklet, which addresses a number of important digital security issues. It also provides a collection of Hands-on Guides, each of which includes a particular freeware or open source software tool, as well as instructions on how you can use that tool to secure your computer, protect your information or maintain the privacy of your Internet communication.

This Community Focus edition is part of a series of guides which aim to further integrate digital security into the context of particular communities and human rights defenders. This edition was created in particular for Lesbian, Gay, Bisexual, Trans* and Intersex individuals and human rights defenders in the sub-Saharan region in Africa. It was preceded by a similar guide for the Arabic-speaking LGBTI community, and includes some of the same content. Both guides were written in collaboration with human rights defenders from the community.

The guide includes:

In most sub-Saharan African countries, LGBTI persons are still far from gaining social recognition. Despite the various social and cultural differences within the region, silence remains a factor that prevails whenever such taboo issues as homosexuality or trans identity are broached.

In recent years, LGBTI persons have indeed become more visible and active in the public sphere. Nonetheless, the State and society all too often force them back "into the closet" with threats of ostracization, harassment, physical violence and even death. Generally, LGBTI persons are still deemed to be at best non-existent, and at worst cursed, possessed, deviant, immoral, abnormal and diseased. With homosexual acts directly criminalized in most countries in the region, in some of which one can face the death penalty, it is already difficult for LGBTI persons to come out, be visible, live out their identities or fight for their rights. While these laws are often ineffective and are not used systematically to prosecute individuals, the social and cultural condemnations of homosexuality remain the biggest threat for LGBTI communities across the region.

In view of the aforementioned context, the Internet has emerged as a viable option for LGBTI persons to gain visibility, communicate, network, and express what one cannot express in public. Social networks, blogging platforms and forums have become, in most African countries, the only spaces where LGBTI persons can have a voice, organize themselves, formulate their discourses around their issues and fight for recognition.

However, authorities and other opponents of LGBTI rights have endeavored to keep up with this change. The Ugandan parliament introduced a bill initially prescribing the death penalty for same sex relationships while the Nigerian parliament prescribed a 14 year prison sentence for same sex relationships and 10 years for LGBTI activists or those who witness civil unions and same-sex marriages. These incidents drew regional and international attention and constituted a pivotal point for LGBTI activists and individuals in the region.

In the years following the proposal of the bills, Uganda had the first ever pride parade, queer Nigerians went to the legislature to defend their rights and groups, blogs and websites started springing up to defend LGBTI rights. Within the same timeline, a man was arrested in Cameroon for sending an SMS text message to another man that said "I am very much in love with you"; another was charged in Uganda with "trafficking obscene publications" because his stolen laptop contained gay porn. A gay man from Sierra Leone was attacked after he visited a gay site from an internet café, and young men in Nigeria formed 'punishment clubs' where they engage gay men on social networks and dating sites to extort, and blackmail their victims. These incidents started to expose the pitfalls of the Internet and the many insecurities and problems that come with its use for a community who at the same time feel liberated by it.

Social networks and dating websites remain a common way of targeting LGBTI persons, through accessing their personal pages (blogs, email addresses, Facebook or Twitter accounts); using their information and at times pictures to blackmail or 'out' them to their families, and setting up fake accounts, by police and others, to ambush LGBTI persons and ultimately arrest, threaten and scandalize them. The insecurities of information on the Internet are considerable in number, and despite the recent increase in awareness about the dangers of insecure usage of the Internet, access to the most practical solutions that could ensure digital safety for LGBTI users remains limited.

Consequently, there is an increasing and dire need for both knowledge of the most recent methods and tools for digital security, as well as a stronger ethos of caution and care in our online activities, through which LGBTI persons and human rights defenders could ensure their online privacy, circumvent governmental censorship and threats, and protect their information, personal pages, profiles and websites from being hacked, accessed, and ultimately used against them.

There is an inherent tension between the desire to claim one's rights openly and publically, and the desire to act cautiously and work out of the public eye. It is ultimately a personal decision to select a comfortable point in this range. However, we do believe that in all cases there is great value in studying security tactics to protect yourself, your colleagues, and your community.

With that in mind, we have created this guide in order to help contextualise digital security threats for LGBTI persons and human rights defenders from sub-Saharan Africa, as well as the tools and tactics that can be used for overcoming them.

The guide, which was designed and written in collaboration with the community it is intended to assist, serves an introduction to Tactical Technology Collective and Front Line Defenders' Security in-a-Box toolkit for human rights defenders and expands upon its content to include important contextual information, tools and tips particularly relevant to the LGBTI community, as identified by members of the community in workshops and other interactions in 2013 and 2014. The aim of the toolkit is to make the issue of digital security clearer and easier to understand and implement in the personal and professional context of LGBTI individuals from the region.

2
Digital threats to the African LGBTI community

1. Digital threats to the African LGBTI community

This section includes an overview of the situation of some of the threats and vulnerabilities faced by LGBTI human rights defenders and persons in the forty-seven sub Saharan African countries which arise from our use of computers, the Internet and mobile phones in order to carry out our work, establish networks and communities, and express our identities.

Marginalisation and attacks the LGBTI community in the region come in various forms and arise from, unfortunately, a widespread attitude of social and political hostility towards the community. In Africa, members of the LGBTI community face insults, threats and exclusion from family members on the discovery of their sexual orientation and gender identity status. LGBTI persons across the continent often find themselves victims of a witch-hunt mentality, led by family, community or State, and are desperate to conceal their identities or orientations lest they be targeted by homophobic compatriots.

Although there are exceptions, religious institutions, both Muslim and Christian, tend to also foster hostility towards the LGBTI community. Some religious leaders even preach against homosexuality and advise their followers not to accept the practice.

Because homosexuality is still viewed as "un-African" on a large part of the continent, politicians and religious leaders speak loudly against LGBTI groups to gain traction. Some religious leaders view homosexuality as a threat to traditional, socio-cultural and moral beliefs and values and perceive it as a negative western culture that should not be accepted. Other political campaigns translate into hateful demagoguery which is then used to get votes, and to distract people from their political, social, and economic failings. Such campaigns translate into violence, ostracism, and oppression that LGBT people have to face on a daily basis. In 2014, laws were passed in Nigeria and Uganda imposing harsher criminalisation of homosexuality, and were followed by campaigns of persecution from State and homophobic elements of society.

These are not the only threats faced by LGBTI persons on the continent. With the proilferation of mobile phones and smartphones, computers and Internet access in the region, LGBTI people have taken to these new means of communication in order to express their identities and build networks of contacts and communities. However, homophobic elements of State and society are also discovering

new means of attacking the community. Within the past few years, technology has also been used as a tool to attack LGBTI persons in Africa. The use of mobiles, social media platforms, email and dating sites in harassment, bullying, sexual violence, and even as a means of gathering evidence for prosecution is increasingly common. This section will outline the major risks from a digital security perspective faced by LGBTI persons in the region and link into chapters of the toolkit which can help us to avoid these kinds of attacks.

Among the most common digital threats faced by the community are:

ACCESS TO ACCOUNTS AND DEVICES

The problem:

Breach of privacy leading to 'outing' is one of the biggest fears some LGBTI persons face within the continent. A common way for this to happen is by having your computer or devices accessed by someone else who can then see the sensitive information stored on them. This information include your:

- pictures or videos,
- previous browsing history in phones and computers,
- dating apps,
- private email conversations,
- SMS or various chatting apps

Furthermore, "phishing" is also often used as a technique to trick unsuspecting users into handing over their passwords for e-mail or other personal accounts. This often takes the form of an e-mail, which looks as though it was sent by someone known to you, which usually invites you to download an attachment (often a virus) or click on a link where you are prompted to sign in to your e-mail or other account, and enter your password. If this information falls into the wrong hands, it could lead to our sensitive and personal information falling into the public domain, or worse.

Example incidents

In August 2012, the offices of Gays and Lesbians of Zimbabwe (GALZ) were raided by police and computers and other material was seized on suspicion of containing pornography or material insulting of the President. The materials were held for two years until GALZ won [1] a court case ordering their return in January 2014.

In Uganda in 2013, a 65-year-old businessman was arrested and charged with 'trafficking obscene publications' after his computer was stolen and gay pornography stored on it was discovered. The thieves passed the material to Uganda's *Red Pepper* newspaper which splashed details of the video on its front page under the headline: 'Exposed – Top City Tycoon's Sodomy Sex Video Leaks', and the material was subsequently passed to the police and used as a basis for his prosecution.

In January 2014, the offices of the LGBTI rights organisation "Alternative" in Côte d'Ivoire were attacked by an angry mob of local residents, and all their computers were stolen.

Staying safe

With increasing social and legal persecution of LGBTI people, we need to take action to protect our devices and accounts from unwanted access. Luckily, we can be much more secure by taking just a few simple steps:

- First, we should protect our devices and accounts with strong passwords with the help of programs like **KeePass**.
- We should use a trustable browser like Mozilla **Firefox** with Add-Ons and get to know its privacy settings. Or, we can use the **Tor** Browser which facilitates anonymous browsing online and which won't remember your browsing history.
- For even stronger security, we can encrypt our sensitive material, or our entire hard drives with programs like **TrueCrypt**. Full disk encryption is even built into many operating systems, such as Windows Professional, Mac OS X, many Linux systems, as well smartphone systems such as Android 4.0 or later, and iOS, although it often has to be activated manually.
- If you use internet on a shared computer or an Internet Caf È, ensure that when logging into your account you never activate the option for Remain logged in, Remember me or Save my password. Also, be sure to clear your browsing history, search history and browser cache if you were visiting any LGBTI-related pages.

Human Rights Defender Testimonies

"I really, really love TrueCrypt and I wish more people in the community can use it. I give my computer to my sister a lot and now I am no longer bothered about her finding anything she shouldn't. I put everything in a truecrypt file and after that, I use **CCleaner** *to wipe the computer before I give it to her. "*

Anonymous Human Rights Defender

"The people at the office are very excited about encryption. Everybody is now going around feeling and acting like 007. They even encrypt things on their flash drives. I see it when they give me a document on a flash, I just look at the size of the documents and it makes me smile. We talk about it and we laugh.
Anonymous Human Rights Defender

But it's not just about software. We also have to be on the lookout for suspicious mails and keep the following points in mind:

- If you receive an unexpected or suspicious mail, always verify with your contact whether they actually sent the mail.
- Never open or download a suspicious attachment unless you have verified that it is legitimate.
- Check the actual destination of links by hovering over them with your cursor.
- NEVER send your e-mail or other account password to anyone.
- NEVER enter your e-mail or other account password on any login page which appears after following a link in an email.
- ALWAYS ensure that you are on the legitimate login page of your email or other account by checking the URL carefully at the top of the screen.

EVIDENCE FOR PROSECUTION

The problem

Although arrest and detention without trial are common, until recently, arrests that lead to prosecution were rare; only a handful of cases have been recorded in the past decade within the region. The police are, however, beginning to rely on emails, text messages, and documents contained in an individual's computer to gather proof for prosecution. In some cases, the police have also been known to use this evidence to extort money from the individuals.

Example incidents

In 2011, Jean Claude Roger Mbede [2]**, a Cameroonian LGBT human rights defender was arrested for sending an SMS to another man saying, "I'm in love with you." When the text message fell into the hands of the police, he was arrested on suspicion of homosexuality, and subsequently found guilty and sentenced to three years in prison.**

Human Rights Defender Testimonies

"Cellphones are used a lot, especially text messages, and they've been used for cases against people who get arrested. If you are an activist, and you get arrested and your phone is taken away, they use your messages to build a case against you. Also civilians: sometimes if a relationship breaks up and one person does not want to let go, for example in a place like Cameroon... even if I'm a lesbian, and I go to the police and say "look at this person, she's a lesbian, she's been bothering me, look at these messages she's been sending me...". They're gonna arrest the person, and they don't care about me. If you have money to pay them, especially. They won't look at what I sent to the person, but what the person sent me, and build a case."
Anonymous Human Rights Defender

Staying safe:

Protecting ourselves is not just about protecting our own data, but that of our communities too. Knowing how to communicate securely is more important than ever, as many popular platforms like WhatsApp, Facebook and others are not designed with user privacy in mind. However, there are alternatives:

- We can **chat securely** over our mobile devices using apps like **TextSecure** and **ChatSecure**.
- We can chat and **make voice and video calls online securely** with our contacts using programs like **Jitsi**.
- We can **encrypt our emails** and make them inaccessible to unwanted eyes by using **Gpg4usb** or **Thunderbird with Enigmail**.
- We can even get off insecure platforms like facebook and **explore alternatives** such as **Crabgrass**.

This way, you can reduce the risks of having emails intercepted or accessed, and establish secure communications with people in your network.

Human Rights Defender Testimonies

"I love that encryption! I love it! The idea that you can relate with someone without a third party knowing what is happening, you can code your languages, your communication, wow! [...] I came to find that when we communicate with each other there is a 'Big Brother' somewhere who somehow [can get] this information. Jitsi enables the coding of this information so even that 'Big Brother' cannot decode it. It's useful because it makes your communication private, so it's just between you and the person you're addressing."
Anonymous Human Rights Defender

"Last month, an ex of mine outed me to my family. My mother was very curious but she had no proof. Because my phone and computer had a password, she could not check anything without me being there. When I noticed she liked to look over my shoulder, I cleaned all my browsing history and put all my pictures and videos inside a TrueCrypt file. I was using TextSecure so all my messages were safe. [...] Also, because my ex had shared her password with me, it was easy to delete everything on her phone when we broke up: pictures, texts, emails. I am now very happy that I learned not to share my password!"
Anonymous Human Rights Defender

ENTRAPMENT AND EXTORTION

The problem

Dating sites and social networks have provided members of the LGBTI community with new potential for communicating and establishing partnerships, networks and communities. However, these tools are also being used by homophobic elements of the State and society to entrap LGBTI people and subject them to humiliation, extortion, or even violence. Attacks are increasingly common whereby individuals or groups — be they civilian or police — set up fake profiles on gay dating sites or social networks and use them to lure people into meetings. Users of the site may unwittingly believe they are arranging to meet someone like them, but upon meeting they are attacked.

Example incidents

In Nigeria, police and ordinary citizens set up profiles on dating sites to attract gay men. In 2012, a newspaper article appeared to glorify one of such groups that had set up a punishment group that trapped and specialized in extorting gay men. 'We call them up, set a meeting in a hotel room then snap pictures in compromising positions. We then use this to collect money from them' said one of the young men.

The Gay and Lesbian Coalition of Kenya [3] **say incidents of blackmail and extortion are high and constantly growing within the country and accounts for one of the highest crimes commited against LGBTI persons.**

Human Rights Defender Testimonies

"If you go on some social network and you let people know you're a lesbian, or even if you don't and some guy would just pretend that he's a girl and you think you're talking to a girl, you start exchanging pictures and he keeps all the pictures. He would even send a nude picture of a girl! I met someone on Badoo once, we were talking, so I said 'give me your number' but I couldn't call immediately. So later I called and it was a guy's voice!"
Anonymous Human Rights Defender

"We had an intern recently who met somebody on facebook, and they invited him and the person pretended that he was a partner. He went for an appointment and met 5 other people other than this one, it was in an isolated part of town. He got beaten silly, he got stripped naked and photographed naked, they threatened that they would put that on Facebook, and they took all the money he had on him and his phones as well. And it wasn't possible to report to the police because then the story would all come out and they would be worse off for it."
Anonymous Human Rights Defender

Staying safe:

Avoiding snooping and entrapment on dating sites and social networks is partly technical, but is mostly to do with our behaviour:

- For a start, it's a good idea to only connect to dating sites securely and anonymously such as through using the **Tor Browser**
- Or as a minimum, by enabling the **HTTPS Everywhere** add-on to our **Firefox** browser.
- It's important to delete our browsing history and cookies after each session, or have them disabled to begin with.

However, most of the solutions are behavioural, not technical. You should never associate any identifiable information of yours on a dating site. You must also be very careful when exchanging pictures and only do so once significant trust has been established. And your first meetings should only be in a safe, public place.

Human Rights Defender Testimonies

"I get targeted as a woman especially as an older woman usually on Facebook with people who might have checked my profile and seen "Interested in: women". In the past I didn't even know how to delete someone from my friends list or from my Skype but after a training I sat down and sifted through my friends list and removed the ones I felt I did not know and including those who have been harassing me. [...] Facebook is very deceptive because people put up fake pictures and pretend to be someone else. What made me able to handle those kind of infiltrations was first to check for how long the person has been

registered. Then if they are a new registeration, I start to wonder why are they trying to friend me. Secondly, there are people you only have one common friend and that common friend is so remote, so that is also a bad sign. Then when I go to photos and I see only one photo or 4 photos maximum, ahhh! Sometimes, I see that they are all profile pictures of different people and those people don't even look the same. It gives me a hint that the photos have been stolen or photoshopped to give people a false impression that. I have learnt to really check before giving people access to me."
Anonymous Human Rights Defender

HARASSMENT, PHYSICAL AND SEXUAL ATTACKS:

The problem

Within the sub-Saharan African region, members of the LGBTI community face insults, threats and exclusion from family members on the discovery of their sexual orientation and gender identity status. Moreover, our identities and work often fly in the face of heteronormative social structures and misogyny. As a result, the violence faced by LGBTI people is structural, physical, and often sexualised. Harassment, violence, rape, and in some cases murder have been recorded against members of the community.

Now, many of these threats have expanded into the online space. Online bullying is a form of harrasment which may include repeatedly taunting, ganging up, threatening, or name calling individuals to cause harm or discomfort. Because of the proliferation of social networking and communication platforms, and the fact that people often feel anonymous when using them, online and social media bullying are very prevalent and LGBTI persons and groups are not exempt from it. On the contrary, a lot of people have been 'outed' to their family because of their posts and behaviour online while others have been harrassed for being LGBTI, posting LGBTI-related content or showing support for the community. Seemingly random conversations have been known to turn into homophobic threads and in some situations, what begins as online harassment turns into real-life violence.

Example incidents

In 2013, an 18-year-old Senegalese girl was forced to flee [4] the country after video footage of her kissing another girl was uploaded to the internet and the story spread. In Senegal, the punishment for same-sex sexual activity is up to five years in prison and fines of up to $3000.

Human Rights Defender Testimonies:
"[Sometimes on] twitter, someone will just send you a Direct Message and try to lure you out [of the closet]. And once you admit, "fine, I'm this way", then they post out your whole messages, and people go "oh this lesbian, so disgusting...". Some people try to open your phone, just to see what you have in your text messages, they want to see your mail, and this is a kind of digital attack."
Anonymous Human Rights Defender

Smartphone chat apps like WhatsApp, Viber, or 2go can access our phone numbers and provide them to the whole world without our permission and give potential harrassers direct access to us. Some apps also encourage us to share our location information and who we are with; this information could also be used to facilitate an attack.

Staying safe

For more on how to keep your phones safe, keep your browsing history to yourself and avaoid sharing your location information that may lead to attacks, see the chapters that follow.

Regarding harassment, as a general rule, it is advisable not to engage in arguments with people online who only want to spread hate because your discomfort encourages them to continue. It is also unwise to share or confirm intimate details about yourself with unknown persons as they can use that to target you. More technical and behavioural solutions which can be employed to minimise the effect of online bullying. For more, see: ***Chapter 10: How to protect yourself and your data when using social networking sites***

MALWARE INFECTION

The problem:

Access to technology and education on how computers work and how to use them in the most hygenic way is quite limited in the region. Most people learn to use computers "by doing" and don't get much theoretical background on how computers work, and basic measures to keep a computer healthy - that is to say, free of malicious software. This is exagerrated by a number of factors. In particular, due to limited resources, a number of us are unable to obtain registered copies of proprietary software such as Microsoft Windows or Microsoft Office, and instead rely on "cracked" or unlicensed versions. Many of these "cracked" softwares are themselves malicious, or at best, they leave us vulnerable to malware infections. Furthermore, many of us rely on using internet cafés for access to the internet, and are unaware of whether or

not the computers are infected. This can have a very damaging effect, as infection of our computer or USB memory devices can lead to data loss, or facilitate spying on our activities.

"Phishing" is also often used as a technique to trick unsuspecting users into handing over their passwords for e-mail or other personal accounts. This often takes the form of an e-mail, which looks as though it was sent by a person or company known to you, which usually invites you to download an attachment (often a virus) or click on a link where you are prompted to sign in to your e-mail or other account, and enter your password. If this information falls into the wrong hands, it could lead to our sensitive and personal information falling into the public domain, or worse.

Example incidents

In 2014 in Uganda, a number of LGBTI human rights organisations received suspicious e-mails, which appeared to be from colleagues in the human rights movement, which invited them to click on links wherein they were prompted to hand over the passwords to their accounts. The human rights defenders luckily double-checked with their colleagues whether they had actually sent the mails, which they had not: they were in fact victims of the Zeus malware [5]**, which spreads through accessing individuals' accounts and sending emails to their contacts, and is often used to access personal accounts such as online banking services. This simple act of verification saved many of them from malware infection and a potentially very damaging breach of privacy.**

Staying safe

To be more effective advocates, we must protect our information from malware and hackers. It's important for us to make use of Free and Open Source (**FOSS**) operating systems (like Linux) and programs (like Mozilla Firefox): these programs are free and regularly updated, and so offer increased security to users regardless of their resources. It's also fundamental to have updated Anti-Virus and Anti-Spyware programs like **Avast!** or **Spybot**.

Human Rights Defender Testimonies

"We have been worried about viruses . We got the free anti-virus and anti-spyware, and this has helped secure us. I think this is the longest period we have not had to bring any computer engineer into our office to check our computers, just blowing air into it, and installing all sorts of software to clean, reformat and all that. We used to lose so much through those reformatting processes because when we don't have access, we go to internet cafés and we pick viruses from there and they end up in our system: then all kinds of trouble will start. But since we were trained and the access we got to free anti virus, anti spyware, and our general change of attitude in the office, we have not invited anybody: not once to come into our offices and check the stomach of our computers."
Anonymous Human Rights Defender

However, it's not just about software. We also have to be on the lookout for suspicious mails and keep the following points in mind:

- If you receive an unexpected or suspicious mail, always verify with your contact whether they actually sent the mail.'
- Never open or download a suspicious attachment unless you have verified that it is legitimate.
- Check the actual destination of links by hovering over them with your cursor.
- NEVER send your e-mail or other account password to anyone.
- NEVER enter your e-mail or other account password on any login page which appears after following a link in an email.
- ALWAYS ensure that you are on the legitimate login page of your email or other account by checking the URL carefully at the top of the screen.

For more, see:

- How to protect your computer from malware and hackers
- How to keep your internet communication private

MONITORING AND TRACKING

The problem

A large number of activities we used to conduct offline have now been moved online. Such examples include banking, shopping, surveys and tests, socialising and sharing ideas. Both personal and seemingly random data that are continuously required by governments (biometric registration), mobile phone companies, company databases, 'random surveys', gaming companies and mobile apps have been confirmed by the Snowden leaks in 2013 to be tools used by companies and governments to gather data en masse about us, which can lead to targeted surveillance and attacks.

The aggregation and analysis of data related to our use of services have made it possible to predict our traits and attributes. In 2013, Michal Kosinski developed [6] a mathematical tool that can predict

an individual's traits like age, sex, sexual orientation, religion and political leanings using their Facebook 'likes' alone. With such tools being available to businesses and governments alike, it is easy to see the possibility of abuse and targeting of LGBTI groups and persons especially in countries where such activities are criminalised. The various services that can be used to build a profile of our interests, habits and characteristics, include our social network accounts, online banking, online commerce, and smartphone apps.

Furthermore, the rapidly-growing surveillance industry is continuously making remote intrusion and surveillance products available to States. Nigeria and Ethiopia are among the first in Africa that have been exposed [7] for purchasing and using these tools.

Human Rights Defender Testimonies:

"Digital Security is extremely important for human rights lawyers and LGBTI activists in this part of the world. In Nigeria for example, the government has employed the services of cyber security gurus from Israel and other developed countries to hack into and gather intelligence from hapless and ignorant citizens, especially human rights activists, to be able to gain knowledge of their work, their communication and track down their activities."
Anonymous Human Rights Defender

"The state has interest in accessing information relating to our work, and mainly our databases. This includes through confiscation of computers, but also phone tapping, surveillance, and interfering with our Internet Service Provider"
Anonymous Human Rights Defender

Staying safe

A helpful rule of thumb is to share identifying data on social platforms only on a need-to-know basis. However, some information is created and communicated by our very use of the Internet, which can include our browsing history or even our location information. To avoid this, we must consider using software which helps to anonymise our online activities, such as the **Tor Browser**, or even **Tails** which is an easy-to-use bootable operating system which you can run from a flash drive.

Human Rights Defender Testimonies

"We use Tor Browser a lot to remain anonymous when we are getting in touch with other MSM men. That is because you never know who is watching what sites you are going to. All my searches on google used to show on my history but with Tor, that is not the case."
Anonymous Human Rights Defender

"I use Tor every day. I also use Orbot on my phone so I always enjoying being anonymous when using the phone or computer."
Anonymous Human Rights Defender

For more, see:

- How to remain anonymous and bypass censorship on the Internet
- How to protect yourself and your data when using social networking sites

LINKS

[1] *http://www.galz.co.zw/?p=1109*
[2] *http://wikipedia.org/wiki/Jean-Claude_Roger_Mbede*
[3] *http://irasciblemusings.com/nairobi-police-say-closeted-gays-being-blackmailed-and-attacked-by-gangs-2/*
[4] *http://newsone.com/2768476/senegal-anti-gay-law-africa-homosexuality/*
[5] *https://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29*
[6] *http://www.pnas.org/content/early/2013/03/06/1218772110*
[7] *https://citizenlab.org/wp-content/uploads/2014/02/SUN_NOON_WORLD1.jpg*

3
How to assess your digital security risk

3. How to assess your digital security risk

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

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

'SECURITY' AND 'DIGITAL SECURITY'

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

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

This guide focuses on one subset of 'security', which we call 'digital security'. Digital security refers to ensuring the ability to use digital information and information systems without interference, disruption, unauthorised access or data collection. That is to say, having control over the storage, communication, use and access of our digital information. Sometimes, we may want to share information publicly in order to stay safe: for example, you may share your location with your friends and support network via text message or a social network if you find yourself being followed. Other times, we may want to keep information secret in order to stay safe: for example, we may encrypt our email conversations with our colleagues when organising a meeting, so that the location isn't discovered.

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

'THE WHO' AND 'THE WHY'

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

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

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

Resisting forces

Unfortunately, as human rights defenders, we cannot always count on the full support of our State, our society, or at times even our families. Our work to promote and defend human dignity is often a direct challenge to power structures, whether in government, society or the family, and directly threatens those who currently weild that power. Moreover, as women human rights defenders, or LGBTI human rights defenders, we often challenge long-standing patriarchal, 'cultural' or 'traditional' norms which are jealously guarded by individuals and institutions alike.

This means that a number of different actors may take action against us to hinder or stop our work. In some cases it may be agents of the State, who often threaten, stigmatise, arrest, detain, mistreat and prosecute human rights defenders. In other cases, it may be social actors – religious institutions or groups, political movements, armed groups, or even family members – who try to prevent us from promoting and defending human rights.

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

Supporting forces

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

Unknown forces

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

Assessing Risk

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

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

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

Capacities and vulnerabilities are often "two sides of the same coin".

Identifying threats, capacities and vulnerabilities

To begin with, as noted above, it's good to consider the threats we face. Threats may be targeted, that is to say, directly or indirectly related to

our work; or they may be incidental, that is to say, not related to our work but other factors, such as common delinquency.

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

It's a good idea to, on your own or with others, do a brainstorm of the possible threats you face, and consider how they might relate to your use of technology – your mobile phone, your computer, your smartphone, email, social networks, and so on.

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

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

Threats	Who?	Vulnerabilities	Capacities	Capacities required

An example for an LGBT human rights defender might look like this:

Threats	Who?	Vulnerabilities	Capacities	Capacities required
Office raid, confiscation, legal action	Police, judiciary	Sensitive files are not protected, Computers have unregistered copies of windows, LGBT material in browsing history	Backups are regular and kept outside the office	Hiding sensitive information Using Free Software Deleting information securely
Entrapment and assault	Homophobic gangs	Dating website profile is public, with face pictures	Always carry mobile: text friends where & when I meet someone	Safer use of dating sites
Burglary	Local delinquents	Old locks on office doors, organisation smartphones not kept in a safe place	Smartphones have SIM lock and no social networking apps	Smartphone encryption, and a safe place to keep them

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

THE 'RISK MATRIX': PROBABILITY AND IMPACT

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

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

PROBABILITY				
Very High				
High				
Medium				
Low				
IMPACT	Low	Medium	High	Catastrophic

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

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

Plot the threats on the materix according to your judgement of their probability and impact. An example might look like this:

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

Once you have prioritised the risks to yourself and your work, you can

then start to take action to reduce them through building the relavent capacities and integrating them into a security plan.

FURTHER READING AND REFERENCES

For more information on risk assessment and security planning, including not only digital but physical, organisational and psychological well-being, see the following resources:

- *Front Line Defenders' Workbook on Security for Human Rights Defenders* in English and Arabic
- Protection International's *New Protection Manual for Human Rights Defenders*, 3rd Edition
- Protection International's *Protection Manual for LGBTI Defenders*
- Electronic Frontier Foundation: *Risk Management as part of the Surveillance Self Defence project*.
- Front Line Defenders, Kvinna till Kvinna and Urgent Action Fund, *Insiste, Resiste, Persiste, Existe – Women Human Rights Defenders Security Strategies*

LINKS

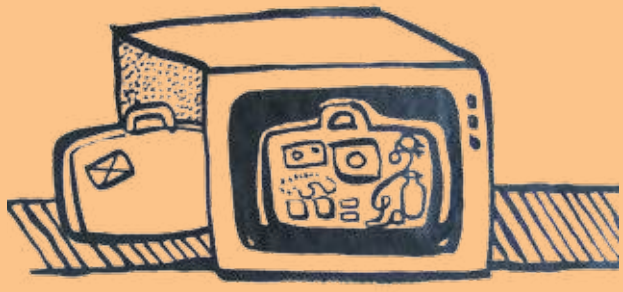
[1] ***Kvinna till Kvinna, Integrated Security Manual, http://integratedsecuritymanual.org/***
[2] ***www.frontlinedefenders.org/files/workbook_eng.pdf***
[3] ***www.frontlinedefenders.org/files/workbook_ar.pdf***
[4] ***http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/***
[5] ***http://protectioninternational.org/publication/protection-manual-for-lgbti-defenders-2nd-edition/***
[6] ***https://ssd.eff.org/risk***
[7] ***https://ssd.eff.org/***
[8] ***www.frontlinedefenders.org/files/en/Insiste%20Resiste%20Persiste%20Existe.pdf***

PART II:

How-to Booklet

1

How to protect your computer from malware and hackers



1. How to protect your computer from malware and hackers

Regardless of your broader objectives, keeping your computer healthy is a critical first step down the path toward better security. So, before you begin worrying too much about strong passwords, private communication and secure deletion, for example, you need to make sure that your computer is not vulnerable to **hackers** or plagued by malicious software, often called **malware**, such as viruses and spyware. Otherwise, it is impossible to guarantee the effectiveness of any other security precautions you might take. After all, there is no in point locking your door if the burglar is already downstairs, and it doesn't do you much good to search downstairs if you leave the door wide open.

Accordingly, this chapter explains how to maintain your software and use tools like **Avast**, **Spybot** and **Comodo Firewall** to protect your computer against the ever-present dangers of malware infection and **hacker** attacks. Although the tools recommended in this chapter are for Windows, which is the operating system most vulnerable to these threats, **GNU/Linux** and Apple OS X users are also at risk and should still adopt the tactics presented below.

What you can learn from this chapter

- More about the nature of a few of the specific threats that **malware** poses to the privacy and integrity of your information, the stability of your computer and the reliability of other security tools
- How you can use a number of recommended tools to help protect yourself from these threats
- How to keep your computer secure by updating your software frequently
- Why you should use **freeware** tools, to avoid the dangers associated with expired licenses or pirated software, and popular **FOSS** tools, where possible, to enhance your security.

VIRUSES

There are many different ways to classify viruses, and each of these methods comes with its own set of colorfully-named categories. Worms, macroviruses, trojans and backdoors are some of the more well-known examples. Many of these viruses spread over the Internet, using email, malicious webpages or other means to infect unprotected computers. Others spread through removable media, particularly devices like USB memory sticks and external hard drives that allow users to write information as well as reading it. Viruses can destroy,

damage or infect the information in your computer, including data on external drives. They can also take control of your computer and use it to attack other computers. Fortunately there are many anti-virus tools that you can use to protect yourself and those with whom you exchange digital information.

Anti-virus software

There is an excellent **freeware** anti-virus program for Windows called **Avast**, which is easy to use, regularly updated and well-respected by anti-virus experts. It requires that you register once every 14 months, but registration, updates and the program itself are all free-of-charge.

Hands-on: Get started with *Avast! – Anti-Virus*

There are various other well-known commercial anti-virus programs as alternatives to Avast. **Clam Win** is a **FOSS** alternative to **Avast**. Although it lacks certain features that are important for a primary anti-virus program, Clam Win has the advantage that it can be run from a USB memory stick in order to scan a computer on which you are not allowed to install software.

Tips on using anti-virus software effectively

- Do not run two anti-virus programs at the same time, as this might cause your computer to run extremely slowly or to crash. Uninstall one before installing another.
- Make sure that your anti-virus program allows you to receive updates. Many commercial tools that come pre-installed on new computers must be registered (and paid for) at some point or they will stop receiving updates. All of the software recommended here supports free updating.
- Ensure that your anti-virus software updates itself regularly. New viruses are written and distributed every day, and your computer will quickly become vulnerable if you do not keep up with new virus definitions. Avast will automatically look for updates when you are connected to the Internet.
- Enable your anti-virus software's 'always on' virus-detection feature if it has one. Different tools have different names for it, but most of them offer a feature like this. It may be called 'Realtime Protection,' 'Resident Protection,' or something similar. Take a look at *Section 3.2.1* of the *Avast Guide* to learn more about that tool's 'Resident Scanner.'
- Scan all of the files on your computer regularly. You don't have to do this every day (especially if your anti-virus software has an 'always on' feature, as described above) but you should do it from time to time. How often may depend on the circumstances. Have you connected your computer to unknown networks recently? With whom have you been sharing USB memory sticks? Do you frequently receive strange attachments by email? Has someone else in your home or office recently had virus problems? For more information on how best to scan files, see the *Avast Guide*.

Preventing virus infection

- Be extremely cautious when opening email attachments, any files received (e.g. over Instant Messaging like MSN, Skype, etc.) or downloaded from the Internet. It is best to avoid opening any files received from an unknown source. If you need to do so, you should first save the attachment to a folder on your computer, then open the appropriate application (such as Microsoft Word or Adobe Acrobat) yourself. If you use the program's File menu to open the attachment manually, rather than double-clicking the file or allowing your email program to open it automatically, you are less likely to contract a virus.
- Consider the possible risks before inserting removable media, such as CDs, DVDs and USB memory sticks, into your computer. You should first check that your anti-virus program has the latest updates and that its scanner is running. It is also a good idea to disable your operating system's 'AutoPlay' feature, which can be used by viruses to infect your computer. Under Windows XP, this can be done by going inside My Computer, right-clicking on your CD or DVD drive, selecting Properties and clicking on the AutoPlay tab. For each content type, select the Take no action or Prompt me each time to choose an action options then click OK.
- You can also help prevent some virus infections by switching to free and open source software, which is often more secure, and which virus writers are less likely to target.

However, just an anti-virus isn't enough to keep your computer healthy. We also need to protect our computers from Malware and hackers, so we'll need to install a couple of other tools too.

SPYWARE

Spyware is a class of malicious software that can track the work you do, both on your computer and on the Internet, and send information about it to someone who shouldn't have access to it. These programs

can record the words you type on your keyboard, the movements of your mouse, the pages you visit and the programs you run, among other things. As a result, they can undermine your computer's security and reveal confidential information about you, your activities and your contacts. Computers become infected with spyware in much the same way that they contract viruses, so many of the suggestions above are also helpful when defending against this second class of malware. Because malicious webpages are a major source of spyware infection, you should pay extra attention to the websites you visit and make sure that your browser settings are secure.

Spyware may sound like something from a spy movie, but it is much more common than it sounds. In particular, if you have been using a Windows computer and regularly use Internet Explorer for browsing, there's a good chance that you may have downloaded a spyware or been affected by a malicious webpage.

Anti-spyware software

You can use anti-spyware tools to protect your computer from this type of threat. Spybot is one such program, and it does a very good job of identifying and removing certain types of malware that anti-virus programs simply ignore. Just like with anti-virus software, though, it is extremely important that you update Spybot's malware definitions and run regular scans.

Hands-on: Get started with *Spybot – Anti-Spyware*

Preventing spyware infection

- Stay alert when browsing websites. Watch for browser windows that appear automatically, and read them carefully instead of just clicking Yes or OK. When in doubt, you should close 'pop up windows' by clicking the X in the upper right-hand corner, rather than by clicking Cancel. This can help prevent webpages from tricking you into installing malware on your computer.
- Improve the security of your Web browser by preventing it from automatically running the potentially dangerous programs that are sometimes contained within webpages you visit. If you are using Mozilla **Firefox**, you can install the **NoScript** add-on, as described in *Section 4* of the *Firefox Guide*.
- Never accept and run this sort of content if it comes from websites that you don't know or trust.

You may have also come across terms such as 'Java applets' and 'ActiveX controls': these are small programs that your Web browser sometimes downloads along with whatever page you're reading. WEb designers use them to create complex sites, but they can also spread viruses and spyware. You don't have to to worry too much about how they actually work, as long as you have NoScript installed and running propperly.

Example incidents

In 2014 in Uganda, a number of LGBTI human rights organisations received suspicious e-mails, which appeared to be from colleagues in the human rights movement, which invited them to click on links wherein they were prompted to hand over the passwords to their accounts. The human rights defenders luckily double-checked with their colleagues whether they had actually sent the mails, which they had not: they were in fact victims of the Zeus malware [5], which spreads through accessing individuals' accounts and sending emails to their contacts, and is often used to access personal accounts such as online banking services. This simple act of verification saved many of them from malware infection and a potentially very damaging breach of privacy.

Human Rights Defender Testimonies

"We have been worried about viruses . We got the free anti-virus and anti-spyware, and this has helped secure us. I think this is the longest period we have not had to bring any computer engineer into our office to check our computers, just blowing air into it, and installing all sorts of software to clean, reformat and all that. We used to lose so much through those reformatting processes because when we don't have access, we go to internet cafés and we pick viruses from there and they end up in our system: then all kinds of trouble will start. But since we were trained and the access we got to free anti virus, anti spyware, and our general change of attitude in the office, we have not invited anybody: not once to come into our offices and check the stomach of our computers."

Anonymous Human Rights Defender

FIREWALLS

A firewall is the first program on a computer that sees incoming data from the Internet. It is also the last program to handle outgoing information. Like a security guard, posted at the door of a building to decide who can

enter and who can leave, a firewall receives, inspects and makes decisions about all incoming and outgoing data. Naturally, it is critical that you defend yourself against untrusted connections from the Internet and from local networks, either of which could give hackers and viruses a clear path to your computer. In fact, though, monitoring outgoing connections originating from your own computer is no less important.

A good firewall allows you to choose access permissions for each program on your computer. When one of these programs tries to contact the outside world, your firewall will block the attempt and give you a warning unless it recognizes the program and verifies that you have given it permission to make that sort of connection. This is largely to prevent existing malware from spreading viruses or inviting hackers into your computer. In this regard, a firewall provides both a second line of defense and an early-warning system that might help you recognize when your computer's security is being threatened.

Firewall software

Recent versions of Microsoft Windows include a built-in firewall, which is now turned on automatically. Unfortunately, the Windows firewall is limited in many ways, for example, it does not examine outgoing connections. However, there is an excellent **freeware** program called **Comodo Personal Firewall**, which does a better job of keeping your computer secure.

Hands-on: Get started with *Comodo Personal Firewall*

- Remember, don't run two anti-virus programs or two firewalls at the same time.

Preventing untrusted network connections

- Only install essential programs on the computer you use for sensitive work, and make sure you get them from a reputable source. Uninstall any software that you do not use.
- Disconnect your computer from the Internet when you are not using it and shut it down completely overnight
- Do not share your Windows password with anyone.
- If you have enabled any 'Windows services' that you are no longer using, you should disable them. See the *Further reading* section for more
- Make sure that all of the computers on your office network have a firewall installed
- If you do not already have one, you should consider installing an additional firewall to protect the entire local network at your office. Many commercial broadband **gateways** include an easy-to-use firewall, and turning it on can make your network much more secure. If you are not sure where to start with this, you might want to ask for assistance from whoever helped set up your network.

KEEPING YOUR SOFTWARE UP-TO-DATE

Computer programs are often large and complex. It is inevitable that some of the software you use on a regular basis contains undiscovered errors, and it is likely that some of these errors could undermine your computer's security. Software developers continue to find these errors, however, and release updates to fix them. **It is therefore essential that you frequently update all of the software on your computer, including the operating system**. If Windows is not updating itself automatically, you can configure it to do so by clicking the **Start** menu, selecting **All Programs** and clicking **Windows Update**. This will open Internet Explorer, and take you to the Microsoft Update page, where you can enable the **Automatic Updates** feature. See the *Further reading* section to learn more about this.

Similarly it is important to make sure that all of the other software installed on your computer is updated. In order to do it you first need to know what programs you have on your computer and perhaps uninstall those that are not essential (on Windows go to Control Panel and **Programs** or **Add/Remove Programs**). Then it is good to review for each program if it is the latest version, how can it be updated and will it update itself automatically in the future.

Staying up-to-date with freeware and FOSS tools

Proprietary software often requires proof that it was purchased legally before it will allow you to install updates. If you are using a pirated copy of Microsoft Windows, for example, it may be unable to update itself, which would leave you and your information extremely vulnerable. By not having a valid license, you put yourself and others at risk. Relying on illegal software can present non-technical risks, as well. The authorities in a growing number of countries have begun to verify that organisations possess a valid license for each piece of software that they use. Police have confiscated computers and closed down organizations on the basis of 'software piracy.' This justification can be abused quite easily in countries where the authorities have political reasons to interfere with a given organisation's work. Fortunately, you do not have to purchase expensive software to protect yourself from tactics like this.

We strongly recommend that you try out the **freeware** or **FOSS** (free and open source software) alternatives to any propriety software that you currently use, especially those programs that are unlicensed. Freeware and FOSS tools are often written by volunteers and non-profit organisations who release them, and even update them, free of charge. FOSS tools, in particular, are generally considered to be more secure than **proprietary** ones, because they are developed in a transparent way that allows their **source code** to be examined by a diverse group of experts, any one of whom can identify problems and contribute solutions.

Many FOSS applications look like, and work almost the same way as, the proprietary software that they were written to replace. At the same time, you can use these programs alongside proprietary software, including the Windows operating system, without any problems. Even if your colleagues continue to use the commercial version of a particular type of program, you can still exchange files and share information with them quite easily. In particular, you might consider replacing Internet Explorer, Outlook or Outlook Express and Microsoft Office with Firefox, Thunderbird and LibreOffice, respectively.

In fact, you could even move away from the Microsoft Windows operating system entirely, and try using a more secure FOSS alternative called **GNU/Linux**. The best way to find out if you're ready to make the switch is simply to give it a try. You can download a **LiveCD** version of Ubuntu **Linux**, burn it to a CD or DVD, put it in your computer and restart. When it's done loading, your computer will be running GNU/Linux, and you can decide what you think. Don't worry, none of this is permanent. When you're finished, simply shut down your computer and remove the Ubuntu LiveCD. The next time you start up, you'll be back in Windows, and all of you applications, settings and data will be just as you left them. In addition to the general security advantages of open-source software, Ubuntu has a free, easy-to-use update tool that will keep your operating system and much of your other software from becoming outdated and insecure.

FURTHER READING

- See the chapter on *Malicious Software and Spam* and the Appendix on *Internet Program Settings* in the *Digital Security and Privacy for Human Rights Defenders* [1] book.
- Keep up to-date with news about viruses on the *Virus Bulletin* [2] website.
- Learn how to *determine which 'Windows services' are unnecessary* and *disable those you do not need* [3].
- Other toolkits from the Tactical Technology Collective (*TTC*) [4] can help you switch to using FOSS and Freeware tools for all of your software needs.
- If you think your computer is infected with a virus or some other malicious software read *Malware Removal Guide for Windows* [5].
- Download free bootable rescue CDs to scan your computer and remove the viruses, without starting Windows on your computer. [6]
- LibreOffice is the power-packed free, libre and open source personal productivity suite for Windows, Macintosh and GNU/Linux. [7]
- See Ubuntu which is a Fast, free and incredibly easy to use operating system. Ubuntu will work with your existing PC files, printers, cameras, music players and smartphones - and it comes with thousands of free apps. [8]

LINKS

[1] ***www.frontlinedefenders.org/esecman***
[2] ***www.virusbtn.com***
[3] ***www.marksanborn.net/howto/turn-off-unnecessary-windows-services***
[4] ***www.tacticaltech.org***
[5] ***http://www.selectrealsecurity.com/malware-removal-guide***
[6] ***http://www.askvg.com/download-free-bootable-rescue-cds-from-kaspersky-bitdefender-avira-f-secure-and-others/***
[7] ***https://www.libreoffice.org***
[8] ***http://www.ubuntu.com/***

2
Protect your information from physical threats

2. How to protect your information from physical threats

No matter how much effort you have put into building a digital barrier around your computer, you could still wake up one morning to find that it, or a copy of the information on it, has been lost, stolen, or damaged by any number of unfortunate accidents or malicious acts. Anything from a power surge to an open window to a spilt cup of coffee might lead to a situation in which all of your data are lost and you are no longer able to use your computer. A careful risk assessment, a consistent effort to maintain a healthy computing environment and a written **security policy** can help avoid this type of diaster.

What you can learn from this chapter

- More about a few of the **physical threats** to your computer and to the information stored on it
- How best to secure computer equipment against some of these threats
- How to create a healthy operating environment for computers and network equipment
- What to consider when creating a security plan for the computers in your office

ASSESSING YOUR RISKS

Many organisations underestimate the importance of keeping their offices and their equipment physically secure. As a result, they often lack a clear policy describing what measures they should take to protect computers and backup storage devices from theft, severe weather conditions, accidents, and other physical threats. The importance of such policies may seem obvious, but formulating them properly can be more complicated than it sounds. Many organisations, for example, have good quality locks on their office doors, and many even have secure windows; but if they do not pay attention to the number of keys that have been created, and who has copies of those keys, their sensitive information remains vulnerable.

Unfortunately there is no one-size-fits-all solution to the challenge of physical security. The specifics of a good policy almost always depend on a particular organisation's individual circumstances. When you're trying to come up with a plan, you need to observe your work environment very carefully and think creatively about where your weak points might be and what you can do to strengthen them.

When assessing the risks and vulnerabilities that you or your

organisation face, you must evaluate several different levels at which your data may be threatened.

- Consider the communication channels you use and how you use them. Examples might include paper letters, faxes, landline phones, mobile phones, emails and **Skype** messages.
- Consider how you store important information. Computer hard drives, email and web servers, USB memory sticks, external USB hard drives, CDs and DVDs, mobile phones, printed paper and hand-written notes are all likely possibilities.
- Consider where these items are located, physically. They could be in the office, at home, in a trash bin out back or, increasingly, 'somewhere on the Internet.' In this last case, it might be quite challenging to to determine the particular piece of information's actual, physical location.

Keep in mind that the same piece of information might be vulnerable on many different levels. Just as you might rely on anti-virus software to protect the contents of a USB memory stick from malware, you must rely on a detailed physical security plan to protect the same information from theft, loss or destruction. While some security practices, such as having a good off-site backup policy, are helpful against both digital and physical threats, others are clearly more specific.

When you decide whether to carry your USB memory stick in your pocket or sealed in a plastic bag at the bottom of your luggage, you are making a decision about physical security, even though the information you are trying to protect is digital. As usual, the correct policy depends greatly on the situation. Are you walking across town or travelling across a border? Will somebody else be carrying your bag? Is it raining? These are the sorts of questions that you should consider when making decisions like this.

PROTECTING YOUR INFORMATION FROM PHYSICAL INTRUDERS

Malicious individuals seeking access to your sensitive information represent one important class of physical threat. It would be a mistake to assume that this is the only such threat to the security of your information, but it would be even move shortsighted to ignore it. There are a number of steps you can take to help reduce the risk of physical intrusion. The categories and suggestions below, many of which may apply to your home as well as your office, represent a foundation upon which you should build in accordance with your own particular physical security situation.

Around the office

- Get to know your neighbours. Depending on the security climate in your country and in your neighbourhood, one of two things may be possible. Either you can turn them into allies who will help you keep an eye on your office, or you can add them to the list of potential threats that your security plan must address.
- Review how you protect all of the doors, windows and other points of entry that lead into your office.
- Consider installing a surveillance camera or a motion-sensor alarm.
- Try to create a reception area, where visitors can be met before they enter the office, and a meeting room that is separate from your normal work space.

In the office

- Protect network cables by running them inside the office.
- Lock network devices such as **servers**, **routers**, **switches**, **hubs** and modems into secure rooms or cabinets. An intruder with physical access to such equipment can install **malware** capable of stealing data in transit or attacking other computers on your network even after he leaves. In some circumstances it may be beneficial to hide servers, computers or other equipment in attics, over a fake ceiling, or even with a neighbor, and use them through wireless connection.
- If you have a wireless network, it is critical that you secure your **access point** so that intruders cannot join your network or monitor your traffic. If you are using an insecure wireless network, anyone in your neighbourhood with a laptop becomes a potential intruder. This is an unusual definition of 'physical', but it helps to consider that a malicious individual who can monitor your wireless network has the same access as one who can sneak into your office and connect an ethernet cable. The steps required to secure a wireless network will vary, depending on your access point hardware and software, but they are rarely difficult to follow.

At your workplace

- You should position your computer screen carefully, both on your desk and when you are away from the office, in order to prevent others from reading what is displayed there. In the office, this means considering the location of windows, open doors and the guest waiting area, if you have one.
- Most desktop computer cases have a slot where you can attach a padlock that will prevent anyone without a key from getting inside. If you have cases like this in the office, you should lock them so that

intruders cannot tamper with their internal hardware. You might also consider this feature when purchasing new computers.

- Use a locking **security cable**, where possible, to prevent intruders from stealing the computers themselves. This is especially important for laptops and small desktops that could be hidden inside a bag or under a coat.

Software and settings related to physical security

- Make sure that, when you restart your computer, it asks you for a password before allowing you to run software and access files. If it does not, you can enable this feature in Windows by clicking on the Start menu, selecting the Control Panel, and double-clicking on User Accounts. In the User Accounts screen, select your own account and click Create a Password. Choose a secure password, as discussed in *Chapter 3: How to create and maintain good passwords*, enter your password, confirm it, click Create Password and click Yes, Make Private.
- There are a few settings in your computer's **BIOS** that are relevant to physical security. First, you should configure your computer so that it will not **boot** from the USB device, CD-ROM or DVD drives. Second, you should set a password on the BIOS itself, so that an intruder can not simply undo the previous setting. Again, be sure to choose a secure password.
- If you rely on a secure password database, as discussed in *Chapter 3*, to store your Windows or BIOS passwords for a particular computer, make sure that you do not keep your only copy of the database on that computer.
- Get in the habit of locking your account whenever you step away from your computer. On Windows, you can do this quickly by holding down the Windows logo key and pressing the L key. This will only work if you have created a password for your account, as described above.
- **Encrypt** sensitive information on computers and storage devices in your office. See *Chapter 4: How to protect the sensitive files on your computer* for additional details and pointers to the appropriate Hands-on Guides.

Note: You should be very careful changing any BIOS settings on your computer. The settings that you might want to change are pretty simple, but the BIOS screen itself can be a little intimidating, and it is possible to leave your computer temporarily unable to start if you do something wrong. In general, if you're uncomfortable working in BIOS, you should ask someone with more computer experience to help you out.

Portable devices

- Keep your laptop, your mobile phone and other portable devices that contain sensitive information with you at all times, especially if you are travelling or staying at a hotel. Travelling with a laptop **security cable** is a good idea, although it is sometimes difficult to find an appropriate object to which you can attach one. Remember that meal times are often exploited by thieves, many of whom have learnt to check hotel rooms for laptops during hours of the day when they are likely to be unattended.
- If you have a laptop, tablet or other mobile device, try to avoid putting them on display. There is no need to show thieves that you are carrying such valuable hardware or to show individuals who might want access to your data that your shoulder bag contains a hard drive full of information. Avoid using your portable devices in public areas, and consider carrying your laptop in something that does not look like a laptop bag.

MAINTAINING A HEALTHY ENVIRONMENT FOR YOUR COMPUTER HARDWARE

Like many electronic devices, computers are quite sensitive. They do not adapt well to unstable electricity supplies, extreme temperatures, dust, high humidity or mechanical stress. There are a number of things you can do to protect your computers and network equipment from such threats:

- Electrical problems such as power surges, blackouts and brownouts can cause physical damage to a computer. Irregularities like this can 'crash' your hard drive, damaging the information it contains, or physically harm the electronic components in your computer.
  - If you can afford them, you should install Uninterruptible Power Supplies (**UPSs**) on important computers in your office. A UPS stabilises electricity supply and provides temporary power in the event of a blackout.
  - Even where UPSs are deemed inappropriate or too costly, you can still provide power filters or surge protectors, either of which will help protect you from power surges.
  - Test your electrical network before you connect important equip ment to it. Try to use power sockets that have three slots, one of them being a 'ground line', or 'earth'. And, if possible, take a day or two to see how the electrical system in a new office behaves when powering inexpensive devices, such as lamps and fans, before put ting your computers at risk.
- To defend against accidents in general, avoid placing important

hardware in passages, reception areas or other easily accessible locations. UPSs, power filters, surge protectors, power strips and extension cables, particularly those attached to servers and networking equipment, should be positioned where they will not be switched off by an accidental misstep.

- If you have access to high-quality computer cables, power strips and extension cables, you should purchase enough to serve your entire office and pick up a few extras. Power strips that fall out of wall sockets, fail to hold plugs securely and spark constantly are more than just annoying. They can be quite damaging to the physical security of any computers attached to them. They can also lead frustrated users to secure their loose computer cables to a sparking power strip with tape, which creates an obvious fire hazard.
- If you keep any of your computers inside cabinets, make sure they have adequate ventilation, or they might overheat
- Computer equipment should not be housed near radiators, heating vents, air conditioners or other ductwork

CREATING YOUR PHYSICAL SECURITY POLICY

Once you have assessed the threats and vulnerabilities that you or your organisation face, you must consider what steps can be taken to improve your physical security. You should create a detailed **security policy** by putting these steps in writing. The resulting document will serve as a general guideline for yourself, your colleagues and any newcomers to your organisation. It should also provide a checklist of what actions should be taken in the event of various different physical security emergencies. Everybody involved should take the time to read, implement and keep up with these security standards. They should also be encouraged to ask questions and propose suggestions on how to improve the document.

Your physical security policy may contain various sections, depending on the circumstances:

- An office access policy that addresses the alarm systems, what keys exist and who has them, when guests are allowed in the office, who holds the cleaning contract and other such issues
- A policy on which parts of the office should be restricted to authorized visitors
- An inventory of your equipment, including serial numbers and physical descriptions
- A plan for securely disposing of paper rubbish that contains sensitive information
- Emergency procedures related to:
  - Who should be notified if sensitive information is disclosed or misplaced
  - Who to contact in the event of a fire, flood, or other natural disaster
  - How to perform certain key emergency repairs
  - How to contact the companies or organizations that provide services such as electrical power, water and Internet access
  - How to recover information from your off-site backup system. You can find more detailed backup advice in *Chapter 5: How to recover from information loss*.

Your **security policy** should be reviewed periodically and modified to reflect any policy changes that have been made since its last review. And, of course, don't forget to back up your security policy document along with the rest of your important data. See the *Further reading* section for more information about creating a security policy.

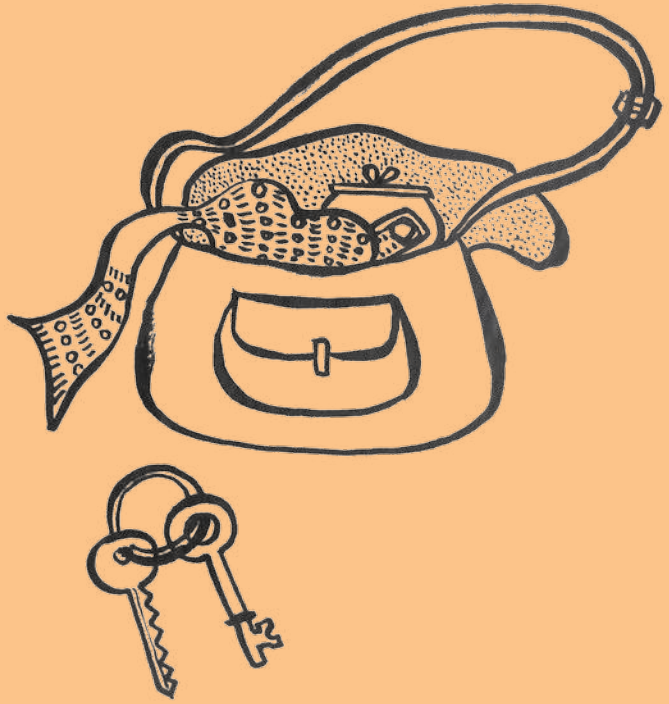
FURTHER READING

- For additional information on assessing risks, see the *Security Awareness*, and *Threat Assessment* sections of the *Digital Security and Privacy for Human Rights Defenders* book [1].
- For a more detailed explanation of how to set a BIOS password, see the *Windows Security* chapter in the *Digital Security and Privacy for Human Rights Defenders* book [1].
- For guidelines on creating a security policy, see *Case Study 1* in the *Digital Security and Privacy for Human Rights Defenders* book [1].
- See also the *Workbook on Security: Practical steps for human rights defenders at risk, Protection Manual and Protection Handbook for Human Rights Defenders.* [2]

LINKS

[1] ***www.frontlinedefenders.org/esecman***
[2] ***http://www.frontlinedefenders.org/security-training***

3
Create and maintain secure passwords



3. How to create and maintain secure passwords

Many of the secure services that allow us to feel comfortable using digital technology to conduct important business, from signing in to our computers and sending email to encrypting and hiding sensitive data, require that we remember a password. These secret words, phrases or strings of gibberish often provide the first, and sometimes the only, barrier between your information and anyone who might want to read, copy, modify or destroy it without your permission. There are many ways in which someone could learn your passwords, but you can defend against most of them by applying a few specific tactics and by using a secure password database tool, such as KeePass.

What you can learn from this chapter

- The elements of a secure password
- A few tricks for remembering long, complicated passwords
- How to use the **KeePass secure password database** to store passwords instead of remembering them

SELECTING AND MAINTAINING SECURE PASSWORDS

In general, when you want to protect something, you lock it up with a key. Houses, cars and bicycle locks all have physical keys; protected files have **encryption** keys; bank cards have PIN numbers; and email accounts have passwords. All of these keys, physical and electronic, have one thing in common: they open their respective locks just as effectively in the hands of somebody else. You can install advanced firewalls, secure email accounts, and **encrypted** disks, but if your password is weak, or if you allow it to fall into the wrong hands, they will not do you much good.

Elements of a strong password

A password should be difficult for a computer program to guess.

- **Make it long:** The longer a password is, the less likely it is that a computer program would be able to guess it in a reasonable amount of time. You should try to create passwords that include ten or more characters. Some people use passwords that contain more than one word, with or without spaces between them, which are often called passphrases. This is a great idea, as long as the program or service you are using allows you to choose long enough passwords.
- **Make it complex:** In addition to length, the complexity of a password also helps prevent automatic 'password cracking' software from

guessing the right combination of characters. Where possible, you should always include upper case letters, lower case letters, numbers and symbols, such as punctuation marks, in your password.

A password should be difficult for others to figure out.

- **Make it practical:** If you have to write your password down because you can't remember it, you may end up facing a whole new category of threats that could leave you vulnerable to anybody with a clear view of your desk or temporary access to your home, your wallet, or even the trash bin outside your office. If you are unable to think of a password that is long and complex but still memorable, the *Remembering secure passwords* section, below, might be of some help. If not, you should still choose something secure, but you may need to record it using a **secure password database** such as **KeePass**. Other types of password-protected files, including Microsoft Word documents, should not be trusted for this purpose, as many of them can be broken in seconds using tools that are freely available on the Internet.
- **Don't make it personal:** Your password should not be related to you personally. Don't choose a word or phrase based on information such as your name, social security number, telephone number, child's name, pet's name, birth date, or anything else that a person could learn by doing a little research about you.
- **Keep it secret:** Do not share your password with anyone unless it is absolutely necessary. And, if you must share a password with a friend, family member or colleague, you should change it to a temporary password first, share that one, then change it back when they are done using it. Often, there are alternatives to sharing a password, such as creating a separate account for each individual who needs access. Keeping your password secret also means paying attention to who might be reading over your shoulder while you type it or look it up in a secure password database.

A password should be chosen so as to minimise damage if someone does learn it.

- **Make it unique:** Avoid using the same password for more than one account. Otherwise, anyone who learns that password will gain access to even more of your sensitive information. This is particularly true because some services make it relatively easy to crack a password. If you use the same password for your Windows user account and your Gmail account, for example, someone with physical access to your computer can crack the former and use what they learn to access the latter. For similar reasons, it is a bad idea to rotate passwords by swapping them around between different accounts.
- **Keep it fresh:** Change your password on a regular basis, preferably at least once every three months. Some people get quite attached to a particular password and never change it. This is a bad idea. The longer you keep one password, the more opportunity others have to figure it out. Also, if someone is able to use your stolen password to access your information and services without you knowing about it, they will continue to do so until you change the password.

Many people considering telling their passwords to someone they trust. Keep in mind though, that just because you trust somebody with your password doesn't necessarily mean you trust them to take good care of it!

REMEMBERING AND RECORDING SECURE PASSWORDS

Looking over the list of suggestions above, you might wonder how anyone without a photographic memory could possibly keep track of passwords that are this long, complex and meaningless without writing them down. The importance of using a different password for each account makes this even more difficult. There are a few tricks, however, that might help you create passwords that are easy to remember but extremely difficult to guess, even for a clever person using advanced 'password cracking' software.

You also have the option of recording your passwords using a tool like **KeePass** that was created specifically for this purpose.

Remembering secure passwords

It is important to use different types of characters when choosing a password. This can be done in various ways:

- Varying capitalisation, such as: 'My naME is Not MR. MarSter'
- Alternating numbers and letters, such as: 'a11 w0Rk 4nD N0 p14Y'
- Incorporating certain symbols, such as: 'c@t(heR1nthery3'
- Using multiple languages, such as: 'Let Them Eat 1e gateaU au ch() colaT'

Any of these methods can help you increase the complexity of an otherwise simple password, which may allow you to choose one that is secure without having to give up entirely on the idea of memorizing it. Some of the more common substitutions (such as the use of a zero instead of an 'o' or the '@' symbol in place of an 'a') were long-ago incorporated into password-cracking tools, but they are still a good idea. They increase the amount of time that such tools would require to learn a password and, in the more common situations where tools

of this sort cannot be used, they help prevent lucky guesses.

Passwords can also take advantage of more traditional mnemonic devices, such as the use of acronyms. This allows long phrases to be turned into complex, seemingly-random words:

- 'To be or not to be? That is the question' becomes '2Bon2B?TitQ'
- 'We hold these truths to be self-evident: that all men are created equal' becomes 'WhtT2bs-e:taMac='
- 'Are you happy today?' becomes 'rU:-)2d@y?'

These are just a few examples to help you come up with your own method of encoding words and phrases to make them simultaneously complex and memorable. A little effort to make the password more complex goes a very long way. Increasing the length of a password even just by a few characters, or by adding numbers or special characters, makes it much more difficult to crack. For demonstrative purposes, the table below shows how much longer it may take a hacker to break a list of progressively more complex passwords by trying different combinations of the password one after another.

Sample password	Time to crack with an everyday computer	Time to crack with very fast computer
bananas	Less than 1 day	Less than 1 day
bananalemonade	2 days	Less than 1 day
BananaLemonade	3 months, 14 days	Less than 1 day
B4n4n4L3m0n4d3	3 centuries, 4 decades	1 month, 26 days
We Have No Bananas	19151466 centuries	3990 centuries
W3 H4v3 N0 B4n4n45	20210213722742 centuries	4210461192 centuries

Of course, the time it would take to crack any of the above passwords would vary widely depending on the nature of the attack, and the resources available to the attacker. Moreover, new methods to crack passwords are constantly being devised. All the same, the table does demonstrate that passwords become vastly more difficult to break by simply varying characters and using two words or, even better, a short phrase.

The table above is based on Passfault's calculations. Passfault [5] is one of a number of websites which allows you to test the strength of your passwords. However, while such resources are good for demonstrating the relative efficiency of different types of passwords, you should avoid introducing your actual passwords into these sites.

Recording passwords securely

While a little creativity may allow you to remember all of your passwords, the need to change those passwords periodically means that you might quickly run out of creativity. As an alternative, you can generate random, secure passwords for most of your accounts and simply give up on the idea of remembering them all. Instead, you can record them in a portable, encrypted secure password database, such as KeePass.

Hands-on: Get started with *KeePass – Secure Password Storage*

Of course, if you use this method, it becomes especially important that you create and remember a very secure password for **KeePass**, or whatever tool you choose. Whenever you need to enter a password for a specific account, you can look it up using only your master password, which makes it much easier to follow all of the suggestions above. KeePass is portable, as well, which means that you can put the database on a USB memory stick in case you need to look up a password while you are away from your primary computer.

Although it is probably the best option for anybody who has to maintain a large number of accounts, there are a few drawbacks to this method. First, if you lose or accidentally delete your only copy of a password database, you will no longer have access to any of the accounts for which it contained passwords. This makes it extremely important that you back up your KeePass database. Look over *Chapter 5: How to recover from information loss* for more information on backup strategies. Fortunately, the fact that your database is encrypted means that you don't have to panic if you lose a USB memory stick or a backup drive containing a copy of it.

The second major drawback could be even more important. If you forget your KeePass master password, there is no way to recover it or the contents of the database. So, be sure to choose a master password that is both secure and memorable!

The strength of this method may, in certain situations, become its weakness. If somebody forces you to give away your Keepass database master password, they will gain access to all of the passwords stored in the Keepass database. If this is a situation you may face, you could treat your Keepass database as a sensitive file, and protect it as we describe in *Chapter 4: How to protect the sensitive files on your computer*. You can also create a separate Keepass database to contain passwords protecting more sensitive information, and take extra precautions with

that database. It's also a good idea to regularly update your Master Password.

Human Rights Defender Testimonies

"Keepass is lovely because I no longer have to remember any password. I have it on my computer, on my phone and on my ipad so it makes my life so easy when I am opening new accounts."
Anonymous human rights defender

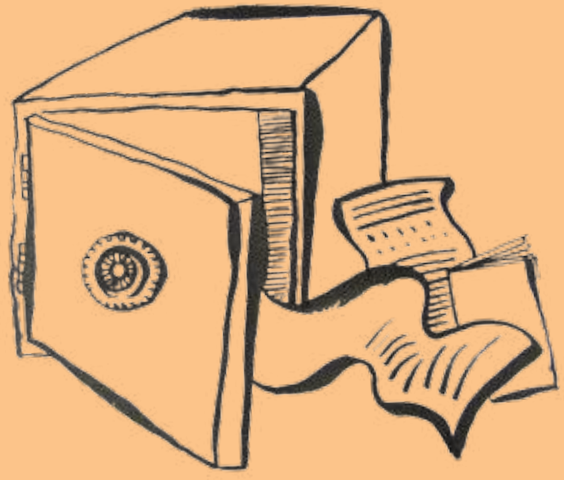
FURTHER READING

- To learn more about secure passwords, see the *Password Protection* chapter and the *How long should my password be?* Appendix in the *Digital Security and Privacy for Human Rights Defenders* book [1].
- Wikipedia has informative articles on *Passwords* [2], *Guidelines for password strength* [3], and *password cracking* [4].
- Passfault evaluates the strength of passwords accurately enough to predict the time to crack. It makes creating passwords and password policies significantly more intuitive and simple. [5]

LINKS

[1] ***www.frontlinedefenders.org/esecman***
[2] ***www.en.wikipedia.org/wiki/Password***
[3]***www.en.wikipedia.org/wiki/Password_strength***
[4] ***www.en.wikipedia.org/wiki/Password_cracking***
[5] ***https://passfault.appspot.com/password_strength.html***

4
Protect the sensitive files on your computer



4. How to protect the sensitive files on your computer

Unauthorised access to the information on your computer or portable storage devices can be carried out remotely, if the 'intruder' is able to read or modify your data over the Internet; or physically, if he manages to get hold of your hardware. You can protect yourself against either type of threat by improving the physical and network security of your data, as discussed in *Chapter 1: How to protect your computer from malware and hackers* and *Chapter 2: How to protect your information from physical threats*. It is always best to have several layers of defence, however, which is why you should also protect the files themselves. That way, your sensitive information is likely to remain safe even if your other security efforts prove inadequate.

There are two general approaches to the challenge of securing your data in this way. **You can encrypt your files**, making them unreadable to anyone but you, or **you can hide them** in the hope that an intruder will be unable to find your sensitive information. There are tools to help you with either approach, including a **FOSS** application called **TrueCrypt** [*more on page 73], which can both encrypt and hide your files.

Accounts of Attacks and Censorship

In Uganda in 2013, a 65-year-old businessman was arrested and charged with "trafficking obscene publications" after his computer was stolen and gay pornography stored on it was discovered. The theives passed the material to Uganda's *Red Pepper* newspaper which splashed details of the video on its front page under the headline: "Exposed – Top City Tycoons Sodomy Sex Video Leaks", and the material was subsequently passed to the police and used as a basis for his prosecution.

Human Rights Defender Testimonies

"We go to meetings where our houses can be raided, information found and used against us as activists to indicate we are promoting LGBT Propaganda. We travel with our laptops to meetings, workshops and seminars, and airports especially can be a risky place if you are detained or even loose your luggage!"

Anonymous Human Rights Defender

What you can learn from this chapter

- How to encrypt information on your computer
- What risks you might face by keeping your data encrypted
- How to protect data on USB memory sticks, in case they are lost or stolen
- What steps you can take to hide information from physical or remote intruders

ENCRYPTING YOUR INFORMATION

The first step to protecting the data on your computer, naturally, is to have a login password. However, especially for Windows users, these passwords are still quite easy to break; the same goes for passwords for certain programs like Microsoft Word or Adobe Acrobat. These passwords do not encrypt the data on your computer, meaning that anyone with a little time alone with your computer could access the data, even without the passwords. The same goes for other users on your device: they may by default be able to access your folders, and even if they are made 'private', they are not safe from other users unless they are encrypted.

Encrypting your information is a bit like keeping it in a locked safe. Only those who have a key or know the lock's combination (an encryption key or password, in this case) can access it. The analogy is particularly appropriate for **TrueCrypt** and tools like it, which create secure containers called 'encrypted volumes' rather than simply protecting one file at a time. You can put a large number of files into an encrypted volume, but these tools will not protect anything that is stored elsewhere on your computer or USB memory stick.

Hands-on: Get started with the *TrueCrypt – Secure File Storage*

While other software can provide similar strength **encryption**, **TrueCrypt** contains several important features to allow you to design your information security strategy. It offers the possibility of permanently **encrypting the whole disk** of your computer including all your files, all temporary files created during your work, all programs you have installed and all Windows operating system files. TrueCrypt supports **encrypted** volumes on portable storage devices. It provides 'deniability' features described in the *Hiding your sensitive information* section below. In addition TrueCrypt is a **free and open source** program.

Tips on using file encryption safely

Storing confidential data can be a risk for you and for the people you work with. Encryption reduces this risk but does not eliminate it. The first step to protecting sensitive information is to reduce how much of it you keep around. Unless you have a good reason to store a particular file, or a particular category of information within a file, you should simply delete it (see *Chapter 6: How to destroy sensitive information* for more information about how to do this securely). The second step is to use a good file encryption tool, such as **TrueCrypt.**

Returning to the analogy of a locked safe, there are a few things you should bear in mind when using TrueCrypt and tools like it. No matter how sturdy your safe is, it won't do you a whole lot of good if you leave the door open. When your TrueCrypt volume is 'mounted' (whenever you can access the contents yourself), your data may be vulnerable, so you should keep it closed except when you are actually reading or modifying the files inside it.

There are a few situations when it is especially important that you remember not to leave your encrypted volumes mounted:

- Disconnect them when you walk away from your computer for any length of time. Even if you typically leave your computer running overnight, you need to ensure that you do not leave your sensitive files accessible to physical or remote intruders while you are gone.
- Disconnect them before putting your computer to sleep. This applies to both 'suspend' and 'hibernation' features, which are typically used with laptops but may be present on desktop computers as well.
- Disconnect them before allowing someone else to handle your computer. When taking a laptop through a security checkpoint or border crossing, it is important that you disconnect all encrypted volumes and shut your computer down completely.
- Disconnect them before inserting an untrusted USB memory stick or other external storage device, including those belonging to friends and colleagues.
- If you keep an encrypted volume on a USB memory stick, remember that just removing the device may not immediately disconnect the volume. Even if you need to secure your files in a hurry, you have to dismount the volume properly, then disconnect the external drive or memory stick, then remove the device. You might want to practice until you find the quickest way to do all of these things.

If you decide to keep your **TrueCrypt** volume on a USB memory stick, you can also keep a copy of the TrueCrypt program with it. This will allow you to access your data on other people's computers. The usual

rules still apply, however: if you don't trust the machine to be free of malware, you probably shouldn't be typing in your passwords or accessing your sensitive data.

Human Rights Defender Testimonies

"The people at the office were very excited about encryption. Everybody is now going around feeling and acting like 007. They even encrypt things on their flash drives. I see it when they give me a document on a flash, I just look at the size of the documents and it makes me smile. We talk about it and we laugh. "
Anonymous Human Rights Defender

"I'm a legal practitioner working with the LGBTI community, especially women. Truecrypt is important to my work because I deal with a lot of documents, I do a lot of analysis. That's important to me, I wouldn't like someone opening my laptop and seeing all that. It puts not only me but the people I work for at risk. And if I lose that data, it's almost like a warehouse for whatever they do, I'm a background worker for them. My position is key, I take it seriously. This empowers me to work safely, and to store it safely for them."
Anonymous Human Rights Defender

HIDING YOUR SENSITIVE INFORMATION

One issue with keeping a safe in your home or office, to say nothing of carrying one in your pocket, is that it tends to be quite obvious. Many people have reasonable concerns about incriminating themselves by using encryption. Just because the legitimate reasons to encrypt data outnumber the illegitimate ones does not make this threat any less real. Essentially, there are two reasons why you might shy away from using a tool like TrueCrypt: the risk of self-incrimination and the risk of clearly identifying the location of your most sensitive information.

Considering the risk of self-incrimination

Encryption is illegal in some countries, which means that downloading, installing or using software of this sort might be a crime in its own right. And, if the police, military or intelligence services are among those groups from whom you are seeking to protect your information, then violating these laws can provide a pretext under which your activities might be investigated or your organisation might be persecuted. In fact, however, threats like this may have nothing to do with the legality of the tools in question. Any time that merely being associated with encryption software would be enough to expose you to accusations of criminal activity or espionage (regardless of what is actually inside your encrypted volumes), then you will have to think carefully about whether or not such tools are appropriate for your situation.

If that is the case, you have a few options:

- You can avoid using data security software entirely, which would require that you store only non-confidential information or invent a system of code words to protect key elements of your sensitive files.
- You can rely on a technique called steganography to hide your sensitive information, rather than encrypting it. There are tools that can help with this, but using them properly requires very careful preparation, and you still risk incriminating yourself in the eyes of anyone who learns what tool you have used.
- You can try to store all of your sensitive information in a secure webmail account, but this demands a reliable network connection and a relatively sophisticated understanding of computers and Internet services. This technique also assumes that network encryption is less incriminating than file encryption and that you can avoid accidentally copying sensitive data onto your hard drive and leaving it there.
- You can keep sensitive information off of your computer by storing it on a USB memory stick or portable hard drive. However, such devices are typically even more vulnerable than computers to loss and confiscation, so carrying around sensitive, unencrypted information on them is usually a very bad idea.

If necessary, you can employ a range of such tactics. However, even in circumstances where you are concerned about self-incrimination, it may be safest to use TrueCrypt anyway, while attempting to disguise your encrypted volume as best you can.

If want to make your encrypted volume less conspicuous, you can rename it to look like a different type of file. Using the '.iso' file extension, to disguise it as a CD image, is one option that works well for large volumes of around 700 MB. Other extensions would be more realistic for smaller volumes. This is a bit like hiding your safe behind a painting on the wall of your office. It might not hold up under close inspection, but it will offer some protection. You can also rename the **TrueCrypt** program itself, assuming you have stored it as you would a regular file on your hard drive or USB memory stick, rather than installing it as a program. The *TrueCrypt Guide* explains how to do this.

The risk of identifying your sensitive information

Often, you may be less concerned about the consequences of 'getting caught' with **encryption** software on your computer or USB memory stick and more concerned that your encrypted volume will indicate

precisely where you store the information that you most wish to protect. While it may be true that no one else can read it, an intruder will know that it is there, and that you have taken steps to protect it. This exposes you to various non-technical methods through which that intruder might attempt to gain access, such as intimidation, blackmail, interrogation and torture. It is in this context that TrueCrypt's deniability feature, which is discussed in more detail below, comes into play.

TrueCrypt's deniability feature is one of the ways in which it goes beyond what is typically offered by file encryption tools. This feature can be thought of as a peculiar form of **steganography** that disguises your most sensitive information as other, less sensitive, hidden data. It is analogous to installing a subtle 'false bottom' inside that not-so-subtle office safe. If an intruder steals your key, or intimidates you into giving her the safe's combination, she will find some convincing 'decoy' material, but not the information that you truly care about protecting.

Only you know that your safe contains a hidden compartment in the back. This allows you to 'deny' that you are keeping any secrets beyond what you have already given to the intruder, and might help protect you in situations where you must reveal a password for some reason. Such reasons might include legal or physical threats to your own safety, or that of your colleagues, associates, friends and family members. The purpose of deniability is to give you a chance of escaping from a potentially dangerous situation even if you choose to continue protecting your data. As discussed in the *Considering the risk of self-incrimination* section, however, this feature is much less useful if merely being caught with a safe in your office is enough to bring about unacceptable consequences.

TrueCrypt's deniability feature works by storing a 'hidden volume' inside your regular encrypted volume. You open this hidden volume by providing an alternate password that is different from the one you would normally use. Even if a technically sophisticated intruder gains access to the standard volume, he will be unable to prove that a hidden one exists.

Of course, he may very well know that TrueCrypt is capable of hiding information in this way, so there is no guarantee that the threat will disappear as soon as you reveal your decoy password. Plenty of people use TrueCrypt without enabling its deniability feature, however, and it is generally considered impossible to determine, through analysis, whether or not a given encrypted volume contains this kind of 'false bottom'. That said, it is your job to make sure that you do not reveal your hidden volume through less technical means, such as leaving it open or allowing other applications to create shortcuts to the files that it contains. The *Further reading* section, below, can point you to more information about this .

Human Rights Defender testimonies

"I really, really love TrueCrypt and I wish more people in the community could use it. I give my computer to my sister a lot and now I am no longer bothered about her finding anything she shouldn't. I put everything in a TrueCrypt volume and after that, I use CCleaner to wipe the computer before I give it to her."
Anonymous Human Rights Defender

"When the police came into the office to check our computers and see what we were doing and if we were working with MSM, I noticed for the first time that everybody in the office was calm because everyone uses TrueCrypt and we were not afraid of being found with anything else that is incriminating."
Anonymous Human Rights Defender

"The government has interest in the work we do, they have sent security agents several times to the organisation to interview us. Sometimes we get wind that they're coming so we have to take the paper, take things out of the office and hide them somewhere, you know - and that may not necessarily be safe either - so now we know that we can actually hide the stuff right there in that office, and they can check from roof to foundation and they won't find what's there."
Anonymous Human Rights Defender

*On 28 May 2014 TrueCrypt developers web page started to inform users that TrueCrypt development is discontinued as of now. The circumstances behind this situation are not clear yet. The developers web page is offering a new version 7.2 of TrueCrypt with some functionality removed.

Despite this new release we recommend that you continue to use the older version 7.1a (see *Downloading instructions*), until we know more about what has happened and what the plans are for the future of TrueCrypt development. For alternatives to TrueCrypt, see the TrueCrypt hands-on guide.

FURTHER READING

- For additional information on securing your files, see the *Cryptology* chapter, the *Steganography* chapter and *Case Study 3* from the *Digital*

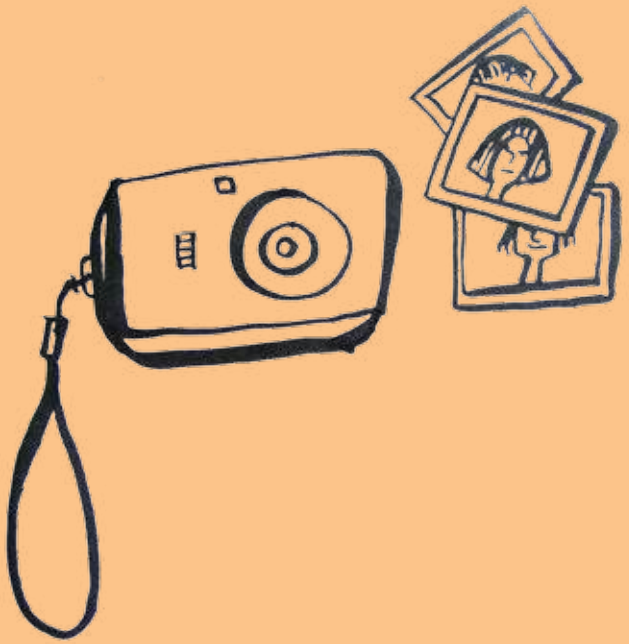
Security and Privacy for Human Rights Defenders book [1].

- The *TrueCrypt Documentation* [2] discusses in details many aspects of information encryption and *TrueCrypt FAQ* [3] provides answers to some common questions about TrueCrypt.

LINKS

[1] ***www.frontlinedefenders.org/esecman***
[2] ***http://andryou.com/truecrypt/docs/index.php***
[3] ***http://andryou.com/truecrypt/docs/faq.php***

5
Recover from information loss



5. How to recover from information loss

Each new method of storing or transferring digital information tends to introduce several new ways in which the information in question can be lost, taken or destroyed. Years of work can disappear in an instant, as a result of theft, momentary carelessness, the confiscation of computer hardware, or simply because digital storage technology is inherently fragile. There is a common saying among computer support professionals: "it's not a question of if you will lose your data; it's a question of when." So, when this happens to you, it is extremely important that you already have an up-to-date backup and a well-tested means of restoring it. The day you are reminded about the importance of a backup system is generally the day after you needed to have one in place.

Although it is one of the most basic elements of secure computing, formulating an effective backup policy is not as simple as it sounds. It can be a significant planning hurdle for a number of reasons: the need to store original data and backups in different physical locations, the importance of keeping backups confidential, and the challenge of coordinating among different people who share information with one another using their own portable storage devices. In addition to backup and file-recovery tactics, this chapter addresses two specific tools, **Cobian Backup** and **Recuva**.

What you can learn from this chapter

- How to organise and back up your information
- Where you should store your backups
- How you can manage your backups securely
- How to recover files that have been deleted accidentally

IDENTIFYING AND ORGANISING YOUR INFORMATION

While it is clearly important that you take steps to prevent disaster, by making sure that your information is physically safe, free of malware and protected by a good **firewall** and strong passwords, on their own these steps are not enough. There are simply too many things that can go wrong, including virus attacks, **hackers**, electrical short circuits, power spikes, water spills, theft, confiscation, demagnetisation, operating system crashes and hardware failure, to name just a few. Preparing for disaster is just as important as defending against it.

Coming up with a good backup plan takes a bit of thought, but it doesn't take all that much time or money. Moreover, unless you have

access to extremely reliable technical and well-informed technical support, it's advisable to take it into your own hands.

The first step to formulating a ***backup policy*** is to picture where your personal and work information is currently located. Your email, for example, may be stored on the provider's mail server, on your own computer, or in both places at once. And, of course, you might have several email accounts. Then, there are important documents on the computers you use, which may be in the office or at home. There are address books, chat histories and personal program settings. It is also possible that some information is stored on removable media as well, including USB memory sticks, portable hard drives, CDs, DVDs, and old floppy disks. Your mobile phone contains a list of contacts and may have important text messages stored in it. If you have a website, it may contain a large collection of articles built up over years of work. And, finally, don't forget your non-digital information, such as paper notebooks, diaries and letters.

Next, you need to define which of these files are 'master copies,' and which are duplicates. The master copy is generally the most up-to-date version of a particular file or collection of files, and corresponds to copy that you would actually edit if you needed to update the content. Obviously, this distinction does not apply to files of which you have only one copy, but it is extremely important for certain types of information. One common disaster scenario occurs when only duplicates of an important document are backed up, and the master copy itself gets lost or destroyed before those duplicates can be updated. Imagine, for example, that you have been travelling for a week while updating the copy of a particular spreadsheet that you keep on your USB memory stick. At this point, you should begin thinking of that copy as your master copy, because the periodic, automated backups of the outdated version on your office computer are no longer useful.

Try to write down the physical location of all master and duplicate copies of the information identified above. This will help you clarify your needs and begin to define an appropriate backup policy. The table below is a very basic example. Of course, you will probably find that your list is much longer, and contains some 'storage devices' with more than one 'data type' and some data types that are present on multiple devices.

In the following table you can see that:

- The only documents that will survive if your office computer's hard drive crashes are the duplicates on your USB memory stick and the CD copies at home.
- You have no offline copy of your email messages or your address book, so if you forget your password (or if someone manages to change it maliciously), you will lose access to them.
- You have no copies of any data from your mobile phone.
- You have no duplicate copies, digital or physical, of printed documents such as contracts and invoices.

Data Type	Master/ Duplicate	Storage Device	Location
Electronic documents	Master	Computer hard drive	Office
A few important electronic documents	Duplicate	USB memory stick	With me
Program databases (photos, address book, calendar, etc.)	Master	Computer hard drive	Office
A few electronic documents	Duplicate	CDs	Home
Email & email contacts	Master	Gmail account	Internet
Text messages & phone contacts	Master	Mobile phone	With me
Printed documents (contracts, invoices, etc.)	Master	Desk drawer	Office

DEFINING YOUR BACKUP STRATEGY

To back up all of the data types listed above, you will need a combination of software and process solutions. Essentially, you need to make sure that each data type is stored in at least two separate locations.

Electronic documents

Create a full backup of the documents on your computer using a program like **Cobian Backup**, which is described in more detail below. Store the backup on something portable so that you can take it home or to some other safe location. External hard drives, CD/DVDs or USB memory sticks are possible choices. Some people use CDs or DVDs for this, since the risk of overwriting and losing your backup is lower. Blank CDs may be cheap enough to allow you to use a new one every time you make a backup. Because this category of data often contains the most sensitive information, it is particularly important that you protect your electronic document backups using encryption. You can learn how to do this in *Chapter 4: How to protect the sensitive files on your computer* and in the *TrueCrypt Guide*.

Program databases

Once you have determined the location of your program databases, you can back them up in the same way as electronic documents.

Email

Rather than accessing your email only through a web browser, install an email client like **Thunderbird** and configure it to work with your account. The *Thunderbird Guide* explains in detail how to do this. Also most webmail services will provide instructions on how to use such programs and, often, how to import your email addresses into them. You can learn more about this in the Further Reading section, below. If you choose to move your old email messages to your computer so they are not stored on the server (e.g. for security reasons), make sure that you include them in the backup of electronic documents described above.

Mobile phone contents

To back up the phone numbers and text messages on your mobile phone, you can connect it to your computer using the appropriate software, which is generally available from the website of the company that manufactured your phone. You may need to buy a special USB cable to do this, however.

Printed documents

Where possible, you should scan all of your important papers, then back them up along with your other electronic documents, as discussed above.

In the end, you should have rearranged your storage devices, data types and backups in a way that makes your information much more resistant to disaster:

Data Type	Master/Duplicate	Storage Device	Location
Electronic documents	Master	Computer hard drive	Office
Electronic documents	Duplicate	CDs	Home
A few important electronic documents	Duplicate	USB memory stick	With me

Data Type	Master/ Duplicate	Storage Device	Location
Program databases	Master	Computer hard drive	Office
Program databases	Duplicate	CDs	Home

Data Type	Master/ Duplicate	Storage Device	Location
Email & email contacts	Duplicate	Gmail account	Internet
Email & email contacts	Master	Thunderbird on office computer	Office

Data Type	Master/ Duplicate	Storage Device	Location
Text messages & mobile phone contacts	Master	Mobile phone	With me
Text messages & mobile phone contacts	Duplicate	Computer hard drive	Office
Text messages & mobile phone contacts	Duplicate	Backup SIM	Home

Data Type	Master/Duplicate	Storage Device	Location
Printed documents	Master	Desk drawer	Office
Scanned documents	Duplicate	CDs	At home

Some people use their e-mail accounts as ad-hoc backup locations, such as by e-mailing files to themselves or attaching them to draft emails. While this may help us recover a handful of our documents, it's not advisable as a general-purpose backup strategy, due to the quanitity of files involved, as well as possible vulnerabilities in the security of the email provider. If you insist on this strategy, however, be sure to at least use a webmail which provides an SSL connection and, ideally, encrypt the files with PGP as well.

CREATING A DIGITAL BACKUP

Of the various data types discussed here, it is the 'electronic documents' that people tend to worry about most when establishing a backup policy. This term is somewhat ambiguous, but generally refers to files that you keep track of yourself and that you open manually, either by double-clicking on them or by using a particular application's File menu. Specifically, it includes text files, word processing documents, presentations, PDFs and spreadsheets, among other examples. Unlike email messages, for example, electronic documents are generally not synchronised with remote copies over the Internet.

When backing up your electronic documents, you should remember to back up your program databases, as well. If you use a calendar application or an electronic address book, for example, you will need to find the folder in which these programs store their data. Hopefully, these databases will be in the same location as your electronic documents, as they are often kept inside your My Documents folder on a Windows computer. If that is not the case, however, you should add the appropriate folders to your regular backup.

Email stored by an application such as **Thunderbird** is a special example of a program database. If you use an email program, especially

if you are unable or unwilling to store a copy of your messages on the server, then you must ensure that this email database is included in your regular backup. You may consider image and video files to be electronic documents or items within a program database, depending on how you interact with them.

Applications like Windows Media player and iTunes, for example, work like databases. If you use programs like this, you might have to search your hard drive to learn where they store the actual media files that they help manage.

Human Rights Defender Testimonies

"I use Cobian backup most often. It asks me for weekly update and because it is not stressful, I am always confident of being covered"
Anonymous Human Rights Defender

"Recently, I had an unfortunate accident where my laptop went for a swim in a lake. I also made the rookie mistake of having my backup in the same bag that fell into the lake so i lost both of them. The only positive is that I had a backup from 3 months before so that made life a little easier to bear. Now, Cobian and I are best friends. I do a weekly backup every weekend on two different devices so I am prepared for most eventualities."
Anonymous Human Rights Defender

Storage devices

Before you can back up your electronic documents, you must decide what kind of storage device you will use.

USB disk or memory sticks

USB disk or memory sticks can be quite inexpensive, and offer large capacity. They are easy to erase or overwrite numerous times. USB disk or memory sticks have a limited lifetime, which greatly depends on ways and frequency of usage but is generally estimated to be around 10 years.

Compact Discs (CDs)

CDs store around 700 Megabytes (MB) of data. You will need a CD burner and blank discs in order to create a CD backup. If you want to erase a CD and update the files stored on it, you will need to have a CD-RW burner and rewritable CDs. All major operating systems, including Windows XP, now include built-in software that can write CDs and CD-RWs. Keep in mind that the information written on these discs may begin to deteriorate after five or ten years. If you need to store a backup for longer than that, you will have to recreate the CDs occasionally, buy special 'long life' discs or use a different backup method.

Digital Video Discs (DVDs)

DVDs store up to 4.7 Gigabytes (GB) of data. They work much like CDs but require slightly more expensive equipment. You will need a DVD or DVD-RW burner, and appropriate discs. As with a CD, the data written on a normal DVD will eventually begin to fade.

Remote server

A well-maintained network backup server may have almost unlimited capacity, but the speed and stability of your own Internet connection will determine whether or not this is a realistic option. Keep in mind that running a backup server in your own office, while faster than copying information over the Internet, violates the requirement that you keep a copy of your important data in two different physical locations. There are free storage services on the Internet, as well, but you should very carefully consider the risks of putting your information online and you should always encrypt your backups before uploading them to servers run by organisations or individuals whom you do not know and trust. See the Further reading section for a few examples.

Backup Software

Cobian Backup is a user-friendly tool that can be set to run automatically, at regularly scheduled times, and to include only files that have changed since your last backup. It can also compress backups to make them smaller.

Hands-on: Get started with *Cobian Backup – Secure File Storage*

As always, it is a good idea to encrypt your backup files using a tool such as **TrueCrypt**. More information about about data encryption can be found in *Chapter 4: How to protect the sensitive files on your computer*.

Hands-on: Get started with *TrueCrypt – Secure File Storage*

When using these backup tools, there are a few things you can do to help your backup system work smoothly:

- Organise the files on your computer. Try to move all of the folders

that contain electronic documents you intend to back up into a single location, such as inside the My Documents folder.

- If you use software that stores its data in an application database, you should first determine the location of that database. If it is not in a convenient location, see if the program will allow you to choose a new location for its database. If it does, you can put it in the same folder as your electronic documents.
- Create a regular schedule to perform your backup.
- Try to establish procedures for all of the staff in your office who do not already have a reliable, secure backup policy. Help your coworkers understand the importance of this issue.
- Make sure to test the process of recovering data from your backup. Remember that, in the end, it is the restore procedure, not the backup procedure, that you really care about!

Remember, it's important to store your backup in a different location to your computer: this will help protect your backup from being destroyed or stolen in an accident or break-in.

RECOVERING FROM ACCIDENTAL FILE DELETION

When you delete a file in Windows, it disappears from view, but its contents remain on the computer. Even after you empty the **Recycle Bin**, information from the files you deleted can usually still be found on the hard drive. See *Chapter 6: How to destroy sensitive information* to learn more about this.

Occasionally, if you accidentally delete an important file or folder, this security vulnerability can work to your advantage. There are several programs that can restore access to recently-deleted files, including a tool called **Recuva**.

Hands-on: Get started with *Recuva – File Recovery*

These tools do not always work, because Windows may have written new data over your deleted information. Therefore, it is important that you do as little as possible with your computer between deleting a file and attempting to restore it with a tool like Recuva. The longer you use your computer before attempting to restore the file, the less likely it is that you will succeed. This also means that you should use the portable version of **Recuva** instead of installing it after deleting an important file. Installing the software requires writing new information to the file system, which may coincidentally overwrite the critical data that you are trying to recover.

While it might sound like a lot of work to implement the policies and learn the tools described in this chapter, maintaining your backup strategy, once you have a system in place, is much easier than setting it up for the first time. And, given that backup may be the single most important aspect of data security, you can rest assured that going through this process is well worth the effort.

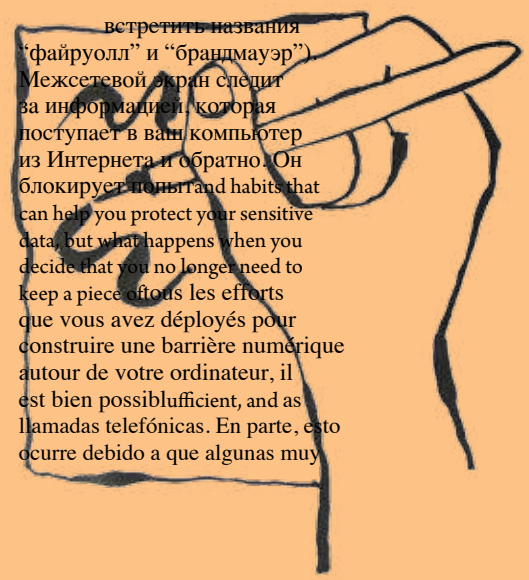
FURTHER READING

- More information on backup and data recovery can be found in the *Information Backup, Destruction and Recovery* chapter of the *Digital Security and Privacy for Human Rights Defenders* [1] book.
- There are several free online data storage services that provide a convenient way to back up a small amount of sensitive information. It is important, however, to understand the risks of your data being online. If you must use any such service, it is important to independently encrypt your data before uploading it to any such free online storage, to provide an added measure of security.
- There is an excellent article on data recovery in *Wikipedia* [2].
- Note that online backup brings new risks. At minimum, remember to encrypt your sensitive information separately yourself before you upload it to the server. Assuming you do the step above, there are free online data storage services as a convenient way to back up your information. Some options include: *Wuala* [3], *SpiderOak* [4], *Google Drive* [5] , *tahoe-lafs* [6].

LINKS

[1] ***www.frontlinedefenders.org/esecman***
[2] ***www.en.wikipedia.org/wiki/Data_recovery***
[3] ***https://www.wuala.com/***
[4] ***https://spideroak.com/***
[5] ***http://www.google.com/drive/about.html?authuser=0***
[6] ***https://tahoe-lafs.org/trac/tahoe-lafs***

6
Destroy sensitive information



встретить названия “файруолл” и “брандмауэр”). Межсетевой экран следит за информацией, которая поступает в ваш компьютер из Интернета и обратно. Он блокирует попыtand habits that can help you protect your sensitive data, but what happens when you decide that you no longer need to keep a piece oftous les efforts que vous avez déployés pour construire une barrière numérique autour de votre ordinateur, il est bien possiblufficient, and as llamadas telefónicas. En parte, esto ocurre debido a que algunas muy

6. How to destroy sensitive information

The previous chapters have discussed a number of tools and habits that can help you protect your sensitive data, but what happens when you decide that you no longer need to keep a piece of information? If you determine, for example, that your encrypted backup copies of a particular file are sufficient, and you want to delete the master, what is the best way to do so? Unfortunately, the answer is more complicated than you might think. When you delete a file, even after you empty the Recycle bin, the contents of that file remain on your hard drive and can be recovered by anyone who has the right tools and a little luck.

In order to ensure that deleted information does not end up in the wrong hands, you will have to rely on special software that removes data securely and permanently. **Eraser** is one such tool, and is discussed below. Using Eraser is a bit like shredding a paper document rather than simply tossing it into a bin and hoping that nobody finds it. And, of course, deleting files is only one example of a situation in which you might need to destroy sensitive data. If you consider the details that someone, particularly a powerful, politically-motivated adversary, could learn about you or your organisation by reading certain files that you thought you had deleted, you will probably think of a few more examples of data that you'd like to permanently erase, by destroying outdated backups, wiping old hard drives before giving them away, deleting old user accounts, and clearing your web browsing history, for example.

CCleaner, the other tool described in this chapter, can help you face the challenge of deleting the many temporary files that your operating system and applications create every time you use them.

What you can learn from this chapter

- How to remove sensitive information from your computer permanently
- How to remove information stored on removable storage devices like CDs and USB memory sticks
- How to prevent someone from learning what documents you have previously been viewing on your computer
- How to maintain your computer so that deleted files cannot be recovered in the future

DELETING INFORMATION

From a purely technical perspective, there is no such thing as a delete function on your computer. Of course, you can drag a file to the Recycle Bin and empty the bin, but all this really does is clear the icon, remove

the file's name from a hidden index of everything on your computer, and tell Windows that it can use the space for something else. Until it actually does use that space, however, the space will be occupied by the contents of the deleted information, much like a filing cabinet that has had all of its labels removed but still contains the original files. This is why, if you have the right software and act quickly enough, you can restore information that you've deleted by accident, as discussed in *Chapter 5: How to recover from information loss*.

You should also keep in mind that files are created and insecurely deleted, without your knowledge, every time you use your computer. Suppose, for example, that you are writing a large report. It may take you a week, working several hours each day, and every time the document is saved, Windows will create a new copy of the document and store it on your hard drive. After a few days of editing, you may have unknowingly saved several versions of the document, all at different stages of completion.

Windows generally deletes the old versions of a file, of course, but it does not look for the exact location of the original in order to overwrite it securely when a new copy is made. Instead, it simply puts the latest version into a new section of the metaphorical filing cabinet mentioned above, moves the label from the old section to the new one, and leaves the previous draft where it was until some other program needs to use that space. Clearly, if you have a good reason to destroy all traces of that document from your filing cabinet, removing the latest copy is not going to be enough, and simply throwing away the label would be even worse.

Remember, too, that computer hard drives are not the only devices that store digital information. CDs, DVDs, USB memory sticks, floppy disks, flash memory cards from mobile phones and removable hard drives all have the same issues, and you should not trust a simple delete or rewrite operation to clear sensitive information from any of them.

WIPING INFORMATION WITH SECURE DELETION TOOLS

When you use a secure deletion tool, such as those recommended in this chapter, it would be more accurate to say that you are replacing, or 'overwriting,' your sensitive information, rather than simply deleting it. If you imagine that the documents stored in those hypothetical filing cabinet discussed above are written in pencil, then secure deletion software not only erases the content, but scribbles over the top of every word. And, much like pencil lead, digital information can still be read, albeit poorly, even after it has been erased and something has been written over the top of it. Because of this, the tools recommended here overwrite files with random data several times. This process is called **wiping**, and the more times information is overwritten, the more difficult it becomes for someone to recover the original content. Experts generally agree that three or more overwriting passes should be made; some standards recommend seven or more. Wiping software automatically makes a reasonable number of passes, but you can change that number if you like.

Wiping files

There are two common ways to **wipe** sensitive data from your hard drive or storage device. You can wipe a single file or you can wipe all of the 'unallocated' space on the drive. When making this decision, it may be helpful to think about the other hypothetical example proposed earlier--the long report that may have left incomplete copies scattered throughout your hard drive even though only one file is visible. If you wipe the file itself, you guarantee that the current version is completely removed, but you leave the other copies where they are. In fact, there is no way to target those copies directly, because they are not visible without special software. By wiping all of the blank space on your storage device, however, you ensure that all previously-deleted information is destroyed. Returning to the metaphor of the poorly-labeled file cabinet, this procedure is comparable to searching through the cabinet, then erasing and scribbling repeated over any documents that have already had their labels removed.

Eraser is a free and open-source secure deletion tool that is extremely easy to use. You can wipe files with Eraser in three different ways: by selecting a single file, by selcting the contents of the Recycle Bin, or by wiping all unallocated space on the drive. Eraser can also wipe the contents of the Windows swap file, which is discussed below.

Hands-on: Get started with *Eraser – Secure File Removal*

While secure deletion tools will not damage any visible files unless you explicitly wipe them, it is still important to be careful with software like this. After all, accidents happen, which is why people find **Recycle Bins** and data recovery tools so useful. If you get accustomed to wiping your data every time you delete something, you may find yourself with no way to recover from a simple mistake. Always make sure you have a secure backup before wiping large amounts of data from your computer.

It's also worth keeping in mind that many programs, including common office programs like Microsoft Office or Libre Office, along with web browsers and chat clients, sometimes make temporary copies of a file while you're working on it or leave traces of your browsing or chat history. All of this information could be sensitive and of interest to third parties who get their hands on your computer. Therefore, regularly wiping your temporary files is highly recommended.

Wiping temporary data

The feature that allows **Eraser** to **wipe** all unallocated space on a drive is not as risky as it might sound, because it only wipes previously-deleted content. Normal, visible files will be unaffected. On the other hand, this very fact serves to highlight a separate issue: Eraser can not help you clean up sensitive information that has not been deleted, but that may be extremely well-hidden. Files containing such data may be tucked away in obscure folders, for example, or stored with meaningless filenames. This is not a major issue for electronic documents, but can be very important for information that is collected automatically whenever you use your computer. Examples include:

- Temporary data recorded by your browser while displaying webpages, including text, images, **cookies**, account information, personal data used to complete online forms and the history of which websites you have visited.
- Temporary files saved by various applications in order to help you recover should your computer crash before you can save your work. These files might contain text, images, spreadsheet data and the names of other files, along with other potentially sensitive information.
- Files and links stored by Windows for the sake of convenience, such as shortcuts to applications you have used recently, obvious links to folders that you might prefer to keep hidden and, of course, the contents of your **Recycle Bin** should you forget to empty it.
- The Windows **swap file**. When your computer's memory is full, for example when you have been running several programs at the same time on an older computer, Windows will sometimes copy the data you are using into a single large file called the swap file. As a result, this file might contain almost anything, including webpages, document content, passwords or encryption keys. Even when you shut down your computer, the swap file is not removed, so you must wipe it manually.

In order to remove common temporary files from your computer, you can use a freeware tool called **CCleaner**, which was designed to clean up after software like Internet Explorer, Mozilla **Firefox** and Microsoft Office applications (all of which are known to expose potentially sensitive information), as well as cleaning Windows itself. CCleaner has the ability to delete files securely, which saves you from having to wipe unallocated drive space, using **Eraser**, after each time you run it.

Hands-on: Get started with *CCleaner – Secure File Deletion and Work Session Wiping*

TIPS ON USING SECURE DELETION TOOLS EFFECTIVELY

You are now familiar with a few of the ways in which information might be exposed on your computer or storage device, even if you are dilligent about erasing sensitive files. You also know what tools you can use to wipe that information permanently. There are a few simple steps that you should follow, especially if it is your first time using these tools, in order to ensure that your drive is cleaned safely and effectively:

- Create an encrypted backup of your important files, as discussed in *Chapter 5: How to recover from information loss.*
- Close down all unnecessary programs and disconnect from the Internet.
- Delete all unnecessary files, from all storage devices, and empty the **Recycle Bin**
- **Wipe** temporary files using CCleaner.
- Wipe the Windows swap file using Eraser.
- Wipe all of the free space on your computer and other storage devices using Eraser. You might need to let this procedure run overnight, as it can be quite slow.

You should then get into the habit of:

- Periodically using **CCleaner** to **wipe** temporary files
- Wiping sensitive electronic documents using **Eraser**, instead of using the Recycle Bin or the Windows delete function
- Periodically using Eraser to wipe the Windows **swap file**
- Periodically using Eraser to wipe all unallocated space on your hard drives, USB memory sticks, and any other storage devices that may have had sensitive information deleted from them recently. This might include floppy disks, rewritable CDs, rewritable DVDs and removable flash memory cards from cameras, mobile phones or portable music players.

TIPS ON WIPING ALL CONTENTS OF A STORAGE DEVICE

You might occasionally need to **wipe** a storage device completely. When you sell or give away an old computer, it is best to remove the

hard drive and let the computer's new owner acquire one for herself. If this is not an option, however, you should at least wipe the drive thoroughly with **Eraser** before handing it over. And, even if you do keep the drive, you will probably want to wipe it anyway, regardless of whether you intend to reuse or discard it. Similarly, if you purchase a new hard drive, you should wipe your old one after copying your data and making a secure backup. If you are intending to throw away or recycle an old drive, you should also consider destroying it physically. (Many computer support professionals recommend a few strong blows with a hammer before discarding any data-storage device that once contained sensitive information.)

In any of the situations described above, you will need to use Eraser to wipe an entire hard drive, which is impossible as long as the operating system is running on that particular drive. The easiest way to get around this issue is to remove the drive and put it into an external USB 'drive enclosure,' which you can then plug into any computer with Eraser installed on it. At that point, you can delete the full contents of the external drive and then use Eraser to wipe all of its unallocated space. Fortunately, this is not something you will have to do often, as it may take quite some time.

Rather than trying to wipe data that have been stored on a rewritable CD or DVD, it is often better to destroy the disc itself. If necessary, you can create a new one containing any information you wish to keep. And, of course, this is the only way to 'erase' content from a non-rewritable disc. It is surprisingly difficult to destroy the contents of a CD or DVD completely. You may have heard stories about information being recovered from such discs even after they were cut into small pieces. While these stories are true, reconstructing information in this way takes a great deal of time and expertise. You will have to judge for yourself whether or not someone is likely to expend that level of resources in order to access your data. Typically, a sturdy pair of scissors (or a very sturdy paper shredder) will do the job nicely. If you want to take extra precautions, you can mix up the resulting pieces and dispose of them in various locations far from your home or office.

FURTHER READING

- While it does not use secure deletion techniques to wipe them permanently, Firefox does provide a built-in way to clear many of its own temporary files.
- The *CCleaner FAQ* [1] provides additional information about installing and using the tool.
- Although much of the paper is quite technical, the introduction of Peter Guttmann's *Secure Deletion of Data from Magnetic and Solid-State Memory* [2] is worth reading, as the *method* [3] he describes has had a major influence on the developers of Eraser and other secure file removal tools.

LINKS

[1] ***www.piriform.com/ccleaner/faq***
[2] ***www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/***
[3] ***www.en.wikipedia.org/wiki/Gutmann_method***

7
How to remove hidden information from files

7. How to remove hidden information from files

Metadata is information about a file (such as a word document, a PDF, a picture, music file etc.) that is stored within the file itself. This information can include the time and date a file was created, the username of the people who created or edited it, information about the device that created it, and other kinds of information. As a result of this, the metadata in a file could tell someone who created a file, on what computer or device, when, and in what location.

While this information is generated automatically by many devices (like cameras, computers, and phones) it can be edited and manipulated by those who know where to look. This can also be a good thing, as it means you can take control over the metadata you choose to share when you share files.

Let's take pictures as an example. When you take a picture with your digital camera, what happens? If your camera or phone knows where you are, then that information (in the form of GPS coordinates) can be saved in the metadata of the file. If your camera knows what time it is, it records the date and time the picture was taken. If your camera or phone has a serial number that may be recorded in metadata as well. Digital image file formats such as TIFF (Tagged Image File Format) and JPEG (Joint Photographic Experts Group) created by digital cameras or smartphones, contain metadata in a format called EXIF (Exchangeable image file format) which could include all of the above information and even a thumbnail of the original image.

Other files such as text documents include metadata too. A text document's metadata, for example, may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.

Metadata can be very useful in helping to organise non-sensitive information. For those who share sensitive or political media widely, however, unknowingly attaching information to files can be very dangerous. If you take a picture of a police officer doing something illegal, and share it on the internet without taking care to scrub metadata from the file first, the data may be used to identify who took the picture (in this case, you).

In order to ensure that this won't happen, it's important to learn how to "scrub" or remove metadata from files when necessary. In part, we have to rely on a special software that removes metadata securely from files. Metanull, which removes metadata from images, is one

such tool, and is discussed below. Furthermore, there are many non-technical, but rather behavioural, ways that we can stop meta-data getting into files in the first place.

What you can learn from this chapter

- How to remove or edit the metadata from files such as image files
- How to remove information stored on removable storage devices like CDs and USB memory sticks
- How to prevent someone from learning what documents you have previously been viewing on your computer
- How to maintain your computer so that deleted files cannot be recovered in the future

DELETING HIDDEN DATA FROM FILES USING METADATA REMOVAL TOOLS

As mentioned above, when you take a picture with your smartphone or a digital camera, information called EXIF (Exchangeable Image File Format) data is stored inside it. EXIF data can contain information that reveals potentially sensitive details about the picture such as the GPS location, the type of camera used, and the exact date and time in which the picture was taken.

You can check the metadata of a photo by right-clicking on it and selecting Properties, or by using a metadata viewer software such as **Photome.**

You will see the following:

GPS information

Field	Content
GPS Tag Version	Version 2.2
North or South Latitude	North Latitude
Latitude	50 28 07, 775
East or west longitude	East Longitude
Longitude	7 37 32, 75
Atitude Reference	Sea Level
Altitude	262 m

The above information can specify your exact location, which is in our example: 1 km northwest of Nauort, Nauort, Westerwaldkreis, Germany, Europe.

Image information

Field	Content
Manufacturer	Nikon Corporation
Image input equipment model	Nikon D80
File change date and time	2007-05-20 11:19:41
Image resolution in width and heigh direction	300 dpi

In the example above, the metadata shows the exact location where the photo was taken, which device was used to take the photo, the time when the photo was taken, and other image specifications.

These are just a sample of the data inlcuded in the image; it also includes further camera details, JPEG details and much more.

There are non-technical ways that can prevent a specific kind of metadata like **GPS** location from being captured. For example:

- Switching off wireless and gps location (under location services) and mobile data (this can be found under data manager -> data delivery).
- When taking a photo, make sure that the settings of the tag-location from the photo app is off too.

Using tools like Metanull, you can ensure that all metadata is removed before you share it. This tool is discussed in details below.

Note: Some files like DOCs and PDFs can hold image files within them. If you aren't careful, you can scrub the metadata on the document that is holding the image, but the metadata for the embedded image is still there! Using metanull before adding the image to the PDF would remove all metadata from it beforehand.

Hands-on: Get started with the *Metanull Guide*

Removing metadata from documents and other files

As noted above, other commonly used file types such as Portable Document Files (PDFs) or word processing documents created by applications such as Microsoft Office or LibreOffice contain metadata which may include:

- The username of the person who created a document
- The name of the person who most recently edited saved a document
- The date when a document was created and modified

In some cases, your document might also contain additional kinds of personally identifiable information such as such as the addresses, e-mail addresses, government ID, IP addresses, or any unique identifier

associated with personally identifiable information in another program on your computer.

Some of this information is easily accessible by viewing the file properties (which can be accessed by right clicking on the file icon and selecting properties). Other information or hidden data need specific softwares to be viewed. In any case, depending on your context, this information might put you at risk if you are working and exchanging sensitive information.

Removing metadata from PDF files

Windows or MAC OS users can use programs such as Adobe Acrobat XI Pro (for which a trial version is available) to remove or edit the hidden data from PDF files.

Opening any PDF file with Acrobat will allow you to edit the metadata by going to File menu and then selecting properties. Here, you can modify the document author's name, title, subject, keywords and any additional metadata. Regarding the creation time, modification time, type of device used for creation the file, and other hidden data you don't see, you can remove it by going to Tools menu, then Protection, and selecting Remove hidden information.

Note: For GNU/Linux users, **PDF MOD** is a free and open source tool to edit and remove metadata from PDF files. However, it doesn't remove the creation or modification time, it also doesn't remove the type of device used for creating the PDF.

Removing metadata from Microsoft Word documents

Microsoft Office Word files has a feature called **Document Inspector** which analyses the file's metadata and allows for its removal.

Note: Once metadata is removed by Document Inspector it can't be recovered. If you want a copy of your document with the metadata still intact, make a duplicate before deleting the metadata.

You can do this by clicking the Microsoft Office Button, point to Prepare and then click Inspect Document. In the Document Inspector dialog box, select the check boxes to choose the types of hidden content that you want to inspect. Then click Inspect to review the results of the inspection. Click Remove All next to the inspection results for the types of hidden content that you want to remove from your document.

Removing metadata from LibreOffice documents

In LibreOffice documents the metadata can be viewed by selecting the File menu, then Properties. Under the General tab you can click Reset to reset the general user data, such as total editing time and revision number. Also make sure the Apply user data checkbox on this screen is unchecked, so the name of the creator will be removed. When you are done, the next step is to go to the Description and the Custom Properties tabs to clear any data there that you don't want to appear. Lastly, click on the Securit** tab and uncheck the *Record change box if it's not unchecked by default.

Note:

- If you use the Versions feature, you can delete older versions of the document which may be stored there through going to the File menu and Versions.
- If you use the Changes feature, go to the Edit menu then Changes to Accept or reject in order to clear the data relating to changes made to the document over time, if you no longer need this information.

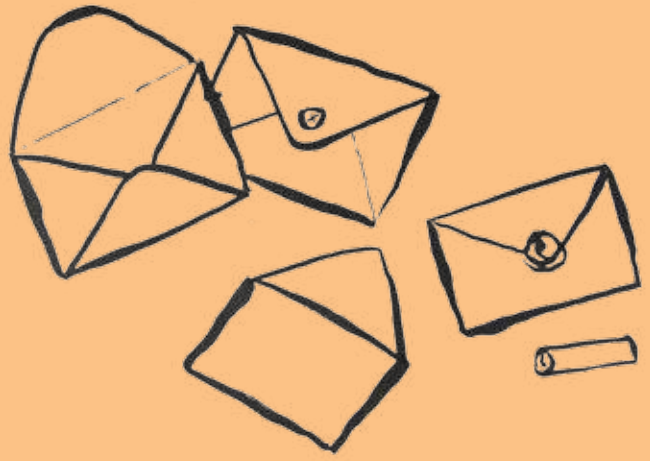
Other Strategies for scrubbing metadata

- Some file types contain more metadata than others, so if you don't want to play around with software, and the formatting of a file doesn't matter, you can change files from ones that contain a lot of metadata (such as .DOCs and .JPEGs for example) to ones that don't (.TXTs and .PNGs for example)
- Avoid using your real name, address, company or organisation name when registering copies of software such as Microsoft Office, Open Office, Libre Office, Adobe Acrobat and others. If you must give a name or address, use a fake one.

FURTHER READING

For more information on metadata removal tools, have a look at *https://en.wikipedia.org/wiki/Comparison_of_metadata_editors*:

8
Keep your Internet communication private



8. How to keep your Internet communication private

The convenience, cost-effectiveness and flexibility of email and instant messaging make them extremely valuable for individuals and organizations with even the most limited access to the Internet. For those with faster and more reliable connections, software such as **Jitsi**, **Skype** and other ***Voice-over-IP*** (**VoIP**) tools also share these characteristics. Unfortunately, these digital alternatives to traditional means of communication can not always be relied upon to keep sensitive information private. Of course, this is nothing new. Postal mail, telephone calls and text messages are all vulnerable as well, particularly when used by those who may have been targeted for surveillance by the authorities.

One important difference between digital, Internet-based communication techniques and more traditional methods, is that the former often allow you to determine your own level of security.

If you send emails, instant messages and VoIP conversations using insecure methods, they are almost certainly less private than letters or telephone calls. In part, this is because a few powerful computers can automatically search through a large amount of digital information to identify senders, recipients and specific key words. Greater resources are required to carry out the same level of surveillance on traditional communication channels. However, if you take certain precautions, the opposite can be true. The flexibility of Internet communication tools and the strength of modern **encryption** can now provide a level of privacy that was once available only to national military and intelligence organizations.

By following the guidelines and exploring the software discussed in this chapter, you can greatly improve your communication security. The **Riseup** email service, the Off the Record (**OTR**) plugin for the **Pidgin** instant messaging program, Mozilla **Firefox** and the **Enigmail** add-on for the Mozilla **Thunderbird** email client are all excellent tools. While using them, however, you should keep in mind that the privacy of a given conversation is never one hundred percent guaranteed. There is always some threat that you did not consider, be it a **keylogger** on your computer, a person listening at the door, a careless email correspondent or something else entirely.

The goal of this chapter is to help you reduce even the threats that do not occur to you, while avoiding the extreme position, favoured by some, that you should not send anything over the Internet that you are not willing to make public.

Human Rights Defender Testimonies

"We're in the digital age and that's the most important means of communication. The postal services aren't even safe! But we call, we send emails, we send messages and that's how we communicate. If you can't protect that, you can't protect yourself, so it's best you're aware, informed, trained to be able to use these tools for your own benefit to protect yourself and protect your family. You're not only protecting yourself, you're protecting those you love."

Anonymous Human Rights Defender

What you can learn from this chapter

- Why most webmail and instant messaging services are not secure
- How to create a new and more secure email account
- How to improve the security in your current email account
- How to use a secure instant messaging service
- What to do if you think someone might be accessing your email
- How to verify the identity of an email correspondent

SECURING YOUR EMAIL

There are a few important steps that you can take in order to increase the security of your email communication. The first is to make sure that only the person to whom you send a given message is able to read it. This is discussed in the *Keeping your webmail private* and *Switching to a more secure email account* sections, below. Going beyond the basics, it is sometimes critical that your email contacts have the ability to verify, without a doubt, that a particular message truly came from you and not from someone who might be attempting to impersonate you. One way to accomplish this is described under *Advanced email security*, in the *Encrypting and authenticating individual email messages* section.

You should also know what to do if you think the privacy of your email account may have been violated. The *Tips on responding to suspected email surveillance* section addresses this question.

Remember, too, that secure email will not do you any good if everything you type is recorded by spyware and periodically sent over the Internet to a third party. *Chapter 1: How to protect your computer from malware and hackers* offers some advice on how to prevent this sort of thing, and *Chapter 3: How to create and maintain secure passwords* will help you protect your accounts for the email and instant messaging tools described below.

Keeping your webmail private

The Internet is an open network through which information typically travels in a readable format. If a normal email message is intercepted on the way to a recipient, its contents can be read quite easily. And, because the Internet is just one large, worldwide network that relies on intermediary computers to direct traffic, many different people may have the opportunity to intercept a message in this way. Your ***Internet Service Provider*** (**ISP**) is the first recipient of an email message as it begins its journey to the recipient. Similarly, the recipient's ISP is the last stop for your message before it is delivered. Unless you take certain precautions, your messages can be read or tampered with at either of these points, or anywhere in between.

There is also a common misconception that information can be securely transmitted by various people sharing the password to a single e-mail account, and writing emails only in draft form, which can give the impression that they are never actually 'sent'. However, any time you read n email on your computer, even if it's just a 'draft,' its contents have been sent to you over the Internet. Otherwise, it couldn't appear on your screen! If someone has you under surveillance, they don't just monitor your email messages, they can scan all readable information going to and from your computer. In other words, this trick wouldn't work unless everyone connects securely to that shared webmail account. And, if they do, then it really doesn't hurt to create separate accounts or to go ahead and hit the 'send' button.

It has long been possible to secure the Internet connection between your computer and the websites that you visit. You often encounter this level of security when entering passwords or credit card information into websites. The technology that makes it possible is called ***Secure Sockets Layer*** (**SSL**) **encryption**. You can tell whether or not you are using SSL by looking closely at your Web browser's address bar.

All Web addresses normally begin with the letters **HTTP**, as can be seen in the example below:

When you are visiting a secure website, its address will begin with **HTTPS**.

The extra **S** on the end signifies that your computer has opened a secure connection to the website. You may also notice a 'lock' symbol, either in the **address bar** or in the **status bar** at the bottom of your browser window. These are clues to let you know that anyone who might be monitoring your Internet connection will no longer be able to eavesdrop on your communication with that particular website.

In addition to protecting passwords and financial transactions, this type of **encryption** is perfect for securing your webmail. However, many webmail providers do not offer secure access, and others require that you enable it explicitly, either by setting a preference or by typing in the **HTTPS** manually. You should always make sure that your connection is secure before logging in, reading your email, or sending a message.

You should also pay close attention if your browser suddenly begins to complain about invalid **security certificates** when attempting to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages. Finally, if you rely on webmail to exchange sensitive information, it is important that your browser be as reliable as possible. Consider installing Mozilla Firefox and its security-related add-ons.

Hands-on: Get started with *Firefox with add-ons – Secure Web Browser*

Switching to a more secure email account

Few webmail providers offer **SSL** access to your email. Yahoo and Hotmail, for instance, provide a secure connection only while you log in, to protect your password, but your messages themselves are sent and received insecurely. In addition, Yahoo, Hotmail and some other free webmail providers insert the **IP address** of the computer you are using into all of the messages you send.

Gmail accounts, on the other hand, use a secure connection during log-in and all the way until you log out. You can confirm this along the way by looking at the address bar and observing the URL starting with '**https'**, where the 's' denotes a secure connection. And, unlike Yahoo or Hotmail, Gmail avoids revealing your **IP address** to email recipients. However, it is not recommend that you rely entirely on Google for the confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom. See the ***Further reading*** section for more information about Google's privacy policy.

If possible, you should create a new **Riseup** email account by visiting ***https://mail.riseup.net***. Riseup offers free email to activists around the world and takes great care to protect the information stored on their servers. They have long been a trusted resource for those in need of secure email solutions. And, unlike Google, they have very strict policies regarding their users' privacy and no commercial interests that might some day conflict with those policies. In order to create a new Riseup account, however, you will need two 'invite codes.' These codes can be given out by anyone who already has a Riseup account. If you have a bound copy of this booklet, you should have received your 'invite codes' along with it. Otherwise, you will need to find two Riseup users and ask them each to send you a code.

Hands-on: Get started with *Riseup – Secure Email Service*

Both Gmail and Riseup are more than just webmail providers. They can also be used with an email client, such as Mozilla **Thunderbird**, that supports the techniques described under *Advanced email security*. Ensuring that your email client makes an **encrypted** connection to your provider is just as important as accessing your webmail through **HTTPS**. If you use an email client, see the Thunderbird Guide for additional details. A the very least, however, you should be sure to enable SSL or encryption for both your incoming and outgoing mail servers.

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. You yourself are only part of the picture. Even if you access your email account securely, consider what precautions your contacts may or may not take when sending, reading and replying to messages. Try to learn where your contacts' email providers are located, as well. Naturally, some countries are more aggressive than others when it comes to email surveillance. **To ensure private communication, you and your contacts should all use secure email services hosted in relatively safe countries**. And, if you want to be certain that messsages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. **Riseup** is one good choice.

Additional tips on improving your email security

- Always use caution when opening email attachments that you are not expecting, that come from someone you do not know or that contain suspicious subject lines. When opening emails like this, you should ensure that your anti-virus software is up-to-date and pay close attention to any warnings displayed by your browser or email program.

- Using anonymity software like **Tor**, which is described in *Chapter 8: How to remain anonymous and bypass censorship on the Internet*, can help you hide your chosen email service from anyone who might be monitoring your Internet connection. And, depending on the extent of Internet filtering in your country, you may need to use Tor, or one of the other circumvention tools described in chapter 8, just to access a secure email provider such as Riseup or Gmail.
- When creating an account that you intend to use while remaining anonymous from your own email recipients, or from public forums to which you might post messages by email, you must be careful not to register a username or 'Full Name' that is related to your personal or professional life. In such cases, it is also important that you avoid using Hotmail, Yahoo, or any other webmail provider that includes your **IP address** in the messages you send.
- Depending on who might have physical access to your computer, clearing email-related traces from your temporary files might be just as important as protecting your messages as they travel across the Internet. See *Chapter 6: How to destroy sensitive information* and the *CCleaner Guide* for details.
- You may consider using several different, anonymous email accounts for communicating with different groups of people to protect of your contact network. You may also use different email accounts for signing up to Internet services which require email accounts.
- After all of the above precautions it is still very important to be aware of what you write in your messages and what impact would it have if it fell into the wrong hands. One way of increasing the security of information exchange is to develope a code system for sensitive information exchange, so you would not use real names of the people, real addresses of places, etc.

TIPS ON RESPONDING TO SUSPECTED EMAIL HACKING AND SURVEILLANCE

If you suspect your email account has been hacked or compromised, you can take steps to reduce the damage done. While it is difficult to be certain, there may be clues such as:

- you notice any changes to your email account content or settings that you didn't make;
- your email contacts notify you that they have received an email that you didn't send;
- you cannot login to your email account, though you are sure your password and other settings are correct;
- you are regularly not receiving some email messages from your colleagues that they insist that they sent to you;
- some private information that was sent or received exclusively by email was made known to a third party, though neither you nor your correspondent shared it with anyone else;
- if on your account activity log (if your email provider offers one) you see that your account was accessed at time that you do not remember or from a place (or IP address) that you did not go to.

In such situations you may want to take some cautionary action:

- **Stop using this email account for sensitive information exchange**, at least until you understand the situation better.
- **Change your password as soon as possible**. See *Chapter 3* to know how to *Create and maintain secure passwords*. In order to be able to change the password for your account (or for other accounts) you need to become familiar with how you do this on your email system, so that when you need to, you can do so quickly. **Change passwords for all other accounts with the same or similar passwords** as they may also be compromised. Use different and strong passwords for each account. You may also want to change passwords for all other accounts that you have. Consider using **KeePass** to store and manage all your passwords. **Change your security question answers** (if you use them) for all accounts, so they are impossible to guess, or find the answer through researching information about you. This is a precaution in the case your computer was infected with spyware which would then put your other accounts at risk.
- **If you are not able to log in** to your account to change the passwords, consider getting in contact with your email provider to try to reclaim your account. Some email providers have special procedures in place to help users in such situation. It is helpful to know these procedures ahead of time.
- **Mitigate information loss and impact** to your community. It is important to make a response plan. Knowing what sensitive kinds of information you had in your account and determining the persons with whom you exchange information via that account, decide whom you should alert and what other accounts you will have to revisit or close. Determine what services (web, financial, etc.) you need to revisit or cancel. It is important that you **check the folders of your account** (if you can) to research on what could have been sent from your account and to act accordingly. To **inform your contacts** you will need to keep a separate backup of your address book. Also **review your account settings** to see possible changes that has been made. Check accounts signature option for links and malware,

forwarding options that would allow to copy emails that you receive to third account, away message, display name, etc.

- **Research how your account was compromised**. Was it because of having a weak password, or due to malware infection, etc. The more you will establish about this, the better you will be able to respond to the situation and better you will be able to protect your contacts.
- **Review the security of all of your devices** that access emails from this account, and devices on which you stored the password to this email account. See *Chapters 1. How to protect your computer from malware and hackers*, *2. How to protect your information from physical threats* and *11. How to use smartphones as securely as possible*. Review your anti-virus software (see the *Avast! – Anti-Virus* and *Spybot - Anti-Spyware hands-on guides*). Scan your computer: read the section *A Short Guide to Dealing with Virus Outbreaks* in the *Avast! hands-on guide*. Use a rescue CD or USB to do a thorough scan – read the section on *Advanced Virus Removal Methods* also in the *Avast! hands-on guide*. If you are not certain that you are able to clean your device, consider reinstalling all software including the operating system from a clean source. Consider switching to more secure programs like **Firefox**, **Thunderbird**, **LibreOffice** and other Free and Open Source Programs. After making the above improvements to the security of your devices, change your account passwords again to new, stronger ones.
- Consider reporting hacking of your account to your email provider.
- Consider using another, more secure account, e.g. one that notifies you of and prevent access from unusual places or devices. Consider using an account that is hosted outside of your country. Consider using email encryption – read gpg4usb – email text and files encryption or Thunderbird with Enigmail and GPG – Secure Email Client.
- Consider avoiding storing read emails on the email server in your email account. Instead download them to your secured computer. Analyse security of the way you access your account and devices that you use for this.

It is important that you act quickly and precisely in the situation like this. Having prepared and rehearsed plan may help you.

If you suspect that someone is already monitoring your email, you may want to create a new account and keep the old one as a decoy. Remember, though, that any account with which you have exchanged email in the past may now be under surveillance as well. As a result, you should observe some additional precautions:

- Both you and your recent email contacts should create new accounts and connect to them only from locations, such as Internet cafes, that you have never used before. We recommend this strategy in order to prevent connections from your usual computer, which may be monitored, from giving away the location of your new account. As an alternative, if you must login to your new account from your normal location, you can use one of the tools described in *Chapter 9: How to remain anonymous and bypass censorship on the Internet*, to hide these connections.
- Exchange information about these new email addresses only through secure channels, such as a face-to-face meetings, secure instant messages or encrypted **VoIP** conversations.
- Keep the traffic on your old account mostly unchanged, at least for a while. It should appear to the eavesdropper as if you are still using that account for sensitive communication. Presumably, you will want to avoid revealing critical information, but you should try not to make it obvious that you are doing so. As you can imagine, this may be somewhat challenging.
- Make it difficult to link your actual identity to your new account. Do not send email between the new account and your old accounts (or the accounts of any contacts whom you think may also be monitored).
- Be aware of what you write when using your new account. It is best to avoid using real names and addresses or phrases like 'human rights' or 'torture.' Develop an informal code system with your email contacts and change it periodically.
- Remember, email security is not just about having strong technical defences. It is about paying attention to how you and your email contacts communicate with each other, and about remaining disciplined in your non-technical security habits.

SECURING OTHER INTERNET COMMUNICATION TOOLS

Much like email, instant messaging and **VoIP** software can be secure or insecure, depending on the tools you choose and how you use them.

Securing your instant messaging software

Instant messaging, also called 'chat,' is not normally secure, and can be just as vulnerable to surveillance as email. Luckily, there are programmes that can help secure the privacy of your chat sessions. **Just like with email, though, a secure communications channel requires that both you and your instant messaging contacts use the same software and take the same security precautions**.

There is a chat programme called **Pidgin** that supports many

existing instant messaging protocols, which means that you can easily begin using it without having to change your account name or recreate your list of contacts. In order to have private, **encrypted** conversations through Pidgin, you will need to install and activate the *Off-the-Record* (**OTR**) plug-in. Fortunately, this is a fairly simple process.

Hands-on: Get started with *Pidgin with OTR – Secure Instant Messaging*

Securing your VoIP software

VoIP calls to other VoIP users are generally free of charge. Some programs allow you to make inexpensive calls to phones as well, including international numbers. Needless to say, these features can be extremely useful. Some of today's more popular VoIP programs include **Skype** (see below), *Jitsi* [1], *Google Hangout*[2] and *Yahoo! Voice* [3].

Normally, voice communication over the Internet is no more secure than unprotected email and instant messaging. When using voice communication to exchange sensitive information it is important to choose a tool that encrypts the call all the way from your computer to the recipient's computer. It also best to use Free and Open-Source Software, preferably those reviewed, tested, and recommended by a trusted community. Taking the above criteria into account we would recommend that you try Jitsi as your choice for VoIP.

Hands-on: Get started with *Jitsi – Secure Audio, Video and Instant Messaging Text Communication*

Human Rights Defender Testimonies

"I love that encryption! I love it! The idea that you can relate with someone without a third party knowing what is happening, you can code your languages, your communication, wow! I came to find that when we communicate with each other there is a "Big Brother" somewhere who sometimes can access this information. Jitsi enables the coding of this information so even that "Big Brother" cannot decode it. It's useful because it makes your communication private, so it's just between you and the person you're addressing."

Anonymous Human rights Defender

Notice about Skype's security

Skype is a very common instant messaging and VoIP tool that also supports calls to landlines and mobile phones. Despite its popularity, several issues make this software not a secure choice. Some of these issues are described below.

While according to Skype, it **encrypts** both messages and voice calls, this would only happen when both communicating sides are using Skype programs. Skype does not encrypt calls to phone or text sent as SMS messages.

If both communicating sides are using (a genuine) Skype program, its encryption may make the call nominally more secure than an ordinary call over phone. But because Skype is a closed-source program, making an independent audit and evaluation of its proclamations about encryption impossible, it is thus impossible to verify how well Skype is protecting the users and their information and communication. *Chapter 1: How to protect your computer from malware and hackers* addresses the virtues of Free and Open-Source Software (**FOSS**) in the *Keeping your software up-to-date* section. As mentioned, while we can't recommend **Skype** as a secure communication tool, it is very important to take some precautions if one still decides to use Skype as a tool for their sensitive communication:

- Download and install Skype only from its official website ***www.skype.com*** to avoid a Skype program infected with spyware. It is important to always double-check the URL to make sure you are connecting to the official site. In some countries the Skype website is blocked, and/or several fake sites claiming to be Skype's official site are in operation. In many such cases, the version of Skype available is likely infected with malware designed to spy on any communication. Use circumvention tools described in *Chapter 8* to connect to the Skype website and download a genuine version of Skype program whenever you want to install or upgrade to newest version of the software.
- It is very important to change your Skype password regularly. Skype allows for multiple logins from different locations and does not inform you about the number of simultaneous sessions. This poses a big risk that if your password is compromised, anyone with that password can also be logged in. All logged sessions receive all the text communication and have access to calls history. Changing the password is the only way to disable such rogue sessions (by forcing a re-login).
- It is also advisable to set the privacy settings on Skype so that it does not keep a history of chats.
- It is recommended to disable the Skype setting which automatically accepts incoming files, as this has occasionally been used to introduce malware/spyware onto computers.
- Always independently verify the identity of a person with whom

you are communicating. It is easier to do this when voice chatting, especially if you know the person you want to talk to.
- Decide if your Skype username should identify your or have any relationship to your real name, or the name of you organisation.
- Always have alternative ways for communicating – Skype can become unavailable at any moment.
- Be careful of what you say – develop a code system to discuss sensitive topics without using specific terminology.

Despite Skype's popularity, the above concerns make it questionable for a secure experience, and we recommend you start using tools like **Jitsi** for VoIP and **Pidgin** with the OTR plugin for secure instant messaging.

ADVANCED EMAIL SECURITY

The tools and concepts discussed below are recommended for experienced computer users.

Using public key encryption in email

It is possible to achieve a greater level of email privacy, even with a non-secure email account. In order to do this, you will need to learn about public key **encryption**. This technique allows you to encode individual messages, making them unreadable to anyone but the intended recipients. The ingenious aspect of public key encryption is that you don't have to exchange any secret information with your contacts about how you are going to encode messages in the future.

This technique can be used with any email service, even one that lacks a secure communication channel, because individual messages are **encrypted** before they leave your computer.

PGP works through clever mathematics. You encode messages to a given email contact using her special 'public key', which she can distribute freely. Then, she uses her secret 'private key', which she has to guard carefully, in order to read those messages. In turn, your contact uses your public key to encrypt messages that she writes to you. So, in the end, you do have to exchange public keys, but you can share them openly, without having to worry about the fact that anybody who wants your public key can get it.

Remember that, by using encryption, you could attract attention to yourself. The type of encryption used when you access a secure website, including a webmail account, is often viewed with less suspicion than the type of public key encryption being discussed here. In some circumstances, if an email containing this sort of encrypted data is intercepted or posted to a public forum, it could incriminate the person who sent it, regardless of the message's content. You might sometimes have to choose between the privacy of your message and the need to remain inconspicuous.

Encrypting and authenticating individual messages

Public key encryption may seem complicated at first, but it is quite straightforward once you understand the basics, and the tools are not difficult to use. The Mozilla **Thunderbird** email program can be used with an extension called **Enigmail** to encrypt and decrypt email messages quite easily.

Hands-on: Get started with *Thunderbird with Enigmail and GPG – Secure Email Client*

VaultletSuite 2 Go, a freeware encrypted email program, is even easier to use than Thunderbird if you are willing to trust the company that provides it and allow them to do some of the work for you.

Hands-on: Get started with *VaultletSuite 2Go – Secure Email Client*

The authenticity of your email is another important aspect of communication security. Anyone with Internet access and the right tools can impersonate you by sending messages from a fake email address that is identical to your own. The danger here is more apparent when considered from the perspective of the recipient. Imagine, for example, the threat posed by an email that appears to be from a trusted contact but is actually from someone whose goal is to disrupt your activities or learn sensitive information about your organisation.

Because we cannot see or hear our correspondents through email, we typically rely on a sender's address to verify her identity, which is why we are so easily fooled by fake emails. **Digital signatures**, which also rely on public key **encryption**, provide a more secure means of proving one's identity when sending a message. The *How to use Enigmail with Thunderbird* section of the *Thunderbird Guide* explains in detail how this is done.

FURTHER READING

- To learn more about faking an email identity, refer to the *Spoofing* section of the *Digital Security and Privacy for Human Rights Defenders* book [4].
- There is a well-known *Man in the Middle attack* [4] attack on SSL

encryption as discussed in the *Digital Security and Privacy for Human Rights Defenders* book.

- The *Gmail Privacy Policy* [5], which you must accept when creating a Gmail account, explains that, "Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services." In fact, all email providers scan your messages, to some extent, so that they can offer anti-spam services and other such features. Gmail goes a bit futher, however, in order to provide 'targeted advertising' based on the actual content of your email. This could be dangerous if information stored by Google were to be intentionally or accidentally exposed.
- In addition to the *RiseUp* and *Thunderbird* Hands-on Guides, there are a number of websites that explain how to use your email program with various popular email providers while leaving a copy of your messages on the mail server:
  - The *Riseup* [6] website
  - Instructions on using *Gmail* [7]
  - Instructions on *how to import your gmail contacts into Thunderbird* [8]
  - For details on how to use other email services in this way, search the help section of the provider's website for keywords like 'POP', 'IMAP' and 'SMTP'.

LINKS

[1] ***https://jitsi.org/***
[2] ***www.google.com/hangouts***
[3] ***www.voice.yahoo.com***
[4] ***www.frontlinedefenders.org/esecman***
[5] ***www.google.com/intl/en/policies/privacy***
[6] ***https://help.riseup.net/en/email-clients***
[7] ***https://support.google.com/mail/topic/3398031?rd=2***
[8] ***email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm***

9
How to remain anonymous and bypass censorship on the internet

9. How to remain anonymous and bypass censorship on the internet

Many countries around the world have installed software that prevents Internet users within those countries from accessing certain websites and Internet services. Companies, schools and public libraries often use similar software to protect their employees, students and patrons from material that they consider distracting or harmful. This kind of filtering technology comes in a number of different forms. Some filters block a site based on its **IP address**, while others blacklist certain **domain names** or search through all unencrypted Internet communication, looking for specific keywords.

Regardless of what filtering methods are present, it is nearly always possible to evade them by relying on intermediary computers, outside your country, to reach blocked services for you. This process is often called censorship circumvention, or simply **circumvention**, and the intermediary computers are called **proxies**. Proxies, too, come in many different forms. This chapter includes a brief discussion of multiple-proxy anonymity networks followed by a more thorough description of basic **circumvention proxies** and how they work.

Both of these methods are effective ways to evade Internet filters, although the former is most appropriate if you are willing to sacrifice speed in order to keep your Internet activities as anonymous as possible. If you know and trust the individual or organization that operates your proxy, or if performance is more important to you than anonymity, then a basic circumvention proxy might serve you better.

What you can learn from this chapter

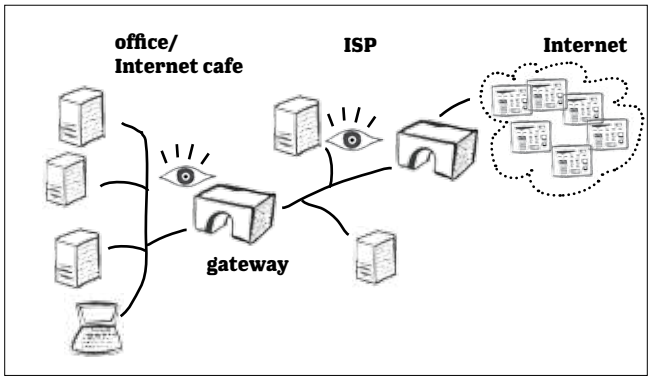
- How to access a website that is blocked from within your country
- How to prevent websites that you visit from knowing your location
- How to ensure that neither your **ISP** nor a surveillance organization in your country can determine which websites and Internet services you visit

UNDERSTANDING INTERNET CENSORSHIP

Research carried out by organisations like the *OpenNet Initiative (ONI)* [1] and *Reporters Without Borders (RSF)* [2] indicates that many countries filter a wide variety of social, political and 'national security' content, while rarely publishing precise lists of what has been blocked. Naturally, those who wish to control their citizens' access to the Internet also make a special effort to block known proxies and websites that offer tools and instruction to help people circumvent these filters.

Despite the guarantee of free access to information enshrined in Article 19 of the Universal Declaration of Human Rights, the number of countries engaged in Internet censorship has continued to increase dramatically over the past few years. As the practice of Internet filtering spreads throughout the world, however, so does access to the circumvention tools that have been created, deployed and publicised by activists, programmers and volunteers.

Before exploring the various ways to bypass Internet censorship, you should first develop a basic understanding of how these filters work. In doing so, it may be helpful to consider a greatly-simplified model of your connection to the Internet.



Your Internet connection

The first step of your connection to the Internet is typically made through an ***Internet Service Provider*** (**ISP**) at your home, office, school, library or Internet cafe. The ISP assigns your computer an **IP address**, which various Internet services can use to identify you and send you information, such as the emails and webpages you request. Anyone who learns your IP address can figure out what city you are in. Certain well-connected organisations in your country, however, can use this information to determine your precise location.

- **Your ISP** will know which building you are in or which phone line you are using if you access the Internet through a modem.
- **Your Internet cafe, library or business** will know which computer you were using at a given time, as well as which port or wireless access point you were connected to.
- **Government agencies** may know all of these details, as a result of their influence over the organisations above.

At this stage, your **ISP** relies on the network infrastructure in your country to connect its users, including you, with the rest of the world. On the other end of your connection, the website or Internet service you are accessing has gone through a similar process, having received its own IP addresses from an ISP in its own country. Even without all of the technical details, a basic model like this can be helpful when considering the various tools that allow you get around filters and remain anonymous on the Internet.

How websites are blocked

Essentially, when you go to view a webpage, you are showing the site's **IP address** to your **ISP** and asking it to connect you with the webserver's ISP. And, if you have an unfiltered Internet connection, it will do precisely that. If you are in a country that censors the Internet, however, it will first consult a **blacklist** of forbidden websites and then decide whether or not to comply with your request.

In some cases, there may be a central organisation that handles filtering in place of the **ISPs** themselves. Often, a blacklist will contain **domain names**, such as www.blogger.com, rather than **IP addresses**. And, in some countries, filtering software monitors your connection, rather than trying to block specific Internet addresses. This type of software scans through the requests that you make and the pages that are returned to you, looking for sensitive key words and then deciding whether or not to let you see the results.

And, to make matters worse, when a webpage is blocked you may not even know it. While some filters provide a 'block page' that explains why a particular page has been censored, others display misleading error messages. These messages may imply that the page cannot be found, for example, or that the address was misspelled.

In general, it is easiest to adopt a worst-case perspective toward Internet censorship, rather than trying to research all of the particular strengths and weaknesses of the filtering technologies used in your country. In other words, you might as well assume that:

- Your Internet traffic is monitored for keywords
- Filtering is implemented directly at the **ISP** level
- Blocked sites are **blacklisted** by both their **IP addresses** and their **domain names**
- You may be given an unclear or misleading reason to explain why a blocked site fails to load.

Because the most effective circumvention tools can be used regardless of which filtering methods are in place, it does not generally do any harm to make these pessimistic assumptions

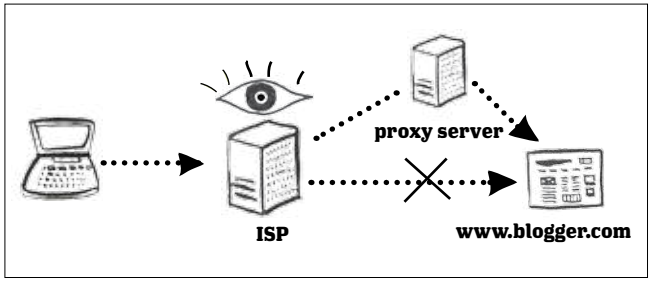
However, if you find that you cannot access some material online that your contacts in other countries still can access, it doesn't necessarily mean it's been blocked for political reasons. There are a number of possible causes for this. In any case, perhaps you should try visitng the site using a circumvention tool, most of which rely on external proxy servers, which is a bit like asking a friend in another country to test a website for you, except you get to do it yourself!

UNDERSTANDING CENSORSHIP CIRCUMVENTION

If you cannot go directly to a website because it is blocked by one of the methods discussed above, you will need to find a way around the obstruction. A secure **proxy** server, located in a country that does not filter the Internet, can provide this kind of detour by fetching the webpages you request and delivering them to you. From your **ISP**'s perspective, you will simply appear to be communicating securely with an unknown computer (the proxy server) somewhere on the Internet.

Of course, the government agency in charge of Internet censorship in your country (or the company that provides updates for its filtering software) might eventually learn that this 'unknown computer' is really a circumvention proxy. If that happens, its **IP address** may itself be added to the blacklist, and it will no longer work. It usually takes some time for proxies to be blocked, however, and those who create and update circumvention tools are well aware of this threat. They typically fight back using one or both of the following methods:

- **Hidden proxies** are more difficult to identify. This is one of the reasons why it is important to use secure proxies, which tend to be less obvious. **Encryption** is only part of the solution, however. The operators of a proxy must also take care when revealing its location to new users if they want it to remain hidden.
- **Disposable proxies** can be replaced very quickly after they are blocked. In this case, the process of telling users how to find replacement proxies may not be particularly secure. Instead, circumvention tools of this type often simply try to distribute new proxies faster than they can be blocked.



In the end, as long as you can reach a **proxy** that you trust to fetch the services you ask for, all you have to do is send it your requests and view whatever comes back using the appropriate Internet application. Typically, the details of this process are handled automatically by circumvention software that you install on your computer, by modifying your browser settings or by pointing your browser to a web-based proxy page. The **Tor** anonymity network, described below, uses the first method. Following that is a discussion of basic, single-proxy circumvention tools, each of which works in a slightly different manner.

ANONYMITY NETWORKS AND BASIC PROXY SERVERS

Anonymity networks

Anonymity networks typically 'bounce' your Internet traffic around between various secure **proxies** in order to disguise where you are coming from and what you are trying to access. This can significantly reduce the speed at which you are able to load websites and other Internet services. In the case of Tor, however, it also provides a reliable, secure and public means of circumvention that saves you from having to worry about whether or not you trust the individuals who operate your proxies and the websites you visit. As always, you must ensure that you have an encrypted connection, using **HTTPS**, to a secure website before exchanging sensitive information, such as passwords and emails, through a browser.

You will have to install software to use **Tor**, but the result is a tool that provides anonymity as well as circumvention. Each time you connect to the Tor network, you select a random path through three secure **Tor proxies**. This ensures that neither your ISP nor the proxies themselves know both your computer's **IP address** and the location of the Internet services you request. You can learn much more about this tool from the *Tor Guide*.

Hands-on: Get started with *Tor* – *Digital Anonymity and Circumvention*

One of Tor's strengths is that it does not just work with a browser but can be used with various types of Internet software. Email programs, including Mozilla **Thunderbird**, and instant messaging programs, including **Pidgin**, can operate through Tor, either to access filtered services or to hide your use of those services.

Basic circumvention proxies

There are three important questions that you should consider when selecting a basic circumvention **proxy**. First, is it a web-based tool or does it require you to change settings or install software on your computer? Second, is it secure? Third, is it private or public?

Web-based and other proxies:

Web-based **proxies** are probably the easiest to use. They require only that you point your browser at a proxy webpage, enter the filtered address you wish to view and click one button. The proxy will then display the requested content inside its own webpage. You can follow links normally or enter a new address into the proxy if you want to view a different page. You do not need to install any software or change any browser settings, which means that web-based proxies are:

- Easy to use
- Reachable from public computers, such as those at Internet cafes, that may not allow you to install programs or change settings
- Potentially safer if you are concerned about being 'caught' with circumvention software on your computer

Web-based proxies tend to have certain disadvantages, as well. They do not always display pages correctly, and many web-based proxies will fail to load complex websites, including those that feature streaming audio and video content. Also, while any proxy will slow down as it gains more users, this tends to be more of an issue with public web-based proxies. And, of course, web-based proxies only work for webpages. You can not, for example, use an instant messaging program or an email client to access blocked services through a web-based proxy. Finally, secure web-based proxies offer limited confidentiality because they must themselves access and modify the information returned to you by the websites you visit. If they did not, you would be unable to click on a link without leaving the proxy behind and attempting to make a direct connection to the target webpage. This is discussed further in the following section.

Other types of proxies generally require you to install a program or configure an external proxy address in your browser or operating system. In the first case, your circumvention program will typically provide some way of turning the tool on and off, which will tell your browser whether or not to use the proxy. Software like this often allows you to change proxies automatically if one is blocked, as discussed above. If you have to configure an external proxy address in your browser or operating system, you will need to learn the correct proxy address, which may change if that proxy is blocked or slows down so much that it becomes unusable.

Although it may be slightly more difficult to use than a web-based proxy, this method of circumvention is more likely to display complex pages correctly and may take longer to slow down as more people begin to use a given proxy server. Furthermore, proxies can be found for a number of different Internet applications. Examples include HTTP proxies for browsers, SOCKS proxies for email and chat programs and VPN proxies, which can redirect all of your Internet traffic to avoid filtering.

Secure and insecure proxies:

A secure proxy, in this chapter, refers to any **proxy** that supports **encrypted** connections from its users. An insecure proxy will still allow you to bypass many types of filtering, but will fail if your Internet connection is being scanned for key words or particular website addresses. It is a particularly bad idea to use an insecure proxy when accessing websites that are normally encrypted, such as webmail accounts and banking websites. By doing so, you may expose sensitive information that would normally be hidden. And, as mentioned previously, insecure proxies are often easier for those who update Internet filtering software and policies to discover and block. In the end, the fact that free, fast, secure proxies exist means that there are very few good reasons to settle for an insecure one.

You will know that a web-based proxy is secure if you can access the proxy webpage itself using an **HTTPS** address. As with webmail services, secure and insecure connections may be supported, so you should be certain to use the secure address. It may happen that, in such cases, you will be asked to accept a 'security certificate warning' from your browser in order to continue. This is the case for the **Peacefire** proxy, discussed below. Warnings like this tell you that someone, such as your ISP or a hacker, could be monitoring your connection to the proxy. Despite these warnings, it may be still a good idea to use secure proxies whenever possible. However, when relying on such proxies for circumvention, you should avoid visiting secure websites unless you verify the proxy's **SSL** fingerprint. In order to do this, you will need a way of securely communicating with the proxy's administrator. It is best not to enter passwords or exchange sensitive information when using web proxies in general.

Appendix C of the *Psiphon User's Guide* explains the steps that both you and the proxy administrator should follow in order to verify the proxy's fingerprint.

You should also avoid accessing sensitive information through a web-based proxy unless you trust the person who runs it. This applies

regardless of whether or not you see a security certificate warning when you visit the proxy. It even applies if you know the proxy operator well enough to verify the server's fingerprint before directing your browser to accept the warning. When you rely on a single proxy server for circumvention, its administrator will always know your IP address and which websites you are accessing. More importantly, however, if that proxy is web-based, a malicious operator could gain access to all of the information that passes between your browser and the websites you visit, including the content of your webmail and your passwords.

For proxies that are not web-based, you may have to do a little research to determine whether or not secure connections are supported. All of the proxies and anonymity networks recommended in this chapter are secure.

Private and public proxies:

Public proxies accept connections from anyone, whereas private **proxies** typically require a username and password. While public proxies have the obvious advantage of being freely available, assuming they can be found, they tend to become overcrowded very quickly. As a result, even though public proxies may be as technically sophisticated and well-maintained as private ones, they are often relatively slow. Finally, private proxies tend to be run either as for-profit businesses or by administrators who create accounts for users that they know personally or socially. Because of this, it is generally easier to determine what motivates the operators of a private proxy. You should not assume, however, that private proxies are therefore fundamentally more trustworthy. After all, the profit motive has led online services to expose their users in the past.

Simple, insecure, public proxies can often be found by searching for terms like 'public proxy' in a search engine, but you should not rely on proxies discovered this way. Given the choice, it is better to use a private, secure proxy run by people that you know and trust, either personally or by reputation, and who have the technical skill to keep their server secure. Whether or not you use a web-based proxy will depend on your own particular needs and preferences. Any time you are using a proxy for circumvention, it is also a good idea to use the **Firefox** browser and to install the NoScript browser extension, as discussed in the *Firefox Guide*. Doing so can help protect you both from malicious **proxies** and from websites that might try to discover your real **IP address**. Finally, keep in mind that even an encrypted proxy will not make an insecure website secure. You must still ensure that you have an **HTTPS** connection before sending or receiving sensitive information.

If you are unable to find an individual, organisation or company whose proxy service you consider trustworthy, affordable and accessible from your country, you should consider using the Tor anonymity network, which is discussed above, under *Anonymity networks*.

Human Rights Defender Testimonies

We use Tor Browser a lot to remain anonymous when we are getting in touch with other MSM men. That is because you never know who is watching what sites you are going to. All my searches on Google used to show on my history, but with Tor, that is not the case.
Anonymous Human Rights Defender

SPECIFIC CIRCUMVENTION PROXIES

Below are a few specific tools and proxies that can help you circumvent Internet filtering. New circumvention tools are produced regularly, and existing ones are updated frequently, so you should visit the online Security in-a-Box website, and the resources mentioned in the *Further reading* section below, to learn more.

Virtual Private Network (VPN) based proxies

VPN proxies listed below make your entire Internet connection pass through the proxy while you are "connected". This can be helpful if you use email or instant messaging providers that are filtered in your country

Riseup VPN is for users who have email accounts on the Riseup server. The collective offers the possibility of connecting to a secure, private, free VPN proxy server. Please read more about ***Riseup VPN*** [3] and ***how to connect to it*** [4].

Hotspot Shield is a public, secure, VPN, freeware circumvention proxy. In order to use it, you will need to download the tool and install it. The company that develops Hotspot Shield receives funding from advertisers, so you will see a "banner ad" at the top of your browser window whenever you use it to visit websites that do not provide **encryption**. Although it is impossible to verify, this company claims to delete the **IP addresses** of those who use the tool, rather than storing or sending them to advertisers. [5].

Your-Freedom is a private, secure, VPN/SOCKS circumvention **proxy.** It is a **freeware** tool that that can be used to access a free

circumvention service. There are restrictions on bandwidth and for how long can you can use it (3 hours per day, up to 9 hours per week). You can also pay a fee to access a commercial service, which is faster and has fewer limitations. In order to use Your-Freedom, you will need to download the tool and create an account, both of which can be done at the ***Your-Freedom website*** [6]. You will also need to configure your browser to use the **OpenVPN** proxy when connecting to the Internet. You can read more in ***Your-Freedom documentation*** [7].

Freegate is a public, secure, VPN, freeware circumvention proxy. You can download the ***latest version of Freegate*** [8] or read an ***interesting article*** about it [9].

SecurityKISS is a public, secure, VPN, freeware circumvention proxy. To use it you need to ***download and run a free program*** [10]. There is no need to register an account. Free users are restricted to a 300 MB per day usage limit and by higher Internet traffic through the proxy. Paid subscription offers restriction-free usage and more VPN servers. Please see ***the SecurityKISS homepage*** [11] to learn more.

Psiphon3 is a secure, public circumvention tool that utilizes VPN, SSH and HTTP Proxy technology to provide you with uncensored access to Internet content. In order to use it you need to download the program from the ***Psiphon3 homepage*** [12] and run it to select which mode you would like to use [VPN, SSH, SSH+]. Psiphon3 works with Android devices as well. Please see the ***homepage*** to learn more.

Web Proxies:

Peacefire maintains a large number of public, web-based proxies, which can be secure or insecure, depending on how you access them. When using a Peacefire proxy, you must enter the HTTPS address in order to have a secure connection between yourself and the proxy. New proxies are announced to a large mailing list on a regular basis. You can sign up to receive updates at the ***Peacefire website*** [13].

FURTHER READING

- See the *Internet Surveillance and Monitoring* and *Censorship circumvention* chapters of the *Digital Security and Privacy Manual for Human Rights Defenders* book [14].
- The FLOSS Manuals website contains a guide on *How to Bypass Internet Censorship* [15].
- The *Internet Censorship Wiki* [16], written by Freerk, is available in English, German and Spanish.
- The CitizenLab has produced *Everyone's guide to by-passing Internet Censorship* [17], which is being translated into Burmese, English, French, Russian, Spanish and Urdu.
- Reporters Without Borders has released a second edition of its *Handbook for Bloggers and Cyberdissidents* [18], which is available in Arabic, Burmese, Chinese, English, Farsi, French, Russian and Spanish.
- Ethan Zuckerman of Global Voices Online has published a useful guide to *Anonymous Blogging with Wordpress and Tor* [19].

LINKS

[1] ***www.opennet.net***
[2] ***www.rsf.org***
[3] ***https://help.riseup.net/en/riseup-vpn***
[4] ***https://we.riseup.net/riseuphelp+en/vpn-howto***
[5] ***www.hotspotshield.com***
[6] ***http://your-freedom.net/***
[7] ***https://www.your-freedom.net/index.php?id=doc***
[8] ***www.dit-inc.us/freegate***
[9] ***http://www.addictivetips.com/windows-tips/freegate-lets-you-access-blocked-websites-at-optimal-speed/***
[10] ***http://www.securitykiss.com/resources/download/linux/***
[11] ***http://www.securitykiss.com/***
[12] ***http://psiphon3.com***
[13] ***www.peacefire.org***
[14] ***www.frontlinedefenders.org/esecman***
[15] ***http://en.flossmanuals.net/bypassing-censorship/***
[16] ***www.en.cship.org/wiki/Main_Page***
[17] ***http://citizenlab.org/guides/everyones-guide-english.pdf***
[18] ***http://en.rsf.org/IMG/pdf/guide_gb_md-2.pdf***
[19] ***http://advocacy.globalvoicesonline.org/projects/guide/***

10
How to protect yourself and your data when using social networking sites

10. How to protect yourself and your data when using social networking sites

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Although these networks can be very useful, and promote social interaction both online and offline, when using them you may be making information available to people who want to abuse it. Think of a social networking site as being like a huge party. There are people there that you know, as well as some that you don't know at all. Imagine walking through the party with all your personal details, and up-to-the-minute accounts of what you are thinking, written on a big sign stuck on your back so that everyone can read it without you even knowing. Do you really want everyone to know all about you?

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with.

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

We do not encourage you to stop using social networking tools

altogether. However you should take proper security measures, so that you can use these tools without making yourself or anyone else vulnerable.

What you can learn from this chapter

- How social networking sites make it easy for sensitive information to be revealed unintentionally
- How to safeguard information about yourself and others when using social networking sites

GENERAL TIPS ON USING SOCIAL NETWORKING TOOLS

- **Always ask the questions:**
  - Who can access the information I am putting online?
  - Who controls and owns the information I put into a social networking site?
  - What information about me are my contacts passing on to other people?
  - Will my contacts mind if I share information about them with other people?
  - Do I trust everyone with whom I'm connected?
- Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine. See *Chapter 3. How to create and maintain secure passwords for more information*.
- Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.
- Consider using **separate accounts/identities**, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine. See *Chapter 6: How to destroy sensitive information*.
- **Access social networking sites using https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site. See *Chapter 8: How to remain anonymous and bypass censorship on the internet*.

- Be careful about putting too much information into your **status updates** – even if you trust the people in your networks. It is easy for someone to copy your information.
- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts**! You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. **Never rely on a social networking site as a primary host for your content or information**. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

POSTING PERSONAL DETAILS

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common.

In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities.

The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- birth dates
- contact phone numbers
- addresses
- details of family members
- sexual orientation
- education and employment history

Friends, followers and contacts

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded individuals that you have never met. The most important thing to understand is

what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

Status updates

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for "Protect Your Tweets". In Facebook, change your settings to share your updates with "Friends Only". Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

Sharing internet content

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have?

If you say you like a site which is in some way related to bringing down a repressive regime, that regime might take an interest and then target you. If you want your contacts to be the only people to see the things you share or mark as interesting, make sure you check your privacy settings.

Revealing your location

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

See also *On Locational Privacy, and How to Avoid Losing it Forever* from the Electronic Frontier Foundation website [1].

Sharing videos/photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

Instant chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to **HTTPS** (and is more prone to exposure).

It is more secure to use a specific application for your chats, such as Pidgin with OTR, which uses encryption. Read the *Pidgin with OTR – secure instant messaging hands-on guide*.

Joining/creating groups, events and communities

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing

something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. If you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps you have set up a gay and lesbian support group to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

Hands-on: Get started with the *Social networking tools: Facebook, Twitter, YouTube and others guide*

Human Rights Defender Testimonies

"I get targeted as a woman especially as an older woman usually on Facebook with people who might have checked my profile and seen "Interested in: women". In the past I didn't even know how to delete someone from my friends list or from my Skype but after a training I sat down and sifted through my friends list and removed the ones I felt I did not know and including those who have been harassing me."
Anonymous Human rights Defender

"Facebook is the most used to target people. Its very deceptive because you are seeing pictures which people claim are of themselves, but sometimes they are not. What made me able to handle these situations was first to check for how long the person has been registered. Then if they are a new registration, I start to wonder why are they trying to friend me. Secondly, there are people with whom you only have one common friend, and if that common friend is very remote, that is also a bad sign. Then when I go to photos and I see only one photo or four photos maximum, ahhh! Sometimes, I see that they are all profile pictures of different people and those people don't even look the same. It gives me a hint that the photos have been stolen or photoshopped to give people a false impression. I have learned to really check before giving people access to my profile."
Anonymous Human rights Defender

LINK

[1] *www.eff.org/wp/locational-privacy*

11
How to protect yourself and your data when using LGBT dating sites

11. How to protect yourself and your data when using LGBT dating sites

For LGBT individuals, particularly in repressive political or social environments, it is quite common to turn to the internet as a means of communicating with, and meeting other people like you. This is quite natural, especially since the internet connects us to such a vast and diverse global community, and also gives us a certain feeling of anonymity. LGBT dating sites are also particularly useful in this respect..

However, while these sites represent a wonderful resource for meeting people and expressing ourselves where we otherwise can't or may not want to, they are not necessarily the safe, anonymous spaces we want them to be and, unless we are careful, our interaction with them could facilitate an undesired 'outing', or much worse. In some countries, personal disagreements have led to some LGBT people having their dating site profiles being printed out and posted to their families. In others, like Egypt, LGBT individuals have been preyed upon by authorities who have subjected them to entrapment through creating fake profiles and lying to them.

Therefore, while these sites may be a good – or indeed the only – way of meeting new people, it's a good idea to keep the following information, tips, and tools in mind in order to stay safe.

Example incidents

In Nigeria, police and ordinary citizens set up profiles on dating sites to attract gay men. In 2012, a newspaper article appeared to glorify one of such groups that had set up a punishment group that trapped and specialized in extorting gay men. 'We call them up, set a meeting in a hotel room then snap pictures in compromising positions. We then use this to collect money from them' said one of the young men.

The Gay and Lesbian Coalition of Kenya say incidents of blackmail and extortion are high and constantly growing within the country and account for one of the highest crimes commited against LGBTI persons. [1]

What you can learn from this chapter

- Some of the technical vulnerabilities of common dating sites that may put you at risk, and useful strategies for overcoming them
- How to safeguard information about yourself and others when using LGBT dating sites

KEEPING YOUR PRIVATE BITS PRIVATE

Browsing history and cookies

It's a good idea to minimize evidence of your use of LGBT dating sites on your computer, should anyone else inadvertently discover it through using, stealing or finding your computer.

The first and most basic step is to simply delete your browsing history after each use, or disable browsing history altogether.

Many websites, particularly social networking sites, store small files called cookies on your computer, which collect information about your interaction with that website and others, so that they can provide you with advertisements relevant to your interests. Therefore, if you are logged into an account such as Facebook or Google while also logged into your dating site profile (even in a different tab), these sites may collect this information about you and use it to serve you advertisements, or even hand it over to third parties. It's a good idea to disable cookies on your browser any time you log into a dating site, to avoid linking your use of this site to any of your other online profiles or activities.

If you'd like to securely delete your browsing history, cookies and other temporary internet files, there are a number of easy-to-use Free and Open-Source Software (FOSS) tools which can help you with this. In particular, we recommend **CCleaner** and **Eraser**.

Finally, be aware that dating sites, like many social networks, are fertile ground for hackers who wish to spread malware. They usually attempt this by creating a fake profile and sending messages, which encourage viewers and recipients to click on a link to "their website" or "their videos". However, you can protect yourself from this threat by observing a very simple principle: if you do not know the sender, simply do not click on any hyperlink they send you, especially if their profile or messages appear suspicious.

For more on these topics, see *Chapter 1: How to protect your computer from malware and hackers*; *Chapter 2: How to protect your information from physical threats*, and *Chapter 10: How to protect yourself and your data when using social networking sites.*

Hands-on: Get started with the
Eraser – Secure File Removal Guide

Hands-on: Get started with the
Avast – Anti-Virus Guide

SSL connection

It's very important to choose a dating site that provides a **Secure Socket Layer connection** (SSL), also known as https. This means that, although someone monitoring your internet traffic will still be able to tell that you are visiting the site, all the communication between your computer and the website's servers will be encrypted. While most sites provide an SSL connection on their login page, they may not provide it for the rest of your interaction with the site – meaning that any profile updates, messages, and pictures you send or receive will be as visible to observers, such as your ISP, as postcards are to a postman. In order to check whether your dating site provides SSL, log in and then check if the address in the browser's address bar begins with "https://". Keep in mind that some sites, such as PlanetRomeo, give you a "secure connection" option on the login page; if you see this, make sure the box is ticked before entering your details. If your site does not provide SSL, we suggest you delete your profile and switch to a site which does. For more information, see Chapter 7: How to keep your internet communication private. If you feel you must continue using a site which doesn't provide SSL, it's imperative that you connect using a circumvtion and anonymity tool such as **Tor** or a **VPN**(see below).

Hands-on: Get started with the
Firefox with add-ons Secure web browser Guide

Circumvention and Anonymous browsing

As noted above, while an SSL connection will protect the content you send to, or receive from, the dating site's servers, it does not make you anonymous. Your computer's **IP address**, and the IP address of the website's servers will still be visible to your ISP, the website's administrators, and possibly others. However, there are solutions to this problem. If anonymity is important to you, there are simple steps you can take to communicate anonymously with the website, such as using the Tor Browser or a **Virtual Private Network (VPN)** connection.

These tools are circumvention tools, which also means that they can be used to access content which would otherwise be censored. For more information on circumvention and anonymity, see Chapter 8: How to remain anonymous and bypass censorship on the internet.

Hands-on: Get started with the
Tor – Digital Anonymity and Circumvention Guide

Mobile apps

Mobile computing devices such as smartphones and tablets have become extremely popular means of communication, combining mobile telephony with instant access to much of our favourite internet content and social networking applications all in one place.

LGBT sites have been quick to adapt to this change, and most major dating sites such as PlanetRomeo, Gaydar, and Scruff now boast their own applications. Moreover, some apps, such as Grindr, are designed especially to take advantage of smartphone and tablet features, such as GPS, in order to broadcast your location to possible partners near you.

Aside from the obvious possible dangers of broadcasting your location and identity as an LGBT individual to other people near you, there are a number of other disadvantages to the smartphone and tablet format, including:

- Many of these apps do not provide an SSL connection, even if their websites do;
- Downloading the apps from the Appstore or Google Play will link them directly to your Apple ID or Google account;
- Your mobile operator will also collect this information, linking it directly to your identity;
- Other social networking apps such as Facebook or Twitter may also collect this information about you

Therefore, we recommend that if your privacy as an LGBT individual is important to you, you do not use mobile apps designed for dating. You can read more about smartphones and tablets in *Chapter 11: How to use smartphones as securely as possible*.

YOU AND DATING SITES

Your identity and financial information

Unfortunately, dating sites are not usually run as non-profit organisations. Rather, they are businesses which aim to profit, and tend to do this in two ways: firstly, though offering a "premium" version of the site, with added features, for an extra fee, and secondly, through collecting as much information as possible about all users in order to pass on to third parties, usually advertisers.

As a result, these websites are often quite keen for you to volunteer as much information about yourself to them as possible. Some sites, like Manjam, even ask for your full name in order to create a profile, and any site which offers a "premium" service will also ask for your credit card details. Naturally, your name and financial details are highly sensitive and will directly link your identity to your activities on the website, which may be illegal. Moreover, many dating sites state in their privacy policies that they will hand over your personal information to third parties, including authorities, if there is a legal request made for them to do so. You should only volunteer real information about yourself which you consider strictly necessary, and never provide your full name, telephone number, or credit card details to a dating site.

Read more in *Chapter 10: How to protect yourself and your data while using social networking sites*.

About exchanging pictures

Before you meet someone, it's a good idea to ask for various pictures of them, which will give you a better idea of how genuine they are. If someone outright refuses to exchange pictures with you before meeting, this is cause for suspicion and best avoided, unless you can verify that they are genuine by other means (such as through your community – see below).

If someone sends you a picture which you think might be fake or taken from a website, you can drag the image into the google image searchbar to find out whether it has been taken from a website. You might also want to read the metadata of the picture. For more, see the metadata stripping hands-on guide.

Regarding your own pictures, while someone might reasonably expect to see you before meeting to ensure that you are genuine, it's a good security practice to at least keep your pictures private until someone asks for them, and only send them in exchange for others. It might also be advisable to strip the metadata from the images before sending them, so as to keep secret information such as the location in which it was taken, the time, the camera make, etc.

Human Rights Defender Testimonies

"If you go on some social network and you let people know you're a lesbian, or even if you don't and some guy would just pretend that he's a girl and you think you're talking to a girl, you start exchanging pictures and he keeps all the pictures. He would even send a nude picture of a girl! I met someone on Badoo once, we were talking, so I said 'give me your number' but I couldn't call immediately. So later I called and it was a guy's voice!"

Anonymous Human Rights Defender

Hands-on: Get started with the *Metanull - Image Metadata Stripper Guide*

Establishing contact and meeting

Before you agree to meet someone, you should establish contact over the phone with them first. Rather than use your house phone or mobile phone, it might be best to use a Voice over IP program such as **jitsi** or **skype**, or arrange to talk over public telephones.

Finally, before meeting someone, it is best to check among your other LGBT contacts and community, if you have one, whether anyone knows or has heard of him or her, as they may be able to alert you as to whether or not the person is trustable.

Too good to be true?

If you come across, or are contacted by someone who seems suspiciously 'perfect', or you notice inconsistencies in the information they give you about themselves you should be cautious. Are their high quality pictures a little too professional-looking? Should they be sharing their face-pics in your city, region or country? Do they sound a little too eager to meet or see a picture of your face, or are they unwilling to exchange pictures? If you have doubts, it's best to steer clear, and check with your friends and contacts whether anyone knows of this person.

GENERAL TIPS AND ADVICE FOR PARTICULAR SITES

As with any social networking site, and especially given the threats facing LGBTI people, it's a good idea to ask the following questions before using an LGBTI dating site.

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me are my contacts passing on to other people?
- Will my contacts mind if I share information about them with other people?
- Do I trust everyone with whom I'm connected?

Advice for particular sites

Manjam

In order to create a profile on Manjam, your personal information including your first and last names are requested. According to their privacy policy, this information will be collected and may be shared with third parties, including in case of a legal request. You should avoid sharing this information when creating a profile at all costs: there is no good reason to give your real name, so give a fake one.

Manjam has a useful guide to safe practices when using their site here: *http://www.manjam.com/support/safetytips.aspx*

Gaydar and GaydarGirls

If you use Gaydar or GaydarGirls, make sure the box next to "secure session" is ticked when you log in, to ensure your session will use SSL. You can make sure that this is always the case by using the HTTPS Everywhere add-on for Firefox.

PlanetRomeo

If you use PlanetRomeo, also ensure that the box next to "secure login" is ticked when you log in, to ensure your session will use SSL. You can make sure that this is always the case by using the HTTPS Everywhere add-on for Firefox.

Planetromeo has a useful guide to safe practices when using their site, under "*Help and Services*".

Grindr

As noted above, Grindr is a smartphone application. If your privacy and security is important to you, it is strongly recommended that you do not use Grindr.

FURTHER READING

- See the Protection International *Protection Manual for LGBTI Defenders* ***http://protectioninternational.org/publication/protection-manual-for-lgbti-defenders-2nd-edition/***
- See Manjam's 10 tips for online safety. *https://www.manjam.com/support/safetytips.aspx*
- See Planetromeo's safety tips, under "*Help and Service*".

LINK

[1] = ***http://irasciblemusings.com/nairobi-police-say-closeted-gays-being-blackmailed-and-attacked-by-gangs-2/***

12
How to use mobile phones as securely as possible

12. How to use mobile phones as securely as possible

Mobile phones are an integral part of our daily communications. All mobile phones have the capacity for voice and simple text messaging services. Their small size, relatively low cost and many uses make these devices invaluable for rights advocates who increasingly use them for communication and organisation.

Recently, mobile devices with many more functions have become available. They may feature **GPS**, multimedia capacity (photo, video and audio recording and sometimes transmitting), data processing and access to the internet. However, the way the mobile networks operate, and their infrastructure, are fundamentally different from how the internet works. This creates additional security challenges, and risks for users' privacy and the integrity of their information and communications.

It is important to start with the understanding that mobile phones are inherently insecure:

- Information sent from a mobile phone is vulnerable.
- Information stored on mobile phones is vulnerable.
- Phones are designed to give out information about their location.

We will explore these issues, and what a user can do in light of these inherent vulnerabilities.

What you can learn from this chapter

- Why communication and storing data on mobile phones is not secure
- What steps you can take to increase the security of using mobile phones
- How can you minimise the chances of being spied on or tracked via your mobile phone
- How can you maximise the chances of remaining anonymous while using your mobile phone

MOBILE DEVICES AND SECURITY

We need to make informed decisions when using mobile phones, in order to protect ourselves, our contacts and our data. The way mobile phone networks and infrastructure work can significantly affect users' ability to keep information and communications private and secure.

- Mobile networks are private networks run by commercial entities, which can be under the monopoly control of the government. The

commercial entity (or government), has practically unlimited access to the information and communications of customers, as well as the ability to intercept calls, text messages, and to monitor the location of each device (and therefore its user).

- The Operating Systems used on mobile devices themselves are custom-designed or configured by phone manufacturers according to the specifications of various service providers and for use on these companies' own networks. As a result, the OS may well include hidden features enabling better monitoring by the service provider of any particular device.
- The number of functions available on mobile phones has grown in the past few years. Modern mobile phones are in fact internet-connected portable mini-computers with mobile phone functions.

In order to work out which aspects of your communications most need to be protected, it may help to ask yourself a few questions: ***What is the content of your calls and text messages? With whom do you communicate, and when? Where are you calling from?*** Information is vulnerable in many ways:

- **Information is vulnerable when sent from a mobile phone**
  Example: Each mobile phone provider has full access to all text and voice messages sent via its network. Phone providers in most countries are legally obliged to keep records of all communications. In some countries the phone providers are under the monopoly control of government. Voice and text communication can also be tapped by third parties in proximity to the mobile phone, using inexpensive equipment.
- **Information is vulnerable within the sender's and the recipient's phones**
  Example: Mobile phones can store all sorts of data: call history, text messages sent and received, address book information, photos, video clips, text files. These data may reveal your network of contacts, and personal information about you and your colleagues. Securing this information is difficult, even – on some phones – impossible. Modern mobile phones are pocket-sized computers. With more features comes higher risk. In addition, phones that connect to the internet are also subject to the insecurities of computers and of the internet.
- **Phones give out information about their location**
  Example: As part of normal operation, every mobile phone automatically and regularly informs the phone service provider where it is at that moment. What's more, many phones nowadays have **GPS** functions, and this precise location information may be embedded in other data such as photos, SMS and internet requests that are sent from the phone.

The evolution of technology brings more features, but also more risks.

The following sections discuss a number of simple steps you can take to decrease the likelihood of security threats arising from using mobile devices.

MOBILITY AND THE VULNERABILITY OF INFORMATION

People often carry mobile phones that contain sensitive information. Communications history, text and voice messages, address books, calendar, photos and many other useful phone functions can become highly compromising if the phone or the data is lost or stolen. It is vital to be aware of the information that is stored, both actively and passively, on your mobile phone. Information stored on a phone could implicate the person using the phone as well as everyone in their address book, message inbox, photo album, etc.

Mobile phones that connect to the internet are also subject to the risks and vulnerabilities associated with the internet and computers, as discussed in the other chapters of this book regarding information security, anonymity, information retrieval, loss, theft and interception. In order to reduce some of these security risks, users should be aware of their phone's potential for insecurity, as well as its set-up options. Once you know what the possible problems may be, you can put safeguards into place and take preventative measures.

Best practices for phone security

As is the case with other devices, the first line of defence for the safety of the information on your mobile phone is to physically protect the phone and its **SIM card** from being taken or tampered with.

- Keep your phone with you at all times. Never leave it unattended. Avoid displaying your phone in public.
- Always use your phone's security lock codes or Personal Identification Numbers (PINs) and keep them secret (unknown to others). Always change these from the default factory settings.
- Physically mark (draw on) the SIM card, additional memory card, battery and phone with something unique and not immediately noticeable to a stranger (make a small mark, drawing, letters or numbers, or try using ultra-violet marker, which will be invisible in normal light). Place printed tamper-proof security labels or tape over the joints of the phone. This will help you easily to identify whether

any of these items have been tampered with or replaced (e.g. the label or tape will be mis-aligned, or leave a noticeable residue).

- Make sure that you are aware of the information that is stored on your SIM card, on additional memory cards and in your phone's memory. Don't store sensitive information on the phone. If you need to store such information, consider putting it on external memory cards that can easily be discarded when necessary – don't put such details into the phone's internal memory.
- Protect your SIM card and additional memory card (if your phone has one), as they may contain sensitive information such as contact details and SMS messages. For example, make sure that you do not leave them at the repair shop when your phone is being serviced.
- When disposing of your phone make sure you are not giving away any information that is stored on it or on the SIM or memory card (even if the phone or cards are broken or expired). Disposing of SIM cards by physically destroying them may be the best option. If you plan to give away, sell or re-use your phone make sure that all information is deleted.
- Consider using only trusted phone dealers and repair shops. This reduces the vulnerability of your information when getting second-hand phones or having your phone repaired. Consider buying your phone from an authorised but randomly chosen phone dealer – this way you reduce the chance that your phone will be specially prepared for you with spying software preinstalled on it.
- Back up your phone information regularly to a computer. Store the backup safely and securely (see *Chapter 4: How to protect the sensitive files on your computer*). This will allow you to restore the data if you lose your phone. Having a backup will also help you remember what information might be compromised (when your phone is lost or stolen), so you can take appropriate actions.
- The 15-digit serial or IMEI number helps to identify your phone and can be accessed by keying *#06# into most phones, by looking behind the battery of your phone or by checking in the phone's settings. Make a note of this number and keep it separate from your phone, as this number could help to trace and prove ownership quickly if it is stolen.
- Consider the advantages and disadvantages of registering your phone with the service provider. If you report your phone stolen, the service provider should then be able to stop further use of your phone. However, registering it means your phone usage is tied to your identity.

Basic functions, trackability and anonymity

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time.

This is also the case when the phone is switched off. If you really don't want to be traced in a given moment, the best thing to do is take the battery out of your phone, or give the phone to someone else who will go to a different location.

About anonymity

If you are conducting sensitive phone conversations or sending sensitive SMS messages, beware of the above tracking 'feature' of all mobile phones. Consider adopting the steps below:

- Make calls from different locations each time, and choose locations that are not associated with you.
- Keep your phone turned off, with the battery disconnected, go to the chosen location, switch your phone on, communicate, switch the phone off and disconnect the battery. Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.
- Change phones and SIM cards often. Rotate them between friends or the second-hand market.
- Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you.

Be aware that phones can also be infected with different types of malware designed for spying. Such malware can perform tasks like remotely switching it on and having it call a number without your knowledge, through which your conversations and daily life can be eavesdropped. In some cases, this can be avoided by removing the battery, though it is often safer simply not to bring the phone with you.

About eavesdropping

Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

- Never let people whom you don't trust get physical access to your

phone; this is a common way of installing spying software on your phone.
- If you are conducting private and important meetings, switch your phone off and disconnect the battery. Or don't carry the phone with you if you can leave it where it will be absolutely safe.
- Make sure that any person with whom you communicate also employs the safeguards described here.
- In addition, don't forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

About interception of calls

Typically, **encryption** of voice communications (and of text messages) that travel through the mobile phone network is relatively weak. There are inexpensive techniques which third parties can use to intercept your written communications, or to listen to your calls, if they are in proximity to the phone and can receive transmissions from it. And of course, mobile phone providers have access to all your voice and text communications. It is currently expensive and/or somewhat technically cumbersome to encrypt phone calls so that even the mobile phone provider can't eavesdrop – however, these tools are expected to become cheaper soon. To deploy the encryption you would first have to install an encryption application on your phone, as well as on the device of the person with whom you plan to communicate. Then you would use this application to send and receive encrypted calls and/or messages. Encryption software is currently only supported on a few models of so-called 'smart' phones.

Conversations between **Skype** and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place.

Text based communications – SMS / text messages

You should not rely on text message services to transmit sensitive information securely. The messages exchanged are in plain text which makes them inappropriate for confidential transactions.

Sent SMS messages can be intercepted by the service operator or by third parties with inexpensive equipment. Those messages will carry the phone numbers of the sender and recipient as well as the content of the message. What's more, SMS messages can easily be altered or forged by third parties.

Consider establishing a code system between you and your recipients. Codes may make your communication more secure and may provide an additional way of confirming the identity of the person you're communicating with. Code systems need to be secure and change frequently.

SMS messages are available after transmission:
- In many countries, legislation (or other influences) requires the network providers to keep a long-term record of all text messages sent by their customers. In most cases SMS messages are kept by the providers for business, accounting or dispute purposes.
- Saved messages on your phone can easily be accessed by anybody who gets hold of your phone. Consider deleting all received and sent messages straightaway.
- Some phones have the facility to disable the logging of phone-call or text-message history. This would be especially useful for people doing more sensitive work. You should also make sure that you are familiar with what your phone is capable of. Read the manual!

Human Rights Defender Testimonies

"Cellphones are used a lot, especially text messages, and they've been used for cases against people who get arrested. If you are an activist, and you get arrested and your phone is taken away, they use your messages to build a case against you. Also civilians: sometimes if a relationship breaks up and one person does not want to let go, for example in a place like Cameroon... even if I'm a lesbian, and I go to the police and say "look at this person, she's a lesbian, she's been bothering me, look at these messages she's been sending me...". They're gonna arrest the person, and they don't care about me. If you have money to pay them, especially. They won't look at what I sent to the person, but what the person sent me, and build a case."

Anonymous Human Rights Defender

Functions beyond speech and messages

Mobile phones are turning into mobile computing devices, complete with their own operating systems and downloadable applications that provide various services to the user. Consequently, viruses and spyware have penetrated the mobile phone world. Viruses can be planted on your phone, or come packaged within applications, ring tones and multimedia messages that you download from the internet.

While some of the earlier mobile phone models have fewer or no internet functions, it is nevertheless important to observe the precautions outlined below on all phones, to make absolutely certain

that your device is not compromised without your knowledge. Some of these precautions may apply only to Smartphones, but it is very important to find out exactly what the capabilities of your phone are, in order to be certain that you have taken appropriate measures:

- Do not store confidential files and photos on your mobile phone. Move them, as soon as you can, to a safe location, as discussed in *Chapter 4: How to Protect Files on Your Computer.*
- Frequently erase your phone call records, messages, address book entries, photos, etc.
- If you use your phone to browse the internet, follow safe practices similar to those you use when you are on the computer (e.g. always send information over encrypted connection like **HTTPS**).
- Connect your phone to a computer only if you are sure it is malware free. See *Chapter 1: How to Protect Your Computer From Malware and Hackers*.
- Do not accept and install unknown and unverified programmes on your phone, including ring tones, wallpaper, java applications or any others that originate from an unwanted and unexpected source. They may contain viruses, malicious software or spying programmes.
- Observe your phone's behaviour and functioning. Look out for unknown programmes and running processes, strange messages and unstable operation. If you don't know or use some of the features and applications on your phone, disable or uninstall them if you can.
- Be wary when connecting to WiFi access points that don't provide passwords, just as you would when using your computer and connecting to WiFi access points. The mobile phone is essentially like a computer and thus shares the vulnerabilities and insecurities that affect computers and the internet.
- Make sure communication channels like **Infra Red (IrDA)**, **Bluetooth** and Wireless Internet (WiFi) on your phone are switched off and disabled if you are not using them. Switch them on only when they are required. Use them only in trusted situations and locations. Consider not using Bluetooth, as it is relatively easy to eavesdrop on this form of communication. Instead, transfer data using a cable connection from the phone to handsfree headphones or to a computer.

FURTHER READING

- ***The Mobile Advocacy Toolkit*** [1] released by The Tactical Technology Collective. Among other things, this contains an extensive range of other tools and examples relating to their use.
- ***Security for Activists*** – A Practical Security Handbook for Activists and Campaigns [2].
- ***A Guide to Mobile Phones*** – A short guide, for activists, to using mobile phones safely and securely [3].
- ***A Brief Introduction to Secure SMS Messaging in MIDP*** – Nokia developer guide [4].
- ***Phones used as spying devices*** [5].

LINKS

[1] ***http://mobiles.tacticaltech.org***
[2] ***www.activistsecurity.org***
[3] ***www.freebeagles.org/articles/mobile_phones.html***
[4] ***http://bit.ly/1f91sWV***
[5] ***www.mysecured.com/?p=27***

13
How to use smartphones as securely as possible

13. How to use smartphones as securely as possible

In *Chapter 10: How to use mobile phones as securely as possible*, we discussed the security challenges of using basic mobile phones – including issues with voice communication and text messaging (SMS/MMS) services. Those phones primarily (if not exclusively) use mobile networks to transfer calls and data.

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wifi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator.

So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer.

Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks.

For instance, some smartphones have built-in geo-location (**GPS**) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone). However, the additional **GPS** functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed.

It's worth reviewing all the risks associated with mobile phones discussed in *Chapter 10: How to use mobile phones as securely as possible* as all of them are also relevant to smartphone use. *Chapter 10* covers issues of eavesdropping, interception of SMS or phone calls, **SIM card** related issues, and best practices.

In this chapter we'll take a look at the additional security challenges posed by smartphones.

Purses, wallets, smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

A simple exercise can help illustrate this:

Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find:

- Pictures of loved ones (~5 pictures)
- Identification cards (driver's license, membership cards, social security cards)
- Insurance and health information (~2 cards)
- Money (~5 bills)
- Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

- Pictures of loved ones (~100 pictures)
- Email applications and their passwords
- Emails (~500 emails)
- Videos (~50 videos)
- Social networking applications and their passwords
- Banking applications (with access to the bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold.

In *Chapter 5: How to recover from information loss* we discussed the importance of backing up data. This applies in particular to smartphones. It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency.

In this chapter we'll start by introducing some smartphone basics – a description of various platforms and some basic setup procedures for securing your information and communication. The remaining parts of this chapter will cover specific precautions related to common uses of smartphones.

What you can learn from this chapter

- What steps you can take to better secure information you store on your smartphone
- Which applications can help you to maximise security of email, SMS and voice communication from smartphones.
- How can you document information more securely using smartphones.
- How to access Internet while protecting your security and privacy using smartphones.

PLATFORMS, SETUP AND INSTALLATION

Platforms and Operating Systems

At the time of writing, the most common smartphones in use are Apple's **iPhone** and Google's **Android**, followed by **Blackberry** and **Windows phone**s. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (**FOSS**) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter.

Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as **GPS** or wireless networking capacities. In this chapter we focus on devices with the Android platform, because, as mentioned above, it's easier to secure data and communications. Nonetheless, basic setup guides and some applications for devices other than Android phones are provided, too.

Blackberry phones have been presented as "secure" messaging and email devices. This is because messages and emails are securely

channeled through Blackberry servers, out of the reach of potential eavesdroppers. Unfortunately, more and more governments are demanding access to these communications, citing need for guarding against potential terrorism and organised crime. India, United Arab Emirates, Saudi Arabia, Indonesia and Lebanon are examples of governments which have scrutinized the use of Blackberry devices and demanded access to user data in their countries.

Feature Phones

Another category of mobiles are often called 'feature phones' (e.g. Nokia 7705 Twist or Samsung Rogue). Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for security applications or improvements. In this chapter, we do not specifically address feature phones, although many measures discussed here make sense for feature phones too.

Branded and locked smartphones

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channelling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone.

For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralises your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

General setup

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the *Hands-on Guides* below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

Hands-on: Get started with the *Basic Android Set-up Guide*

Installing and updating applications

The usual way to install new software on your smartphone is to use the iPhone **Appstore** or **Google Play store**, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices.

The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you should look for alternative applications with appropriate access and rights.

Android apps are also available from sources outside the official Google channels. You just need to check the ***Unknown sources*** box in your ***Application settings*** in order to use these download sites.

It is useful to consider these alternative sites if you want to minimize your online contact with Google. We recommend **F-Droid** [1] ('Free Droid'), which only provides **Free and Open-Source Software**. In this guide, F-Droid is the primary repository for the apps we recommend, and we would only refer you to Google Play if an app is not available in F-Droid.

If you don't want to (or are unable to) go online to access apps, you can transfer apps from someone else's phone by sending **.apk files** (short for 'android application package') via bluetooth. Alternatively, you could download the .apk file to your device's Micro SD card or use a usb cable to move it there from a PC. When you have received the file, simply long tap on the filename and you will be prompted to install it. (Note: be especially careful while using bluetooth – read further in the *Chapter 12* section on *Functions beyond speech and messages*.)

COMMUNICATING VIA SMARTPHONE (VOICE & MESSAGE)

Talking securely

Basic telephony

In the section on *Basic functions, trackability and anonymity* in *Chapter 10: How to use mobile phones as securely as possible* we discussed different measures you should consider to lower the risk of interception when using the mobile phone operator network for your voice communication.

Using Internet through your smartphone over mobile data connections or WiFi can provide more secure ways to communicate with people, namely by using **VoIP** and employing means to secure this channel of communication. Some smartphone tools can even extend some of this security beyond VoIP, to mobile phone calls as well (See **Redphone** below).

Here we list a few tools and their pros and cons:

Skype

The most popular commercial **VoIP** application, **Skype**, is available for all smartphone platforms and works well if your wireless connectivity is reliable. It is less reliable on mobile data connections.

In the section *Securing other internet communication tools* in *Chapter 7: How to keep your Internet communication private*, we discussed the risks of using Skype, and why, if possible, it should be avoided. In summary, Skype is a non Open-Source software what makes it very difficult to independently confirm its level of security. Additionally, Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies retrospective access to all your communications history.

Other VoIP

Using **VoIP** is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. In fact, a secured VoIP call can be the most secure way to communicate.

CSipSimple [2] is a powerful VoIP client for Android phones that is well maintained and comes with many easy set-up wizards for different **VoIP** services.

Open Secure Telephony Network (OSTN) [3] and the server provided by the **Guardian project** [4], **ostel.me** [5], currently offers one of the most secure means to communicate via voice. Knowing and trusting the entity that operates the server for your VoIP communication needs is an important consideration.

When using **OSTN**, you never communicate directly with your communication partner, instead all your data is routed through the Ostel server. This makes it much harder to trace your data and find out who you are talking to. Additionally, Ostel doesn't retain any of the data, except the account data that you need to log in. All your speech is securely **encrypted** and even your meta data, which is usually very hard to disguise, is blurred since traffic is proxied through the ostel.me server. If you download **CSipSimple** from **ostel.co** it also comes preconfigured for use with ostel.me, which makes it easy to install and use.

RedPhone [6] is a Free and Open-Source Software application that **encrypts** voice communication data sent between two devices that run this application. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contact scheme. But people you want to talk to also need to install and use RedPhone. For ease of use RedPhone uses your mobile number as your identificator (like a user name on other VoIP services). However it also becomes easier to analyze the traffic it produces and trace it back to you, through your mobile number. RedPhone uses a central server, which is a point of centralization and thus puts RedPhone in a powerful position (of having control over some of this data).

Hands-on Guides for CSipSimple, Ostel.co and Redphone are forthcoming. In the meantime, more information can be found by following the above links.

Sending Messages Securely

You should use precautions when sending SMS and using instant messaging or chatting on your smartphone.

SMS

As described in *Chapter 10: How to use mobile phones as securely as possible* (in the section on *Text based communications*), SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations.

There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

Securing SMS

TextSecure is a **FOSS** tool for sending and receiving secure SMS on Android phones. It works both for encrypted and non-encrypted

messages, so you can use it as your default SMS application. To exchange encrypted messages this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. TextSecure automatically detects when an encrypted message is received from another TextSecure user. It also allows you to send encrypted messages to more than one person. Messages are automatically signed making it nearly impossible to tamper with the contents of a message. In our *TextSecure hands-on guide* we explain in detail the features of this tool and how to use it.

Hands-on: Get started with the *TextSecure Guide*

Secure Chat

Instant messaging and chatting on your phone can produce a lot of information that is at risk of interception. These conversations might be used against you by adversaries at a later date. You should therefore be extremely wary about what you reveal when you are writing on your phone while instant messaging and chatting.

There are ways to chat and instant message securely. The best way is to use end-to-end **encryption**, as this will enable you to make sure the person on the other end is who you want.

We recommend **Gibberbot** as a secure text chat application for the Android phones. Gibberbot offers easy and strong encryption for your chats with **Off-the-Record** Messaging protocol. This **encryption** provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure.

Gibberbot has been designed to work together with **Orbot** (see below), so your chat messages can be routed through the **Tor** anonymizing network. This makes it very hard to trace it or even find out that it happened.

Hands-on: Get started with the *Gibberbot Guide**

For iPhones, the **ChatSecure** [7] client provides the same features, although it is not easy to use it with the **Tor** network.

**Gibberbot is now known as Chatsecure. A Hands-on Guide is forthcoming. In the meantime, more information can be found on its homepage.*

Whichever application you will use always consider which account you use to chat from. For example when you use Google Talk, your credentials and time of your chatting session are known to Google. Also agree with your conversation partners on not saving chat histories, especially if they aren't encrypted.

STORING INFORMATION ON YOUR SMARTPHONE

Smartphones come with large data storage capacities. Unfortunately, the data stored on your device can be easily accessible by third parties, either remotely or with physical access to the phone. Some basic precautions to reduce inappropriate access to this information are explained in the *Basic Set-Up Guide for Android*. Additionally, you can take steps to encrypt any sensitive information on your phone by using specific tools.

Data encryption tools

The **Android Privacy Guard (APG)** allows OpenGPG encryption for files and emails. It can be used to keep your files and documents safe on your phone when emailing.

Hands-on: Get started with the *APG Guide*

Cryptonite is another **FOSS** files encryption tool. Cryptonite has more advanced features on specially prepared rooted Android phones with a custom firmware. See the *Advanced Smartphone Use* section for more.

Hands-on: Get started with the *Cryptonite Guide*

Secure password keeping

You can keep all your needed passwords in one secure, **encrypted** file by using **Keepass**. You will only need to remember one master password to access all the others. With Keepass you can use very strong passwords for each account you have, as Keepass will remember them for you, and it also comes with a password generator to create new passwords. You can synchronise Keepass password databases between your phone and your computer. We recommend that you synchronise only those passwords that you will actually use on your mobile phone. You can create a separate smaller password database on the computer and syncronise this one instead of coping an entire database with all the passwords that you use to your smartphone. Also, since all the passwords are protected by your master password, it is vital to use very

strong password for your Keepass database. See *Chapter 3: How to create and maintain secure passwords*.

Hands-on: Get started with the *Keepassdroid Guide*

SENDING EMAILS FROM SMARTPHONES

In this section we will briefly discuss the use of email on smartphones. We encourage you to refer to sections *Securing your email* and *Tips on responding to suspected email surveillance* in *Chapter 7: How to keep your Internet communication private* where we discuss basic email security.

In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

- Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
- If you use email **encryption** with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands.

Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Consider creating a mobile-only encryption key-pair (using **APG**) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

Hands-on: Get started with the *K9 and APG Guide*

CAPTURING MEDIA WITH SMARTPHONES

Capturing pictures, video or audio with your smartphone can be a powerful means to document and share important events. However, it is important to be careful and respectful of privacy and safety of those pictured, filmed or recorded. For example, if you take photos or record video or audio of an important event, it might be dangerous to you or to those who appear in the recordings, if your phone fell into the wrong hands. In this case, these suggestions may be helpful:

- Have a mechanism to securely upload recorded media files to a protected online location and remove them from the phone instantly (or as soon as you can) after recording.
- Use tools to blur the faces of those appearing in the images or videos or distort the voices of audio or videos recordings and store only blurred and distorted copies of media files on your mobile device.
- Protect or remove meta information about time and place within the media files.

Guardian Project has created a **FOSS** app called **ObscuraCam** to detect faces on photos and blur them. You can choose the blurring mode and what to blur, of course. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides easy functionality to upload it.

Hands-on: Get started with the *Obscuracam Guide*

At the time of writing, the human rights organisation ***Witness*** [8] is working with the Guardian project on a solution to all three of the above points.

ACCESSING THE INTERNET SECURELY

As discussed in *Chapter 7: How to keep your Internet communication private* and *Chapter 8: How to remain anonymous and bypass censorship on the Internet*, access to content on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. Using your smartphone to communicate with the Internet magnifies this risk.

Access through WiFi or mobile data

Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as **GPRS**, **EDGE**, or **UMTS** provided by your mobile network operator.

Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent developers and security engineers cannot

examine these protocols to see how they are being implemented by mobile data carriers.

In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers.

Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

Anonymise

To access content online anonymously, you can use an Android app called **Orbot**. Orbot channels your internet communication through **Tor**'s anonymity network.

Human Rights Defender Testimonies

I use Tor every day. I also use Orbot on my phone so I always enjoying being anonymous when using the phone or computer.
Anonymous Human Rights Defender

Hands-on: Get started with the *Orbot Guide*

Another app, **Orweb,** is a web browser that has privacy enhancing features like using proxies and not keeping a local browsing history. Orbot and Orweb together circumvent web filters and firewalls, and offer anonymous browsing.

Hands-on: Get started with the *Orweb Guide*

Proxies

The mobile version of **Firefox** – **Firefox mobile** [9] can be equipped with proxy add-ons, which direct your traffic to a proxy server. From there your traffic goes to the site you are requesting. This is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted.

We recommend the **Proxy Mobile** [10] add-on (also from **Guardian Project**, which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the **Tor** network.

ADVANCED SMARTPHONE SECURITY

Get full access to your smartphone

Most smartphones are capable of more than their installed operating system, manufacturers' software (firmware), or the mobile operators' programmes allow. Conversely, some functionalities are 'locked in' so the user is not capable of controlling or altering these functions, and they remain out of reach. In most cases those functionalities are unnecessary for smartphone users. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks.

For this, and other reasons, some smartphone users choose to manipulate the various software and programs running the smartphone in order to gain appropriate privileges to allow them to install enhanced functionalities, or remove or reduce other ones.

The process of overcoming the limits imposed by mobile carriers, or manufacturers of operating systems on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Typically, successful rooting or jailbreaking will result in your having all the privileges needed to install and use additional applications, make modifications to otherwise locked-down configurations, and total control over data storage and memory of the smartphone.

WARNING: Rooting or **jailbreaking** may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

- There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
- The manufacturer or mobile carrier warranty may be voided.
- In some places, this process maybe illegal.

But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

Alternative firmware

Firmware refers to programmes that are closely related to the particular device. They are in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc.

If you have an Android device, you might consider installing a firmware alternative to further enhance your control of the phone. Note that in order to install alternative firmware, you need to root your phone.

An example of an alternative firmware for an Android phone is **Cyanogenmod** [11] which, for example, allows you to uninstall applications from the system level of your phone (i.e. those installed by the phone's manufacturer or your mobile network operator). By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge.

In addition, Cyanogenmod ships by default with an OpenVPN application, which can be tedious to install otherwise. VPN (Virtual Private Network) is one of the ways to securely proxy your internet communication (see below).

Cyanogenmod also offers an incognito browsing mode in which history of your communication is not recorded on your smartphone.

Cyanogenmod comes with many other features. However, it is not supported by all Android devices, so before proceeding, check out the list of **supported devices** [12].

Encryption of whole volumes

If your phone is rooted you may consider encrypting its entire data storage or creating a volume on the smartphone to protect some information on the phone.

Luks Manager [13] allows easy, on-the-fly strong encryption of volumes with an user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the encrypted volumes that the Luks Manager provides to store all your data.

Virtual private networks (VPN)

A VPN provides an encrypted tunnel through the internet between your device and a VPN server. This is called a tunnel, because unlike other encrypted traffic, like **https**, it hides all services, protocols, and contents. A VPN connection is set up once, and only terminates when you decide.

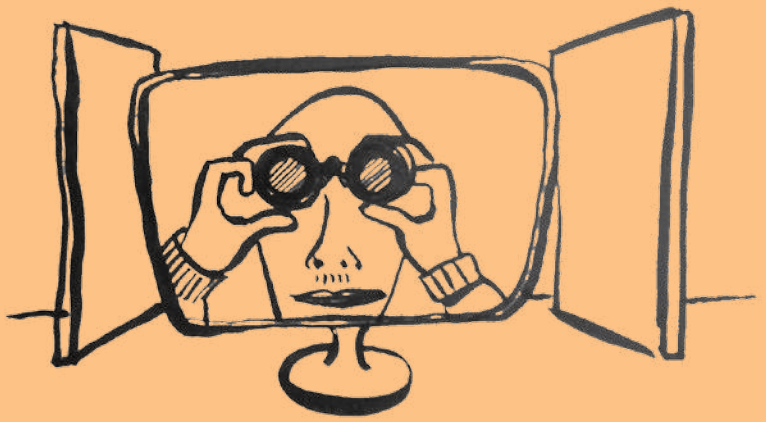
Note that since all your traffic goes through the proxy or VPN server, an intermediary only needs to have access to the proxy to analyze your activities. Therefore it is important to carefully choose amongst proxy services and VPN services. It is also advisable to use different proxies and/or VPNs since distributing your data streams reduces the impact of a compromised service.

We recommend using the **Riseup VPN** [14] server. You can use **Riseup** VPN on Android devices after installing Cyanogenmod (see above). It is also easy to setup connection to Riseup VPN on the iPhone – read more **here** [15].

LINKS

[1] *http://f-droid.org*
[2] *https://play.google.com/store/apps/details?id=com.csipsimple&hl=de*
[3] *https://dev.guardianproject.info/projects/ostn/wiki?title=OSTN*
[4] *https://ostel.co*
[5] *https://guardianproject.info*
[6] *https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone*
[7] *https://chatsecure.org*
[8] *https://www.witness.org*
[9] *http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox*
[10] *https://addons.mozilla.org/en-US/mobile/addon/proxy-mobile/*
[11] *www.cyanogenmod.org*
[12] *www.cyanogenmod.org/w/Devices*
[13] *https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager&hl=de*
[14] *https://help.riseup.net/en/vpn*
[15] *https://support.apple.com/kb/HT1424*

14
Use internet cafés as securely as possible



14. Use internet cafés as securely as possible

Internet Cafés have developed along with the spread of the Internet itself, as a means of giving people access to the Internet, and all it has to offer, without necessarily having to own a personal computer, or for situations where they don't have access to their own internet connection or computer. For many, this remains the easiest and most reliable way to access a computer and connect to the Internet in order to socialise, communicate, make friends and even work. Their wide proliferation, low cost and accessibility has made them an important part of many communities, especially in developing countries.

However, along with the benefits and conveniences of Internet cafés, there comes a number of potential risks to your personal and professional data as a result of using them. Some risks are of a technical nature, such as the higher risk of virus infection; others are more behavioural, and relate to the possibility of spying or monitoring by those who control the computers in the café.

What you can learn from this chapter

- How to reduce the risk of malware infection when using Internet Cafés
- How to securely remove as much of your information as possible from the computers you use, once you are finished using them
- How to mitigate the risk of spying and monitoring of your activities in an Internet Café.

PROTECTING YOUR DATA WHILE USING INTERNET CAFÉS

Risks associated with Internet Cafés

Despite how useful they are to us, the nature of Internet Cafés and the way that they function pose a number of potential threats to our information. There are a many factors which contribute to this risk:

- The computers are shared among dozens or even hundreds of users who may all insert their own removable media, such as Flash Drives or SD cards, which leads to a high risk of malware infection.
- Many users forget to log out of their accounts properly and dispose of cookies and browsing history, leaving them vulnerable to identity theft.
- The computers are usually owned and administered by the people who own or run the Café, who can often monitor the activities of

Avoiding malware

The first and most basic problem we want to avoid is that of exposing our data to malware infection. As noted above, malware infection arising from the use of Internet Cafés is very common, as a result of the number of people who use them and spread viruses to them through removable media, among other things. In order to avoid this, it's a good idea to keep a few basic points in mind when choosing an Internet Café:

- It's safer if the Internet Café uses Linux operating systems, or free and open source software tools such as Mozilla Firefox and LibreOffice or OpenOffice
- If the computers in the Internet Café use a Windows operating system, it should be a legal, licensed version which will receive updates which protect against virus infection.
- The computers should have updated anti-virus and anti-spyware programmes and a firewall programme.

It is a good idea to bring your own flash drive with a portable anti-virus program, such as ClamWin Portable so that you can scan the computer that you are using from an external drive. It is even better if you can obtain a flash drive with a "hardware lock" – a physical button on the flash drive itself – which means it can be 'locked' before it is plugged in to the computer: this will ensure that no malware can write itself to the flash drive from the computer. This problem can also be avoided if your portable applications are burned to a CD or DVD, which can not be written to more than once.

Protecting your personal data

If you absolutely must use internet cafés to work with sensitive, perhaps work-related files such as documents, reports, pictures, or videos, there are a number of potential problems that may arise. If the files are of a sensitive or personal nature, we may think they are safe if we only save them on our own flash drives, and don't save them on the computer in the Café itself. However, this is not necessarily the case: an infected computer in the Internet Café may copy all the content from your flash drive or CD/DVD to the computer or other location in the network. Also many programs such as Microsoft Word or LibreOffice will automatically save drafts of the files we are working on as temporary files, without us having to save them. This is generally positive, as these temporary files mean that we can recover our documents if the program or computer crashes. These files, though, are not securely deleted once we are finished, and can be recovered by someone else who accesses the same device later (see *Chapter 5: How to recover from information loss*).

This is of course also true if we do save our documents on the device we are using in the Internet Café, and even if we empty the Recycle Bin.

Therefore it is important to delete the traces of our sensitive files that we leave behind on the computers we use, if we want to be sure they can't be accessed by others. Thankfully, this is easy to achieve. Programs such as CCleaner Portable can be installed on a flash drive, and then used in order to securely delete files that we have stored on the hard drive of the computer in the Café, as well as temporary files generated while we work. At the end of each session you must simply wipe any temporary files before leaving the computer and the Café.

Hands-on: Get started with the *Portable CCleaner Guide*

A number of other problems may arise when we use Internet Cafés for browsing the Internet or communicating. One such problem is invasion of privacy which can happen when we leave behind our browsing history and cookies, and forget to log out from e-mail and social networking accounts before leaving the Café. This problem could be solved with a little vigilance: simply ensuring that we clear our browsing history and log out correctly from our accounts before we end our session. This can also be done by using CCleaner.

An even easier way to avoid this is by bringing our own browser to the café on a flash drive, such as Portable Firefox or Tor Browser Bundle which is also a portable program. With these tools, you can ensure that your browsing history is not saved on the Internet Café's computers. Furthermore, you can benefit from a number of privacy enhancing add-ons which may not be available on the browser in the Internet Café.

Hands-on: Get started with the *Portable Firefox Guide*

Hands-on: Get started with the *the Portable Tor Browser Guide*

Communicating more safely

Using portable tools, it is also possible to communicate more securely at Internet Cafés. If you want to encrypt your chat conversations, you can use Portable Pidgin with OTR or extract Portable Jitsi to

your flash drive and go on using them as you would on your personal computer.

Hands-on: Get started with the *Portable Pidgin with OTR Guide*

Hands-on: Get started with the *Jitsi Guide*

Similarly, if you want to use GPG to encrypt your emails, you can use Gpg4usb: this will allow you to write and encrypt your emails on your own computer, then bring them to the Internet Café as encrypted text files on a flash drive, and send them from there.

Hands-on: Get started with the *Gpg4usb Guide*

Spying and keyloggers

By far the most difficult risk to overcome when using Internet Cafés for anything of a sensitive nature is that of spying by the Café's administrators and, even worse, keylogging of the computers.

The first thing to consider is how much you can trust the administrators of the Café, and how well you know them. If you have access to a Café which is run by someone you know and trust, it's best to use this as your 'default' Café as much as possible.

It may be safer to assume that all the computers in any Internet Café are keylogging you. Unfortunately, if this is the case, there is very little you can do to protect any sensitive data you deal with on this computer. In this case, it is extremely important to:

- If possible, avoid logging in to any personal accounts
- Change all the passwords you have used from a different device as soon as you log out
- Bring all e-mails to the internet café encrypted in advance with GPG4USB on a USB key or DVD
- Wipe your USB keys with a progam such as CCleaner on a trusted computer with an updated antri-virus program after using

More tips can be found in the Internet Café Checklist.

CHECKLIST: SAFER INTERNET CAFÉ USAGE

This short checklist should help you prepare and use Internet Cafés as securely as possible.

1. General tips

- Consider whether it's a better idea to use a single Internet Café whose owners and administrators you trust, or better to change places regularly in order to make it harder to track you
- Avoid Internet Cafés where you have to provide identification
- Choose a location to sit where your screen can not be seen by others (including through windows), and where you can see others approaching you
- In the event of a raid or inspection, have a plan for closing programs and deleting traces as quickly as possible.

2. If you have your own computer

- Make sure you have anti-virus, anti-spyware and firewall programs installed and updated
- As the internet connection may be monitored, make sure you browse the internet using the Tor Browser or a VPN to prevent others connected to the network from spying on you
- Always ensure that the services you use online (for example, email or social networks) are configured for a secure connection (HTTPS). Along with Tor Browser, you can use Mozilla Firefox with the HTTPS Everywhere add-on as your browser.
- Do not allow your smartphone to connect to the wireless network in the Internet Café

3. If you don't have your own computer

- Try to choose an Internet Café which uses Linux operating systems.
- If possible, try using a bootable operating system from a USB key such as Tails, which is designed for anonymity and privacy and not to leave traces of your activities on the computer itself.
- If this is not possible, try to choose an Internet Café with licensed, updated versions of Windows, anti-virus, anti-spyware and firewall programs.
- Assume that everything you type, including your passwords and all content of your USB flash drive or CD/DVD you connect to the Internet Café computer may be copied and shared.
- Avoid using the software installed on the computers themselves: instead bring portable versions of your programs on your USB flash drive.
- Avoid logging in to any personal or professional accounts unless absolutely necessary. Change passwords of the accounts you logged in from secure computer as soon as you can after this.
- Use a virtual keyboard application such as On-Screen Keyboard

Portable to type your passwords

- You may want to set up a new, empty e-mail account only for use in Internet Cafés and ask your contacts not to send unencrypted mails to this address.
- Write your emails beforehand on a different computer and encrypt them using GPG4USB. Then bring them to the Internet Café on your USB flash drive and copy/paste them into your webmail
- When you're finished with your USB flash drive: ensure that your own computer's anti-virus and anti-spyware programs are up to date and that the Autorun feature on the flash drive is switched off. Then, insert your USB flash drive and wipe it using CCleaner.
- Immediately change passwords of all accounts you used in Internet Café from a different, secure device once you're finished.

Glossary

Glossary

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

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

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

.apk file - The file extension used for Android apps

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

Avast - A freeware anti-virus tool

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

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

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

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

Booting - The act of starting up a computer

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

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

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

Clam Win - A FOSS Anti-virus program for Windows

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

Comodo Firewall - A freeware firewall tool

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

Cryptonite - A FOSS app for file encryption on Android smartphones

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

KeePass - A freeware secure password database

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

VautletSuite 2 Go - A Freeware encrypted email program

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

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

Windows Phone - A smartphone operating system developed by Microsoft

Wiping - The process of deleting information securely and permanently

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

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