

How-to Booklet

This How-to Booklet is designed to explain the issues that you must understand in order to safeguard your own digital security. It seeks to identify and describe the risks you face and help you make informed decisions about how best to reduce those risks. To this end, it answers eight broad questions related to basic security, data protection and communication privacy.

At the beginning of each chapter, you will find a background scenario populated by fictional characters who will reappear in brief conversations throughout the chapter in order to illustrate certain points and answer common questions. You will also find a short list of specific lessons that can be learned from reading the chapter. It is a good idea to scan through this list before you begin reading. As you work through a chapter, you will encounter a number of technical terms that link to definitions in a glossary at the end of the booklet. You will also find references to the specific software discussed in the toolkit's Hands-on Guides.

Any single chapter or guide in this toolkit can be read individually, formatted in your browser for easy printing, or shared electronically. However, you will get more out of Security in-a-box if you can follow the relevant links and references that are scattered throughout both the booklet and the software guides. If you have a printed copy of this Booklet, you should keep it front of you while you work through the Hands-on Guides. You should also remember to finish reading the How-to Booklet chapter covering a particular tool before you begin relying on that tool to protect your digital security.

Where possible, you should read the chapters of the How-to Booklet in order. Security is a process, and there is often little point in trying to defend yourself against an advanced threat to your communication privacy, for example, if you have not yet ensured that your computer is free of viruses and other malware. In many cases, this would be like locking your door after a burglar is already in your home. This is not to say that any one of these eight topics is more important than any other, it is simply that the later chapters make certain assumptions about what you already know and about the state of the computer on which you are about to install software.

Of course, there are many good reasons why you might want to work through these chapters out of sequence. You might need advice on how to back up your important files before you begin installing the tools described in the first Hands-on Guide. You might find yourself faced with an urgent privacy threat that justifies learning How to protect the sensitive files on your computer, which is covered in *Chapter 4*, as quickly as possible. Or perhaps you are working from an Internet café, on a computer whose security is not your responsibility and from which you do not intend to access any sensitive information. If you want to use this computer to visit a website that is blocked in your country, there is nothing to prevent you from skipping ahead to *Chapter 8: How to remain anonymous and bypass censorship on the Internet*.

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* [1] or plagued by malicious software, often called *malware* [2], 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* [3], *Spybot* [4] and *Comodo Firewall* [5] to protect your computer against the ever-present dangers of *malware* [2] infection and *hacker* [1] attacks. Although the tools recommended in this chapter are for Windows, which is the operating system most vulnerable to these threats, *GNU/Linux* [6] and Apple OS X users are also at risk and should still adopt the tactics presented below.

Background scenario

Assani is a human rights activist in a Francophone African country. His two teenage children, Salima and Muhindo, have offered to help him with some routine computer work he has been asked to do. After seeing the state of his computer, they offer to teach him the basics of how to keep it healthy and functional. Assani also likes the idea of using Free and Open Source Software, but he's not sure whether that would be more or less secure, so he asks for their advice.

What you can learn from this chapter

- More about the nature of a few of the specific threats that *malware* [2] 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* [7] tools, to avoid the dangers associated with expired licenses or pirated software, and

popular [FOSS](#) [8] 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](#) [7] anti-virus program for Windows called [Avast](#) [3], 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 the [Avast! - Anti-Virus Guide](#) [9]

There are various other well-known commercial anti-virus programs as alternatives to Avast. [Clam Win](#) [10] is a [FOSS](#) [8] alternative to [Avast](#) [3]. Although it lacks certain features that are important for a primary anti-virus program, [Clam Win](#) [10] 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](#) [3] 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](#) [11] of the [Avast Guide](#) [9] 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](#) [9].

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.

Assani: I have a virus cleaner and I run it regularly, so I figure my computer is healthy, right?

Salima: Actually, just having anti-virus software isn't enough. You also need to protect your computer from spyware and hackers, so you'll have to install and run a couple more tools.

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* [2]. 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.

Assani: It all sounds like something out of a spy movie to me. Is my computer really "infected with spyware?"

Muhindo: Believe it or not, it's really common. If those programs you downloaded from the Internet haven't infected you, there's a good chance at least one of the webpages you've visited has. The fact that you use Windows and Internet Explorer makes it even more likely. If you've never scanned your computer for spyware, I bet you'll be surprised by how much is already installed on it

Anti-spyware software

You can use anti-spyware tools to protect your computer from this type of threat. *Spybot* [4] 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* [2] definitions and run regular scans.

Hands-on: Get started with the *Spybot - Anti-Spyware Guide* [12]

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* [2] 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* [13], you can install the *NoScript* [14] add-on, as described in **Section 4** [15] of the *Firefox Guide* [16].
- Never accept and run this sort of content if it comes from websites that you don't know or trust.

Assani: I've heard that 'Java applets' and 'ActiveX controls' can be dangerous. But I have no idea what they are.

Salima: They're just different examples of the same sort of thing: 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 worry too much about how they actually work, as long as you have NoScript installed and running properly.

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* [2] 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* [7] program called *Comodo Personal Firewall* [5], which does a better job of keeping your computer secure.

Hands-on: Get started with the *Comodo Firewall Guide* [17]

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*** ^[18] section for more about this
- 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*** ^[19] 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

Asani: So, now you want me to install anti-virus, anti-spyware and firewall software? Can my computer cope with all that?

Muhindo: Absolutely. In fact, these three tools are the bare minimum if you want to stay secure on the Internet these days. They're made to work together, so installing them all shouldn't cause any problems. Remember, though, you don't want want to run two anti-virus programs or two firewalls at the same time.

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*** ^[18] 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 (free and open source software) tools

Proprietary software ^[20] 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*** ^[7] or ***FOSS*** ^[8] (free and open source software) alternatives to any ***propriety software*** ^[20] that you currently use, especially those programs that are unlicensed. ***Freeware*** ^[7] and ***FOSS*** ^[8] tools are often written by volunteers and non-profit organisations who release them, and even update them, free of charge. ***FOSS*** ^[8] tools, in particular, are generally considered to be more secure than ***proprietary*** ^[20] ones, because they are developed in a transparent way that allows their ***source code*** ^[21] to be examined by a diverse group of experts, any one of whom can identify problems and contribute solutions.

Many ***FOSS*** ^[8] 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*** ^[22], respectively.

In fact, you could even move away from the Microsoft Windows operating system entirely, and try using a more secure ***FOSS*** ^[8] alternative called ***GNU/Linux*** ^[6]. 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*** ^[23] version of ***Ubuntu Linux*** ^[24], 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*** ^[6], 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*** ^[23]. 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*** ^[25] book.
- Keep up to-date with news about viruses on the ***Virus Bulletin*** ^[26] website.

- Learn how to determine which 'Windows services' are unnecessary and [disable those you do not need](#) [27].
- Other toolkits from the [Tactical Technology Collective](#) [28] can help you switch to using FOSS and Freeware tools for all of your software needs.
- [Download free bootable rescue CDs](#) [29] to scan your computer and remove the viruses, without starting Windows on your computer.
- If you think your computer is infected with a virus or some other malicious software read [Malware Removal Guide for Windows](#) [30].

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](#) [31] can help avoid this type of disaster.

Background scenario

Shingai and Rudo are an elderly married couple with many years of experience helping the HIV-infected population of Zimbabwe maintain access to proper medication. They are applying for a grant to purchase new computers and network equipment for their office. Since they live in a region that is quite turbulent, in terms both of politics and of infrastructure, they and their potential funders want to ensure that their new hardware will be safe, not only from hackers and viruses, but also from confiscation, thunderstorms, electrical spikes and other such disasters. They ask Otto, a local computer technician, to help them devise a plan of action to strengthen the physical security of the computers and network hardware they plan to buy if their grant application is successful.

What you can learn from this chapter

- More about a few of the [physical threats](#) [32] 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](#) [33]. 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.

Shingai: We want to put a brief summary of our security policy into this grant application, but we also need to make sure the policy itself is thorough. What should we include in it?

Otto: I'm afraid I can't recommend a 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. Here's a piece of general advice, though: 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](#) [34] 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 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](#) [2], 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* [33]. 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 more 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* [35], *routers* [19], *switches* [19], *hubs* [19] and modems into secure rooms or cabinets. An intruder with physical access to such equipment can install *malware* [2] 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* [19] 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* [19] hardware and software, but they are rarely difficult to follow.

At your work

- 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* [36], 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*** [37], enter your password, confirm it, click Create Password and click Yes, Make Private.
- There are a few settings in your computer's *BIOS* [38] that are relevant to physical security. First, you should configure your computer so that it will not *boot* [39] from the USB device, CD-ROM or DVD drives. Second, you should set a password on the *BIOS* [38] 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*** [37], to store your Windows or *BIOS* [38] 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*** ^[40] sensitive information on computers and storage devices in your office. See ***Chapter 4: How to protect the sensitive files on your computer*** ^[41] for additional details and pointers to the appropriate Hands-on Guides.#

Rudo: I'm a bit nervous about messing around in BIOS. Can I break my computer if I do something wrong?

tto: You sure can, at least for a little while. In fact, 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*** ^[36] 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 (UPS)* ^[42] on important computers in your office. A ***UPS*** ^[42] stabilises electricity supply and provides temporary power in the event of a blackout.
 - Even where ***UPS*** ^[42] 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 equipment 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 putting your computers at risk.
- To defend against accidents in general, avoid placing important hardware in passages, reception areas or other easily accessible locations. ***UPS***, 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*** ^[31] 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](#) [31] 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](#) [43].

Your [security policy](#) [31] 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](#) [31] document along with the rest of your important data. See the [Further reading](#) [44] section for more information about creating a [security policy](#) [31].

Further reading

- For additional information on assessing risks, see the [1.2 Security Awareness](#), and [1.3 Threat Assessment](#) sections of the [Digital Security and Privacy for Human Rights Defenders](#) [25] book.
- For a more detailed explanation of how to set a BIOS password, see the [2.1 Windows Security](#) chapter in the [Digital Security and Privacy for Human Rights Defenders](#) [25] book.
- For guidelines on creating a security policy, see [4. Case Study 1](#) in the [Digital Security and Privacy for Human Rights Defenders](#) [25] book.
- See also the [Protection Manual](#) [45] and [Protection Handbook](#) [46] for Human Rights Defenders.

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](#) [40] 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](#) [47] tool, such as [KeePass](#) [48].

Background scenario

Mansour and Magda are siblings, in an Arabic-speaking country, who maintain a blog on which they anonymously publicise human rights abuses and campaign for political change. Magda recently tried to log into her personal webmail account and found that her password had been changed. After resetting the password, she was able to log in, but when she opened her inbox she noticed that several new messages were marked as having been read. She suspects that a politically-motivated intruder may have learned or guessed her password, which she uses for several of her website accounts. She is meeting with Mansour, who has less computer experience, to explain the situation and to voice her concerns.

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](#) [48] [secure password database](#) [47] 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](#) [40] 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](#) [40] 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](#) ^[49] 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](#) ^[47] such as [KeePass](#) ^[48]. 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](#) ^[47].

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.

Mansour: What if I trust someone? It's OK for me to tell you my password, right?

Magda: Well, first of all, just because you trust somebody with your password doesn't necessarily mean you trust them to take good care of it, right? Even though I wouldn't do anything bad with your password, I might write it down and lose it or something. That could even be how I got into this mess! And besides, it's not all about trust. If you're the only one who knows your password, then you don't have to waste your time worrying about who to blame if the account gets broken into. Right now, for example, I feel pretty confident that somebody actually guessed or 'cracked' my password, because I never wrote it down or shared it with anyone.

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](#) ^[48] 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* [50], 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 a 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](#) [51]'s calculations. Passfault is one of a number of websites which allow 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* [47], such as [KeePass](#) [48].

Hands-on: Get started with the [KeePass - Secure Password Storage Guide](#) [52]

Of course, if you use this method, it becomes especially important that you create and remember a very secure password for [KeePass](#) [48], 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](#) [48] 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](#) [48] database. Look over [Chapter 5: How to recover from information loss](#) [43] 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](#) [48] 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 it's weakness. If somebody force you to give away your KeePass database master password, he will gain access to all of the passwords stored in this KeePass database. If this is the 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](#) [41]. You can also create a separate KeePass database to containing passwords protecting more sensitive information, and take extra precautions with that database.

Mansour: Wait a minute. If KeePass uses a single master password to protect all of your other passwords, how is it more secure than just using that same password for all of your accounts? I mean, if a bad guy learns the master password, he gets access to everything, right?

Magda: It's a good thought, and you're right that protecting your master password is really important, but there are a couple of key differences. First of all, this 'bad guy' would not only need your password, he'd need your KeePass database file, too. If you just share the same password between all of your accounts, then he'd only need the password itself. Plus, we know that KeePass is extremely secure, right? Well, other programs and websites can go either way. Some of them are much less secure than others, and you don't want someone breaking into a weak website, and then using what he learns to access a more secure account. And there's another thing, too. KeePass makes it really easy to change your master password if you think it's necessary. I should be so lucky! I spent all day today updating my passwords.

Further reading

- To learn more about secure passwords, see the *2.2 Password Protection* chapter and the Appendix D. How long should my password be? in the *Digital Security and Privacy for Human rights Defenders* [25] book.
- Wikipedia has informative articles on *Passwords* [53], *Guidelines for password strength* [54], and *password cracking* [55].

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* [56] and *Chapter 2: How to protect your information from physical threats* [57]. 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*** [40] **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* [8] application called *TrueCrypt* [58], which can both *encrypt* [40] and hide your file.

Background scenario

Claudia and Pablo work with a human rights NGO in a South American country. They have spent several months collecting testimonies from witnesses to the human rights violations that have been committed by the military in their region. If the details of who provided these testimonies were to become known, it would endanger both the courageous people who testified and members of the organisation in that region. This information is currently stored in a spreadsheet on the NGO's Windows XP computer, which is connected to the Internet. Being security conscious, Claudia has made sure to store a backup of the data on a CD, which she keeps outside the office.

What you can learn from this chapter

- How to *encrypt* [40] information on your computer
- What risks you might face by keeping your data *encrypted* [40]
- 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

Pablo: But my computer is already protected by the Windows login password! Isn't that good enough?

Claudia: Actually, Windows login passwords are usually quite easy to break. Plus, anybody who gets his hands on your computer for long enough to restart it with a LiveCD in the drive can copy your data without even having to worry about the password. If they manage to take it away for a while, then you're in even worse trouble. It's not just Windows passwords you need to worry about, either. You shouldn't trust Microsoft Word or Adobe Acrobat passwords either.

Encrypting [40] 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* [40] key or password, in this case) can access it. The analogy is particularly appropriate for *TrueCrypt* [58] 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* [40] 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 Guide* [59]

While other software can provide similar strength *encryption* [40], *TrueCrypt* [58] 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* [40] volumes on portable storage devices. It provides 'deniability' features described in the ***Hiding your sensitive information*** [60] section below. In addition TrueCrypt is a *free and open source* [8] program.

Pablo: Alright, now you have me worried. What about other users on the same computer? Does this mean they can read files in the 'My Documents' folder?

Claudia: I like the way you're thinking! If your Windows password doesn't protect you from intruders, how can it protect you from other people with accounts on the same computer? In fact, your My Documents folder is normally visible to anybody, so other users wouldn't even have to do anything clever to read your unencrypted files. You're right, though, even if the folder is made 'private,' you're still not safe unless you use some kind of encryption.

Tips on using file encryption safely

Storing confidential data can be a risk for you and for the people you work with. *Encryption* [40] 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*** [61] for more information about how to do this securely). The second step is to use a good file *encryption* [40] tool, such as *TrueCrypt* [58].

Claudia: Well, maybe we don't actually need to store information that could identify the people who gave us these testimonies. What do you think?

Pablo: Agreed. We should probably write down as little of that as possible. Plus, we should think up a simple code we can use to protect names and locations that we absolutely have to record.

Returning to the analogy of a locked safe, there are a few things you should bear in mind when using *TrueCrypt* [58] 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* [58] 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* [40] 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* [40] 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* [40] 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* [58] volume on a USB memory stick, you can also keep a copy of the *TrueCrypt* [58] 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* [2], you probably shouldn't be typing in your passwords or accessing your sensitive data.

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* [40]. Just because the legitimate reasons to *encrypt* [40] 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* [58]: 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 [40] 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* [40] software would be enough to

expose you to accusations of criminal activity or espionage (regardless of what is actually inside your *encrypted* [40] 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* [62] 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* [40] is less incriminating than file *encryption* [40] 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* [58] anyway, while attempting to disguise your *encrypted* [40] volume as best you can.

If you 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* [58] 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* [59] explains how to do this.

Considering the risk of identifying your sensitive information

Often, you may be less concerned about the consequences of 'getting caught' with *encryption* [40] 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* [58] deniability feature, which is discussed in more detail below, comes into play.

TrueCrypt's [58] deniability feature is one of the ways in which it goes beyond what is typically offered by file *encryption* [40] tools. This feature can be thought of as a peculiar form of *steganography* [62] 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 [58] deniability feature works by storing a 'hidden volume' inside your regular *encrypted* [40] 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* [58] 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* [58] without enabling its deniability feature, however, and it is generally considered impossible to determine, through analysis, whether or not a given *encrypted* [40] 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*** [63] section, below, can point you to more information about this.

Claudia: Alright, so let's toss some junk into the standard volume, and then we can move all our testimonies into the hidden one. Do you have some old PDFs or something we can use?

Pablo: Well, I was thinking about that. I mean, the idea is for us to give up the decoy password if we have no other choice, right? But, for that to be convincing, we need to make sure those files look kind of important, don't you think? Otherwise, why would we bother to encrypt them? Maybe we should use some unrelated financial documents or a list of website passwords or something.

Further reading

- For additional information on securing your files, see the *2.4 Cryptology* chapter, the *2.8 Steganography* Chapter and *4.2 Case Study 3* from the [Digital Security and Privacy for Human Rights Defenders](#) ^[25] book.
- The [TrueCrypt Documentation](#) ^[64] discusses in details many aspects of information encryption and [TrueCrypt FAQ](#) ^[65] provides answers to some common questions about TrueCrypt.

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](#) ^[66] and [Recuva](#) ^[67].

Background scenario

Elena is an environmentalist in a Russian-speaking country, where she has begun to create a website that will rely on creative presentation of images, videos, maps and stories to highlight the extent of illegal deforestation in the region. She has been collecting documents, media files and geographic information about logging for years, and most of it is stored on an old Windows computer in the office of the NGO where she works. While designing a website around this information, she has come to realize its importance and to worry about preserving it in the event that her computer should be damaged, especially if it should happen before she gets everything copied up to the website. Other members of her organization sometimes use the computer, so she also wants to learn how to restore her files if someone accidentally deletes the folder containing her work. She asks her nephew Nikolai to help her develop a backup strategy.

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](#) ^[2] and protected by a good [firewall](#) ^[68] 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](#) ^[1], 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.

Elena: I know backup is important, Nikolai, but doesn't that mean I should have someone else set it up for me? I mean, am I really going to have the time, resources and expertise to do this on my own?

Nikolai: You'll be fine. Coming up with a good backup plan takes a bit of thought, but it doesn't take all that much time or money. And, compared with losing all of your information, you can hardly call it inconvenient, right? Besides, backup is definitely one of those things that you should manage yourself. Unless the people who normally help you out with tech support are extremely reliable and extremely well-informed about where you keep your digital information, you're better off setting things up on your own.

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.

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

In the table above, 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.

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* ^[66], 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](#) ^[41] and in the [TrueCrypt Guide](#) ^[59].

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* ^[69] and configure it to work with your account. The [Thunderbird Guide](#) ^[70] 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.

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

Elena: I know some people who keep all of their important documents on Gmail, by attaching them to 'draft' messages or emails to themselves. Would that count as a 'second physical location' for my files?

Nikolai: It might help you recover if you lose one or two very important documents, but it's pretty awkward. Honestly, how many documents per week would you be willing to back up like that? Plus, you need to consider whether or not those attachments are safe, especially if you're at all worried about your email being monitored. Unless you're connecting to Gmail securely, this is a bit like handing over your sensitive information on a silver platter. Using an HTTPS connection to Gmail in order to back up small Truecrypt volumes or KeePass database files would be pretty safe, because they're encrypted, but I really wouldn't recommend this as a general-purpose backup strategy.

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* ^[69] 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.

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* ^[71] 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* ^[71], 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** ^[72] 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 the [Cobian Backup Guide](#) ^[73]

As always, it is a good idea to encrypt your backup files using a tool such as [TrueCrypt](#) ^[58]. More information about about data encryption can be found in **Chapter 4: How to protect the sensitive files on your computer** ^[41].

Hands-on: Get started with the [TrueCrypt - Secure File Storage Guide](#) ^[59]

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!

Elena: Alright, so I made an encrypted backup while I was at work, and I put it on a CD. Cobian is scheduled to update my backup in a few days. My desk at work has a drawer that locks, and I'm planning to keep these backup CDs in there so they won't get lost or broken.

Nikolai: But what if your office burns down? Computer, desk, backup CDs and all? Or, what if your website forum gets used to plan some giant environmental demonstration, the authorities crack down, things get out of hand, and the organisation is raided? I doubt your little desk lock will keep the police from confiscating those CDs. What about keeping them at home, or asking a friend to store them for you?

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** ^[61] 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](#) ^[74].

Hands-on: Get started with the [Recuva - File Recovery Guide](#) ^[74]

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](#) ^[74]. 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 *2.3 Information Backup, Destruction and Recovery* chapter of the [Digital Security and Privacy for Human Rights Defenders](#) ^[25] book.
- 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](#) ^[75], [SpiderOak](#) ^[76],

[Google Drive](#) [77], [tahoe-lafs](#) [78].

- There is an excellent article on data recovery in [Wikipedia](#) [79].

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* [80] is one such tool, and is discussed below. Using *Eraser* [80] 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* [81] old hard drives before giving them away, deleting old user accounts, and clearing your web browsing history, for example. *CCleaner* [82], 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.

Background scenario

Elena is an environmentalist in a Russian-speaking country, where she maintains an increasingly-popular website that highlights the extent of illegal deforestation in the region. She has created a backup of the information used to create the website, and she keeps copies of it at home, in the office and on her new laptop. Recently, she has also begun to store a copy of the webserver's visitor logs and the database containing her users' forum posts. Elena will soon be travelling internationally, to attend a large global conference of environmental activists, some of whom have reported having their laptops taken away for over an hour at border-crossings. To protect her sensitive information, and the safety of her more political forum participants, she has moved her home and office backups onto a TrueCrypt volume and removed the copy from her laptop. She asked her nephew Nikolai for advice, and he has warned her that she needs to do more than just delete her old backup if she is worried about having her computer seized by border officials.

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** [43].

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* [81], 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* [81] 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* [81] sensitive data from your hard drive or storage device. You can *wipe* [81] a single file or you can *wipe* [81] 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* [81] 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* [81] 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 [80] is a free and open-source secure deletion tool that is extremely easy to use. You can *wipe* [81] files with *Eraser* [80] in three different ways: by selecting a single file, by selecting the contents of the **Recycle Bin**, or by *wiping* [81] all unallocated space on the drive. *Eraser* [80] can also *wipe* [81] the contents of the Windows *swap file* [83], which is discussed further below.

Hands-on: Get started with the *Eraser - Secure File Removal Guide* [84]

While secure deletion tools will not damage any visible files unless you explicitly *wipe* [81] 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* [81] 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* [81] large amounts of data from your computer.

Elena: I know word processing programs like Microsoft Word and Open Office sometimes make temporary copies of a file while you're working on it. Do other programs do that too, or should I mostly just worry about files that I create and delete myself?

Nikolai: Actually, there are lots of places on your computer where programs leave traces of your personal information and online activities. I'm talking about websites you've visited, draft emails you've worked on recently and other things like that. All of this stuff could be sensitive, depending on how often you use that computer.

Wiping temporary data

The feature that allows *Eraser* [80] to *wipe* [81] all unallocated space on a drive is not as risky as it might sound, because it only *wipes* [81] previously-deleted content. Normal, visible files will be unaffected. On the other hand, this very fact serves to highlight a separate issue: *Eraser* [80] 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* [85], 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* [83]. 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* [83]. 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* [83] 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* [82], which was designed to clean up after software like Internet Explorer, Mozilla *Firefox* [13] and Microsoft Office applications (all of which are known to expose potentially sensitive information), as well as cleaning Windows itself. *CCleaner* [82] has the

ability to delete files securely, which saves you from having to *wipe* [81] unallocated drive space, using *Eraser* [80], after each time you run it.

Hands-on: Get started with the *CCleaner - Secure File Deletion and Work Session Wiping Guide* [86]

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 diligent about erasing sensitive files. You also know what tools you can use to *wipe* [81] 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* [43].
- Close down all unnecessary programs and disconnect from the Internet.
- Delete all unnecessary files, from all storage devices, and empty the **Recycle Bin**
- *Wipe* [81] temporary files using *CCleaner* [82].
- *Wipe* [81] the Windows *swap file* [83] using *Eraser* [80].
- *Wipe* [81] all of the free space on your computer and other storage devices using *Eraser* [80]. 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* [82] to *wipe* [81] temporary files
- *Wiping* [81] sensitive electronic documents using *Eraser* [80], instead of using the **Recycle Bin** or the Windows delete function
- Periodically using *Eraser* [80] to *wipe* [81] the Windows *swap file* [83]
- Periodically using *Eraser* [80] to *wipe* [81] 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 the entire contents of a storage device

You might occasionally need to *wipe* [81] 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* [81] the drive thoroughly with *Eraser* [80] before handing it over. And, even if you do keep the drive, you will probably want to *wipe* [81] it anyway, regardless of whether you intend to reuse or discard it. Similarly, if you purchase a new hard drive, you should *wipe* [81] 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* [80] to *wipe* [81] 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* [80] installed on it. At that point, you can delete the full contents of the external drive and then use *Eraser* [80] to *wipe* [81] 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* [81] 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.

Elena: I still have an old CD backup of the webserver logs, and I heard that you can erase a CD by putting it in the microwave. Somehow, though, it sounds like a really bad idea to me. Do people really do that? Does it work?

Nikolai: I imagine it destroys the data pretty effectively, but I wouldn't know, because I'd never put a CD in my microwave! You're right. That sounds like a terrible idea. Even if the metal doesn't damage your microwave or start a fire, I bet that plastic would give off some pretty unhealthy fumes. Come to think of it, I wouldn't recommend burning CDs in a fire, either.

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. This feature is described in the [Firefox Guide](#) [16].
- The [CCleaner FAQ](#) [87] 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](#) [88] is worth reading, as the [method](#) [89] he describes has had a major influence on the developers of *Eraser* and other secure file removal tools.

7. 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](#) [90], [Skype](#) [34] and other *Voice-over-IP VoIP* [91] 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* [91] 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* [40] 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](#) [92] email service, the Off the Record *OTR* [93] plugin for the [Pidgin](#) [94] instant messaging program, Mozilla [Firefox](#) [13] and the [Enigmail](#) [95] add-on for the Mozilla [Thunderbird](#) [69] 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* [96] 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.

Claudia and Pablo work with a human rights NGO in a South American country. After spending several months collecting testimonies from witnesses to the human rights violations that have been committed by the military in their region, Claudia and Pablo have begun taking steps to protect the resulting data. They have kept only the information they need, which they store in a TrueCrypt partition that is backed up in several physical locations. While preparing to publish certain aspects of these testimonies in a report, they have found that they must discuss sensitive information with a few of their colleagues in another country. Although they have agreed not to mention names or locations, they still want to ensure that their email and instant messaging conversations on this topic remain private. After calling a meeting to discuss the importance of communication security, Claudia has asked if anyone in the office has questions.

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](#) [97] and [Switching to a more secure email account](#) [98] sections, below. Going beyond the basics, it is sometimes critical that your email contacts have the ability to verify 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](#) [99], in the [Encrypting and authenticating individual email messages](#) [100] 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](#) [101] 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](#) [56] offers some advice on how to prevent this sort of thing, and [Chapter 3: How to create and maintain secure passwords](#) [37] 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](#) ^[102] is the first recipient of an email message as it begins its journey to the recipient. Similarly, the recipient's [ISP](#) ^[102] 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.

Pablo: I was talking to one of our partners about all this, and she said that she and her colleagues sometimes just save important messages in the 'Drafts' folder of a webmail account where they all share a password. It sounds kind of strange to me, but would it work? I mean, wouldn't that prevent anyone from reading the messages, since they're never actually sent?

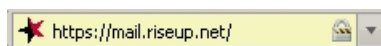
Claudia: Any time you read an email on your computer, even if it's just a 'draft,' its contents have been sent to you over the Internet. Otherwise, it couldn't appear on your screen, right? The thing is, if someone has you under surveillance, they don't just monitor your email messages, they can scan 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 that '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](#) ^[103] [encryption](#) ^[40]. You can tell whether or not you are using [SSL](#) ^[103] 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](#) ^[104] 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](#) ^[105] 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](#) ^[13] and its security-related add-ons.

Hands-on: Get started with the [Firefox with add-ons - Secure Web Browser Guide](#) ^[16]

Pablo: One of the guys who's going to be working on this report with us tends to use his Yahoo webmail account when he's not in the office. And I seem to remember somebody else using Hotmail. If I send a message to these guys, can other people read it?

Claudia: Probably. Yahoo, Hotmail and plenty of other webmail providers have insecure websites that don't protect the privacy of their users' messages. We're going to have to change some people's habits if we want to be able to discuss these testimonies securely.

Switching to a more secure email account

Few webmail providers offer [SSL](#) ^[103] 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](#) ^[106] 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](#) ^[106] to email recipients. However, it is not recommended 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](#) ^[107] section for more information about Google's privacy policy.

If possible, you should create a new [RiseUp](#) ^[92] email account by visiting <https://mail.riseup.net> ^[108]. [RiseUp](#) ^[92] 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](#) ^[92] account, however, you will need two 'invite codes.' These codes can be given out by anyone who already has a [RiseUp](#) ^[92] 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](#)]/[glossary#RiseUp](#)) users and ask them each to send you a code.

Hands-on: Get started with the [RiseUp - Secure Email Service Guide](#) ^[109]

Both Gmail and [RiseUp](#) ^[92] are more than just webmail providers. They can also be used with an email client, such as Mozilla [Thunderbird](#) ^[69], that supports the techniques described under [Advanced email security](#) ^[99]. Ensuring that your email client makes an [encrypted](#) ^[40] connection to your provider is just as important as accessing your webmail through **HTTPS**. If you use an email client, see the [Thunderbird Guide](#) ^[70] for additional details. At the very least, however, you should be sure to enable [SSL](#) ^[103] or [encryption](#) ^[40] for both your incoming and outgoing mail servers.

Pablo: So, should I switch to using RiseUp or I can keep using Gmail, and just switch to the secure 'https' address?

Claudia: It's your call, but there are a few things you should definitely consider when choosing an email provider. First, do they offer a secure connection to your account? Gmail does, so you're OK there. Second, do you trust the administrators to keep your email private and not to read through it or share it with others? That one's up to you. And, finally, you need to think about whether or not it's acceptable for you to be identified with that provider. In other words, will it get you in trouble to use an email address that ends in 'riseup.net', which is known to be popular among activists, or do you need a more typical 'gmail.com' address?

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 messages 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](#) ^[92] 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](#) ^[110], which is described in [Chapter 8: How to remain anonymous and bypass censorship on the Internet](#) ^[111], 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](#) ^[110], or one of the other [circumvention](#) ^[112] tools described in [chapter 8](#) ^[111], just to access a secure email provider such as [RiseUp](#) ^[92] 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](#) ^[106] 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](#) ^[61] and the [CCleaner Guide](#) ^[86] 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 above precautions it is still very important to beware of you write in the 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 develop 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 surveillance

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 8: How to remain anonymous and bypass censorship on the Internet](#) ^[111], 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](#) ^[91] 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](#) ^[91] 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 programs 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 program called [Pidgin](#) ^[94] 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](#) ^[40] conversations through [Pidgin](#) ^[94], you will need to install and activate the *Off-the-Record OTR* ^[93] plug-in. Fortunately, this is a fairly simple process.

Hands-on: Get started with the [Pidgin with OTR - Secure Instant Messaging Guide](#) ^[113]

Pablo: If Yahoo webmail is insecure, does that mean that Yahoo Chat is insecure, too?

Claudia: The thing to remember is that, if we want to use instant messaging to discuss this report, we need to make sure that everyone involved has Pidgin and OTR installed. If they do, we can use Yahoo chat or any other chat service.

Securing your VoIP software

[VoIP](#) ^[91] calls to other [VoIP](#) ^[91] 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](#) ^[91] programs include [Skype](#) ^[114] (see below), [Jitsi](#) ^[115], [Google Talk](#) ^[116], [Yahoo! Voice](#) ^[117], and [MSN Messenger](#) ^[118].

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 is also best to use Free and Open-Source Software, preferably those reviewed, tested, and recommended by a trusted community. Taking above criteria we would recommend that you try [Jitsi](#) ^[115] as your choice for VoIP.

Notice about Skype's security

[Skype](#) ^[34] 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](#) ^[40] 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](#)** ^[56] addresses the virtues of *Free and Open-Source Software FOSS* ^[8] in the **[Keeping your software up-to-date](#)** ^[119] 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](#) ^[114] 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](#) ^[111] 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 the Skype setting to automatically accept incoming files be disabled, 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, if you know t. Especially he 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](#) ^[94] with the [OTR](#) ^[93] 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 an unsecured email account. In order to do this, you will need to learn about public key [encryption](#) ^[40]. This technique allows you to encode individual messages, making them unreadable to anyone but the intended recipients. The ingenious aspect of public key [encryption](#) ^[40] is that you do not have to exchange any secret information with your contacts about how you are going to encode messages in the future.

Pablo: But how does all this work?

Claudia: 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.

This technique can be used with any email service, even one that lacks a secure communication channel, because individual messages are [encrypted](#) ^[40] before they leave your computer.

Remember that by using [encryption](#) ^[40], you could attract attention to yourself. The type of [encryption](#) ^[40] used when you access a secure website, including a webmail account, is often viewed with less suspicion than the type of public key [encryption](#) ^[40] being discussed here. In some circumstances, if an email containing this sort of [encrypted](#) ^[40] data is intercepted or posted on a public forum, it could incriminate the person who sent it, regardless of the content of the message. 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](#) ^[40] may seem complicated at first, but it is quite straightforward once you understand the basics, and the tools are not difficult to use. Simple, user-friendly and portable, the [pgp4usb](#) program can encrypt email messages and files even when you are not connected to the Internet.

Hands-on: Get started with the [Portable *pgp4usb* - email text and files encryption program guide](#) ^[120]

The [Mozilla Thunderbird](#) ^[69] email program can be used with an extension called [Enigmail](#) ^[95] to encrypt and decrypt email messages quite easily.

Hands-on: Get started with the [Thunderbird with Enigmail and GPG - Secure Email Client Guide](#) ^[70]

[VaultletSuite 2 Go](#) ^[121], 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 the [VaultletSuite 2Go - Secure Email Client Guide](#) ^[122]

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.

Given that 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** ^[123], which also rely on public key **encryption** ^[40], provide a more secure means of proving one's identity when sending a message. The **portable gpg4usb** ^[120] guide or **How to use Enigmail with Thunderbird** ^[124] section of the **Thunderbird Guide** ^[70] explains in detail how this is done.

Pablo: I had a colleague once who received email from me that I didn't send. We decided, in the end, that it was just spam, but now I'm imagining how much damage could be done if a fake email appeared in the wrong person's inbox at the wrong time. I've heard you can prevent this kind of thing with digital signatures, but what are they?

Claudia: A digital signature is like a wax seal over the flap of an envelope with your letter inside, except that it can't be forged. It proves that you are the real sender of the message and that it hasn't been tampered with along the way.

Further reading

- To learn more about faking an email identity, refer to the *2.5 Spoofing* section of the **Digital Security and Privacy for Human Rights Defenders** ^[25] book.
- 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 website** ^[125]
 - Instructions on **using Gmail** ^[126] .
 - Instructions on **how to import your gmail contacts into Thunderbird** ^[127]
 - 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'.
- There is a well-known attack on the security of SSL encryption known as the **Man in the Middle attack** ^[128].
- The **Gmail Privacy Policy** ^[129], 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 further, 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.
- A series of interviews in 2008 addressed the **privacy and encryption policies** ^[130] of several major instant messaging services.

8. 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** ^[106], while others blacklist certain **domain names** ^[131] 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** ^[112], and the intermediary computers are called **proxies** ^[132]. **Proxies** ^[132], 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** ^[112] **proxies** ^[132] 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** ^[132], or if performance is more important to you than anonymity, then a basic **circumvention** ^[112] **proxy** ^[132] might serve you better.

Background scenario

Mansour and Magda are siblings, in an Arabic-speaking country, who maintain a blog on which they anonymously publicise human rights abuses and campaign for political change. The authorities in their country have not been able to shut down their website, because it is hosted in another country, but they have often tried to learn the identity of the blog's administrators from other activists. Mansour and Magda are concerned that the authorities may be able to monitor their updates and learn who they are. In addition, they want to prepare for when the government eventually filters their website, not only so that they can continue updating it, but also in order to provide good circumvention advice to readers within their own country, who would otherwise lose access to the blog.

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* [102] nor a surveillance organization in your country can determine which websites and Internet services you visit

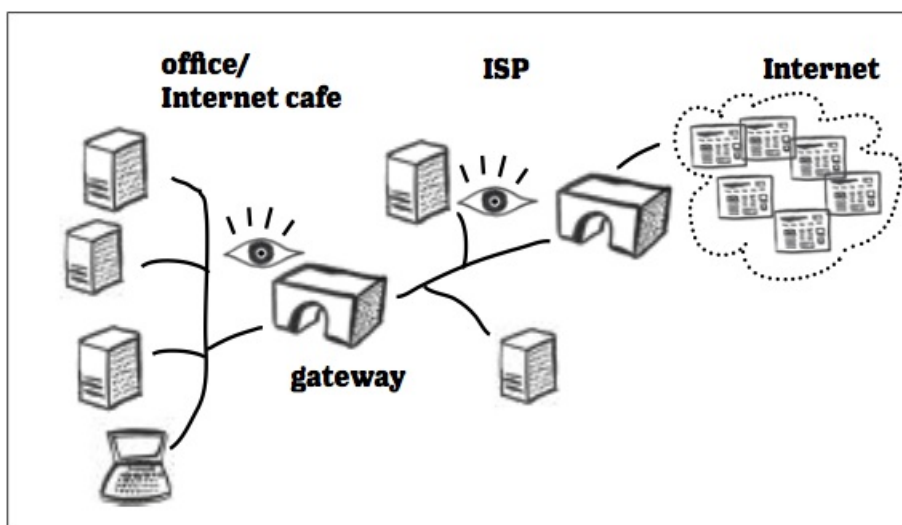
Understanding Internet censorship

Research carried out by organisations like the [OpenNet Initiative \(ONI\)](#) [133] and [Reporters Without Borders \(RSF\)](#) [134] 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* [102] at your home, office, school, library or Internet cafe. The *ISP* [102] assigns your computer an *IP address* [106], 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* [106] 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* [102] 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* [102] 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* [106] to your *ISP* [102] and asking it to connect you with the webserver's *ISP* [102]. 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* [135] 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* [102] themselves. Often, a *blacklist* [135] will contain *domain names* [136], such as [www.blogger.com](#), rather than *IP addresses* [137]. 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* [102] level
- Blocked sites are *blacklisted* [135] by both their *IP addresses* [106] and their *domain names* [131]
- You may be given an unclear or misleading reason to explain why a blocked site fails to load.

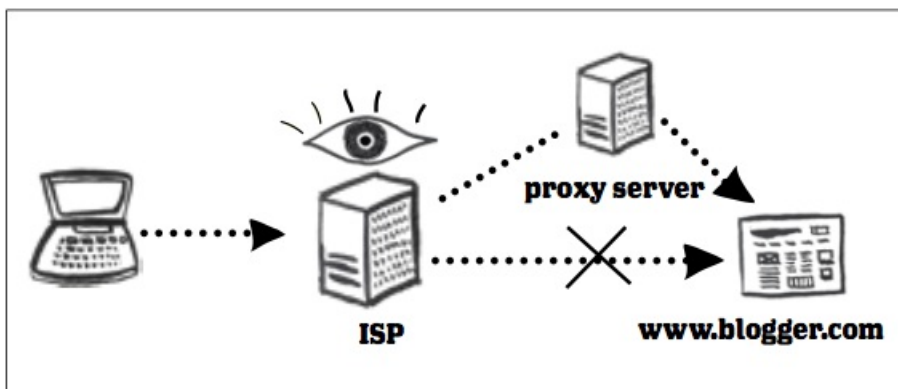
Because the most effective circumvention tools can be used regardless of which filtering methods are in place, it does not generally do any harm to make these pessimistic assumptions

Mansour: So, if I find one day that I can't access the blog, but a friend in another country can still see it just fine, does that mean the government has blocked it?

Magda: Not necessarily. There could be some problem that only affects people who are trying to reach the website from here. Or, it could be some issue with your computer that only shows up on certain types of webpages. You're on the right track, though. You could also try visiting it yourself while using a circumvention tool. After all, most of these tools 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 prodirectly 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* [132] 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* [102] perspective, you will simply appear to be communicating securely with an unknown computer (the *proxy* [132] 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* [132]. If that happens, its *IP address* [106] may itself be added to the *blacklist* [135], and it will no longer work. It usually takes some time for *proxies* [132] 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* [132], which tend to be less obvious. *Encryption* [40] is only part of the solution, however. The operators of a *proxy* [132] 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* [132] may not be particularly secure. Instead, circumvention tools of this type often simply try to distribute new *proxies* [132] faster than they can be blocked.

In the end, as long as you can reach a *proxy* [132] 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* [132] page. The *Tor* [110] anonymity network, described below, uses the first method. Following that is a discussion of basic, single *proxy* [132] 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](#) [132] 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](#) [110], 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](#) [132] and the websites you visit. As always, you must ensure that you have an encrypted connection, [HTTPS](#) [103], 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](#) [110], but the result is a tool that provides anonymity as well as circumvention. Each time you connect to the [Tor](#) [110] network, you select a random path through three secure [Tor](#) [110] [proxies](#) [132]. This ensures that neither your [ISP](#) [102] nor the [proxies](#) [132] themselves know both your computer's [IP address](#) [106] 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 the [Tor - Digital Anonymity and Circumvention Guide](#) [138]

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](#) [69], and instant messaging programs, including [Pidgin](#) [94], 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](#) [132]. 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](#) [132] are probably the easiest to use. They require only that you point your browser at a [proxy](#) [132] webpage, enter the filtered address you wish to view and click one button. The [proxy](#) [132] will then display the requested content inside its own webpage. You can follow links normally or enter a new address into the [proxy](#) [139] 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](#) [132] 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](#) [139] tend to have certain disadvantages, as well. They do not always display pages correctly, and many web-based [proxies](#) [132] will fail to load complex websites, including those that feature streaming audio and video content. Also, while any [proxy](#) [132] will slow down as it gains more users, this tends to be more of an issue with public web-based [proxies](#) [132]. And, of course, web-based [proxies](#) [132] 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](#) [132]. Finally, secure web-based [proxies](#) [132] 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](#) [132] behind and attempting to make a direct connection to the target webpage. This is discussed further in the following section.

Other types of [proxies](#) [132] generally require you to install a program or configure an external [proxy](#) [132] 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](#) [132]. Software like this often allows you to change [proxies](#) [132] automatically if one is blocked, as discussed above. If you have to configure an external [proxy](#) [132] address in your browser or operating system, you will need to learn the correct [proxy](#) [132] address, which may change if that [proxy](#) [132] 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](#) [132], 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](#) [132] server. Furthermore, [proxies](#) [132] can be found for a number of different Internet applications. Examples include HTTP [proxies](#) [132] for browsers, SOCKS [proxies](#) [132] for email and chat programs and VPN [proxies](#) [132], which can redirect all of your Internet traffic to avoid filtering.

Secure and insecure proxies:

A secure [proxy](#) [132], in this chapter, refers to any [proxy](#) [132] that supports [encrypted](#) [40] connections from its users. An insecure [proxy](#) [132] 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](#) [132] when accessing websites that are normally [encrypted](#) [40], 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](#) [132] 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](#) [132] exist means that there are very few good reasons to settle for an insecure one.

You will know that a web-based [proxy](#) [132] is secure if you can access the [proxy](#) [139] webpage itself using an [HTTPS](#) [140]

address. As with webmail services, secure and insecure connections may be supported, so you should be certain to use the secure address. Often, in such cases, you will have to accept a 'security certificate warning' from your browser in order to continue. This is the case for both the *Psiphon2* [141] and *Peacefire* [142] *proxies* [132], discussed below. Warnings like this tell you that someone, such as your ISP or a hacker, could be monitoring your connection to the *proxy* [132]. Despite these warnings, it is still a good idea to use secure *proxies* [132] whenever possible. However, when relying on such *proxies* [132] for circumvention, you should avoid visiting secure websites, entering passwords or exchanging sensitive information unless you verify the *proxy's* [139] *SSL* [103] fingerprint. In order to do this, you will need a way of communicating with the *proxy's* [132] administrator.

You should also avoid accessing sensitive information through a web-based *proxy* [132] 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* [132]. It even applies if you know the *proxy* [132] operator well enough to verify the server's *fingerprint* before directing your browser to accept the warning. When you rely on a single *proxy* [132] server for circumvention, its administrator will always know your *IP address* [106] and which website/s you are accessing. More importantly, however, if that *proxy* [132] 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* [132] 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* [132] and anonymity networks recommended in this chapter are secure.

Private and public proxies:

Public *proxies* [132] accept connections from anyone, whereas private *proxies* [132] typically require a username and password. While public *proxies* [132] 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* [132] may be as technically sophisticated and well-maintained as private ones, they are often relatively slow. Finally, private *proxies* [132] 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* [132]. You should not assume, however, that private *proxies* [132] 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* [132] can often be found by searching for terms like 'public proxy' in a search engine, but you should not rely on *proxies* [132] discovered this way. Given the choice, it is better to use a private, secure *proxy* [132] 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* [132] will depend on your own particular needs and preferences. Any time you are using a *proxy* [132] for circumvention, it is also a good idea to use the *Firefox* [13] browser and to install the *NoScript* [14] browser extension, as discussed in the *Firefox Guide* [16]. Doing so can help protect you both from malicious *proxies* [132] and from websites that might try to discover your real *IP address* [106]. Finally, keep in mind that even an *encrypted* [143] *proxy* [132] will not make an insecure website secure. You must still ensure that you have an *HTTPS* [103] connection before sending or receiving sensitive information.

If you are unable to find an individual, organisation or company whose *proxy* [132] 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*.

Specific circumvention proxies

Below are a few specific tools and *proxies* [132] 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* [144] 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. It 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* [145] and on *how to connect to it* [146].

Hotspot Shield is a public, secure, VPN, freeware circumvention proxy. In order to use it, you will need to *download the tool* [147] 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* [40]. Although it is impossible to verify, this company claims to delete the *IP addresses* [106] of those who use the tool, rather than storing or sending them to advertisers.

Your-Freedom is a private, secure, VPN/SOCKS circumvention *proxy* [132]. It is a *freeware* [7] tool that that can be used to access a free circumvention service. There are restriction 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* [148] and *create an account* [149], both of which can be done at the *Your-Freedom website* [150]. You will also need to configure your browser to use the *OpenVPN* [151] proxy when connecting to the Internet. You can *read more in Your-Freedom documentation* [152].

Freegate is a public, secure, VPN, freeware circumvention proxy. You can [download the latest version of Freegate](#) [153] or [read interesting article about it](#) [154].

SecurityKISS is a public, secure, VPN, freeware circumvention proxy. To use it you need to [download and run a free program](#) [155]. There is no need to register an account. The free users are restricted by the limit to 300 MB per day or the Internet traffic through the proxy. Paid subscription offers no restrictions and more VPN servers to use. Please see [SecureKISS homepage to learn more](#) [156].

Psiphon3 is a secure, public VPN and SSH freeware circumvention proxy. To use it you need to request a link to freeware program that will set you up to use the proxy. To request send an email to get@psiphon3.com. Please [see Psiphon3 homepage](#) [157].

Web Proxies:

Psiphon2 is a private, anonymous webproxy servers system. To use [psiphon2](#) [158] you need the web address (URL) of the proxy server and a account (username and password). You may receive an invitation to create account on psiphon2 from a user who already has a psiphon2 account. You may also use invitation included in the printed copy of the how-to booklet. Please [see Psiphon2 homepage](#) [159].

Peacefire maintains a large number of public, web-based [proxies](#) [132], which can be secure or insecure, depending on how you access them. When using a [Peacefire](#) [142] [proxy](#) [132], you must enter the [HTTPS](#) [103] address in order to have a secure connection between yourself and the [proxy](#) [132]. New [proxies](#) [132] are announced to a large mailing list on a regular basis. You can sign up to receive updates at the [Peacefire website](#) [160].

Further reading

- See the *2.5 Internet Surveillance and Monitoring* and *2.6 Censorship circumvention* chapters of the [Digital Security and Privacy Manual for Human Rights Defenders](#) [25] book.
- The FLOSS Manuals website contains a guide on [How to Bypass Internet Censorship](#) [161].
- The [Internet Censorship Wiki](#) [162], written by Freerk, is available in English, German and Spanish.
- The CitizenLab has produced [Everyone's guide to by-passing Internet Censorship](#) [163], 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](#) [164], 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](#) [165].

9. 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.

Background Scenario:

Mansour and Magda are human rights defenders from north Africa. They are organising a march, to take place in the middle of a large city. They want to use Facebook to publicise the event. They are worried that the authorities could be tipped off and that anyone who shows an interest could be traced. They plan to use Twitter during the march to give updates on the progress of the march. But what if the police could monitor the tweets, and deploy squads to intercept marchers? Mansour and Magda plan how to share photos and videos of the march without revealing people's identities, because they worry that participants could face persecution.

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](#) ^[37] 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](#) ^[37].
- **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](#) ^[111].
- 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](#) ^[166] from the Electronic Frontier Foundation website.

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 an Off-the-record plugin, which uses encryption. Read the 'Pidgin – 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. Also 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 it is a gay and lesbian support group that you have set up 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](#) ^[167]

10. 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](#) ^[168], 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.

Background scenario

Borna and his son Delir are both line workers in a factory, and are helping to create a workers' union. Their efforts are meeting the resistance of the factory owners, who are also well-connected in their local government. Borna's supervisor has warned him that he may be under scrutiny by management, and to beware of who he talks to. Borna has purchased a mobile phone for his union work. Delir is helping his father to use his new mobile phone safely for some of his organising activities.

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]](en/glossary#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.

Borna: Son, I have decided only to use this mobile for planning our meetings from now on, because I think they might be listening to the factory floor phone, and maybe even at the house.

Delir: Father, it's great you have finally got a mobile phone, but do you know what it can and cannot do?

Borna: Of course: it is a phone! You call someone, you talk to them, they talk back. You can do this from wherever you are. AND, I can send small messages on it to the others, or to you, and they will show up in your phone.

Delir: This is all true, but it's not all. There are plenty of things you can do these days with these devices. But let's talk about some risks and safety precautions, especially if you think someone might be interested in finding out who you are communicating with, and what you are saying.

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.

Borna: One advantage to the mobile phone is that they won't know where our meetings are if we organise them using our mobiles, while walking in the bazaar, instead of using the normal phones, where they may be overhearing us as we talk. □

Delir: Well, did you say they have connections with the phone company?

Borna: Someone was saying that they are bribing phone technicians to get information.

Delir: If you signed up using your own identity and address for this mobile phone subscription, it is traceable to you, and any time you make a call, its record is linked to your phone subscription and identity. Did you sign up with your own ID?

Borna: No, I just got a second-hand phone from your uncle's shop; he says he made sure it is clean and safe to use. He also helped me buy one of those prepaid little chips you put in your phone.

Delir: Yes, it is called a [SIM card](#) [169]. The phone company tracks each call or transmission with the phone's number, and the SIM card identification number, AND the phone's identification number. So if they know which phone number, OR phone id number, OR SIM card number belongs to you, they may be able to use their contacts to see your phone-use patterns.

Borna: And I suppose they can listen in to my conversations even on my mobile phone then?

Delir: In your case, and thanks to Uncle, your phone isn't registered to you, and the SIM card is also not connected to you in any way. So even if they track where the SIM card and the phone are they don't necessarily know you are connected to the SIM card, or to the phone.

-
- [9.2.1 Best practices for phone security](#) [170]
 - [9.2.2 Basic functions, trackability and anonymity](#) [171]
 - [9.2.3 Text based communications – SMS / Text messages](#) [172]
 - [9.2.4 Functions beyond speech and messages](#) [173]

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](#) [169] 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 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](#) [41]). 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 (International Mobile Equipment Identity) 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.

Borna: Is there anything else about this phone that I need to know?

Delir: I guess yes, but it depends if you really suspect they are trying to track you down.

Borna: I don't think so, but can they do that?

Delir: Well, yes, if you have your phone turned on, AND the technician has access to the network traffic, AND they know which phone on the system is your phone.

Borna: That won't happen because I simply won't make a call on my phone when I go there.

Delir: That doesn't matter father. As long as you have your phone with you, charged and ready to use, it will keep track of where you go, and talk to the towers of the network nearby, simply because it has to. So at any given time, your location is somewhere between the closest towers of the phone network.

Borna: So I should turn it off until I get there?

Delir: Well, of course the best thing to do is not to take it with you. The next best thing is for you to have it switched off AND take the battery out of it before you go, and not turn it on until you get back.

Borna: What? isn't it enough to turn it off?

Delir: Well, to be on the safe side, you should take the battery out, and here's why: this is a transmission device, and as long as the battery is connected, there is a small chance that somehow someone may turn it on without your knowledge.

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 ^[169] 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.

Borna: You're telling me my phone might be talking to the towers about my whereabouts, even it looks as though it's switched off?

Delir: Yeah, and that is not the worst case

Borna: Oh?

Delir: Well, they are saying that there are programs that can be installed on your phone to secretly, remotely turn it on, and have it call a number without your knowledge. Then, as you start your meeting, it would start acting like a recording and transmitting device.

Borna: No! really?.

Delir: Well, it is pretty easily done technologically. But none of that can happen if the battery is disconnected, so you will be safe in this unlikely case.

Borna: I guess I will just not take it with me if I want to be super careful. But I wonder if I should use this thing at all then?

Delir: Please, father. You used to tell me not to be afraid of new things. Mobiles are like that, you just have to know what the benefits and risks are. Just be careful. If you know the risks, you can take steps to avoid them.

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.

Borna: What if I never make calls on my mobile, and only send and receive these small messages. They can't listen in on something if no one is saying anything, and it is very quick, no?

Delir: Wait a minute. These messages are also easy enough to intercept, and anyone with access to the traffic from the phone company, or even other people with the right equipment, can capture and read these messages which are moving around the network in plain text, being saved from one tower to the next.

Borna: That's just silly. What should I do? Write in code like we did during the war?

Delir: Well, sometimes the oldest shoes are the most comfortable ones.

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!

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.

Chapter 11: How to use smartphones as securely as possible ^[174] covers issues related to these kinds of mobile

devices, as connectivity to internet brings about both potentials as well as risks we have covered in previous chapters.

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. Also you should 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*** [41].
- 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](#) [103]).
- 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*** [56].
- Do not accept and install unknown and unverified programmes on your phone, including ring tones, wallpaper, [java applications](#) [175] 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 [Infrared \(IrDA\)](#) [176], [Bluetooth](#) [177] 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](#) [178] released by The Tactical Technology Collective. Among other things, this contains thorough descriptions and guides to the [security of mobile phones](#) [179] and also an extensive range of other tools and examples relating to their use.
- [Security for Activists - A Practical Security Handbook for Activists and Campaigns](#) [180].
- [A Guide to Mobile Phones – A short guide, for activists, to using mobile phones safely and securely](#) [181].
- [A Guide to Mobile Security for Citizen Journalists](#) [182] released by MobileActive.org
- [A Brief Introduction to Secure SMS Messaging in MIDP - Nokia developer guide](#) [183]
- [Phones used as spying devices](#) [184]

11. How to use smartphones as securely as possible

In ***Chapter 10: How to use mobile phones as securely as possible*** [185], 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* ^[186]) 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** ^[185] as all of them are also relevant to smartphone use. **Chapter 10** ^[185] 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** ^[43] 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. Subsequent sections will cover security aspects of the following:

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 phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (*FOSS* ^[187]) 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* ^[168] 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. 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](#) ^[188]

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 *Security settings* in order to use these download sites. Some users may want to consider these alternative sites to minimize online contact with Google. One of the alternative store is **F-Droid** ^[189] ('Free Droid'), which only provides *FOSS* ^[6] applications. However please remember that you should trust the site before you download any apps from it. For inexperienced users we recommend that you use Google Play store.

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* ^[190] 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 10](#) ^[185] section on [Functions beyond speech and messages](#) ^[191]).

Communicating (Voice and Messages) via Smartphone

Talking Securely

Basic telephony

In the section on [Basic functions, trackability and anonymity](#) ^[192] in [Chapter 10: How to use mobile phones as securely as possible](#) ^[185] 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](#) [193] 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](#) [194], 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](#) [195] of [Chapter 7: How to keep your Internet communication private](#) [196], 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](#) [197] 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 \(OSTN\)](#) [198] and the server provided by the Guardian project, [ostel.me](#) [199], 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 CSipSimple, you never directly communicate 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 this 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.me it also comes preconfigured for use with ostel.me, which makes it very easy to install and use.

[RedPhone](#) [200] 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 identifier (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.me 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](#) [185] (in the section on [Text based communications](#) [201]), 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](#) [202] is a [FOSS](#) [8] 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](#) [203]

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** ^[204] as a secure text chat application for the Android phones. Gibberbot offers easy and strong encryption for your chats with *Off-the-Record* ^[93] 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, so your chat messages can be routed through the *Tor* ^[110] 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* ^[205]

For iPhones, the **ChatSecure** ^[206] client provides the same features, although it is not easy to use it with the *Tor* ^[110] network.

A Hands-on Guide for ChatSecure is forthcoming. In the meantime, more information can be found on its [homepage](#) ^[206].

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* ^[188]. 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)** ^[207] allows OpenPGP encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.

Hands-on: Get started with the *APG Guide* ^[207]

Cryptonite ^[208] is another *FOSS* ^[8] files encryption tool. Cryptonite has more advanced features on specially prepared rooted Android phones with a custom firmware. See the *Advanced Smartphone Use* ^[209] section for more.

Hands-on: Get started with the *Cryptonite Guide* ^[210]

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 synchronise this one instead of copying 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* ^[37].

Hands-on: Get started with the *KeePassDroid Guide* ^[211]

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* ^[212] and *Tips on responding to suspected email surveillance* ^[101] in *Chapter 7: How to keep your Internet communication private* ^[196] 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** [207]) 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](#) [213]

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 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 [214] has created a **FOSS** [8] app called **ObscuraCam** [215] 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](#) [216]

At the time of writing, the human rights organisation **Witness** [217] is working with the Guardian project on a solution to all three of the above points.

Accessing the Internet Securely from Smartphones

As discussed in **Chapter 7: How to keep your Internet communication private** [196] and **Chapter 8: How to remain anonymous and bypass censorship on the Internet** [111], 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** [218]. Orbot channels your internet communication through Tor's anonymity network.

Hands-on: Get started with the [Orbot Guide](#) [219]

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](#) [220]

Proxies

The mobile version of [Firefox](#) [13] – **Firefox mobile** [221] 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** [222] add-on (also from [Guardian Project](#) [223], which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the [Tor](#) [110] 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** [224] 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](#) [225].

Encryption of whole volumes

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

Luks Manager ^[226] 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.

Whisper Systems project is preparing application **WhisperCore** ^[227] that will allow full encryption of your Android device.

Virtual Private Network (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** ^[228] server. You can use RiseUp VPN on Android device after installing Cyanogenmod (see above). It is also easy to setup connection to RiseUp VPN on the iPhone - read more [here](#) ^[229].

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
- **Basic Input/Output System (BIOS)** - 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-RW or DVD-RW disc.
- **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. 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: security.ngoinabox.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
- **Free and Open Source Software (FOSS)** - 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.
- **Google Play**: The default repository from which Android applications can be found and downloaded.
- **GNU/Linux** - A FOSS operating system that provides an alternative to Microsoft Windows
- **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.
- **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
- **iPhone**: A brand of smartphones designed by Apple which run the Apple's iOS operating system.
- **Internet Protocol address (IP address)** - A unique identifier assigned to your computer when it is connected to the Internet
- **Internet Service Provider (ISP)** - 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.
- **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.
- **Java Applications (Applets)** - Small programs that can run under many operating systems, are cross-platform. They are frequently used to provide improved functionalities within web pages.
- **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.
- **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.
- **Off the Record (OTR)** - 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.
- **RiseUp** - A 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
- **Secure Sockets Layer (SSL)** - 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. When you are connected to a website through SSL, the address of the website will begin with **HTTPS** rather than **HTTP**.
- **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, but many people believe it to be true. Skype also supports instant messaging.
- **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 visit 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
- **Undelete Plus** - A freeware tool that can sometimes restore information that you may have deleted accidentally
- **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
- **VaultletSuite 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.

Source URL (retrieved on 26/03/2013 - 11:28): <https://securityinabox.org/en/howtobooklet>

Links:

- [1] <https://securityinabox.org/en/glossary#Hacker>
- [2] <https://securityinabox.org/en/glossary#Malware>
- [3] <https://securityinabox.org/en/glossary#Avast>
- [4] <https://securityinabox.org/en/glossary#Spybot>
- [5] https://securityinabox.org/en/glossary#Comodo_Firewall
- [6] https://securityinabox.org/en/glossary#GNU_Linux
- [7] <https://securityinabox.org/en/glossary#Freeware>
- [8] <https://securityinabox.org/en/glossary#FOSS>
- [9] https://securityinabox.org/en/avast_main
- [10] https://securityinabox.org/en/glossary#Clam_Win
- [11] https://securityinabox.org/en/howtouseavast#Section_3.2.1
- [12] https://securityinabox.org/en/spybot_main
- [13] <https://securityinabox.org/en/glossary#Firefox>
- [14] <https://securityinabox.org/en/glossary#NoScript>
- [15] https://securityinabox.org/en/firefox_noscript
- [16] https://securityinabox.org/en/firefox_main
- [17] https://securityinabox.org/en/comodofirewall_main
- [18] https://securityinabox.org/en/chapter_1_5
- [19] <https://securityinabox.org/en/glossary#Router>
- [20] https://securityinabox.org/en/glossary#Proprietary_software
- [21] https://securityinabox.org/en/glossary#Source_code
- [22] <https://www.libreoffice.org/>
- [23] <https://securityinabox.org/en/glossary#LiveCD>
- [24] <http://www.ubuntu.com/>
- [25] <http://www.frontlinedefenders.org/esecman>
- [26] <http://www.virusbtn.com>
- [27] <http://www.marksanborn.net/howto/turn-off-unnecessary-windows-services>
- [28] <http://tacticaltech.org>
- [29] <http://www.askvg.com/download-free-bootable-rescue-cds-from-kaspersky-bitdefender-avira-f-secure-and-others/>
- [30] <http://www.selectrealsecurity.com/malware-removal-guide>
- [31] https://securityinabox.org/en/glossary#Security_policy
- [32] https://securityinabox.org/en/glossary#Physical_threats
- [33] https://securityinabox.org/en/glossary#Physical_threat
- [34] <https://securityinabox.org/en/glossary#Skype>
- [35] <https://securityinabox.org/en/glossary#Server>
- [36] https://securityinabox.org/en/glossary#Security_cable
- [37] <https://securityinabox.org/en/chapter-3>

[38] <https://securityinabox.org/en/glossary#BIOS>
[39] <https://securityinabox.org/en/glossary#Booting>
[40] <https://securityinabox.org/en/glossary#Encryption>
[41] <https://securityinabox.org/en/chapter-4>
[42] <https://securityinabox.org/en/glossary#UPS>
[43] <https://securityinabox.org/en/chapter-5>
[44] https://securityinabox.org/en/chapter_2_5
[45] <http://www.frontlinedefenders.org/manuals/protection>
[46] <http://www.frontlinedefenders.org/security-training>
[47] https://securityinabox.org/en/glossary#Secure_password_database
[48] <https://securityinabox.org/en/glossary#KeePass>
[49] https://securityinabox.org/en/chapter_3_2
[50] https://securityinabox.org/en/glossary#Mnemonic_device
[51] https://passfault.appspot.com/password_strength.html
[52] https://securityinabox.org/en/keepass_main
[53] <http://en.wikipedia.org/wiki/Password>
[54] http://en.wikipedia.org/wiki/Password_strength
[55] http://en.wikipedia.org/wiki/Password_cracking
[56] <https://securityinabox.org/en/chapter-1>
[57] <https://securityinabox.org/en/chapter-2>
[58] <https://securityinabox.org/en/glossary#TrueCrypt>
[59] https://securityinabox.org/en/truecrypt_main
[60] https://securityinabox.org/en/chapter_4_2
[61] <https://securityinabox.org/en/chapter-6>
[62] <https://securityinabox.org/en/glossary#Steganography>
[63] https://securityinabox.org/en/chapter_4_3
[64] <http://www.truecrypt.org/docs/>
[65] <http://www.truecrypt.org/faq.php>
[66] https://securityinabox.org/en/glossary#Cobian_Backup
[67] <https://securityinabox.org/en/glossary#Recuva>
[68] <https://securityinabox.org/en/glossary#Firewall>
[69] <https://securityinabox.org/en/glossary#Thunderbird>
[70] https://securityinabox.org/en/thunderbird_main
[71] https://securityinabox.org/en/glossary#CD_burner
[72] https://securityinabox.org/en/chapter_5_5
[73] https://securityinabox.org/en/cobian_main
[74] https://securityinabox.org/en/recuva_main
[75] <https://www.wuala.com/>
[76] <https://spideroak.com/>
[77] <https://drive.google.com/start>
[78] <https://tahoe-lafs.org/trac/tahoe-lafs>
[79] http://en.wikipedia.org/wiki/Data_recovery
[80] <https://securityinabox.org/en/glossary#Eraser>
[81] <https://securityinabox.org/en/glossary#Wiping>
[82] <https://securityinabox.org/en/glossary#CCleaner>
[83] https://securityinabox.org/en/glossary#Swap_file
[84] https://securityinabox.org/en/eraser_main
[85] <https://securityinabox.org/en/glossary#Cookie>
[86] https://securityinabox.org/en/ccleaner_main
[87] <http://www.piriform.com/ccleaner/faq>
[88] http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/
[89] http://en.wikipedia.org/wiki/Gutmann_method
[90] <https://jitsi.org/>
[91] <https://securityinabox.org/en/glossary#VoIP>
[92] <https://securityinabox.org/en/glossary#RiseUp>
[93] <https://securityinabox.org/en/glossary#OTR>
[94] <https://securityinabox.org/en/glossary#Pidgin>
[95] <https://securityinabox.org/en/glossary#Enigmail>
[96] <https://securityinabox.org/en/glossary#Keylogger>
[97] https://securityinabox.org/en/chapter_7_1#Keeping_your_webmail_private
[98] https://securityinabox.org/en/chapter_7_1#Switching_to_a_more_secure_email_account
[99] https://securityinabox.org/en/chapter_7_4
[100] https://securityinabox.org/en/chapter_7_4#Encrypting_and_authenticating_individual_email_messages
[101] https://securityinabox.org/en/chapter_7_2
[102] <https://securityinabox.org/en/glossary#ISP>
[103] <https://securityinabox.org/en/glossary#SSL>
[104] <https://securityinabox.org/en/discussion#Encryption>
[105] https://securityinabox.org/en/glossary#Security_certificate
[106] https://securityinabox.org/en/glossary#IP_address
[107] https://securityinabox.org/en/chapter_7_5
[108] <https://mail.riseup.net>
[109] https://securityinabox.org/en/riseup_main
[110] <https://securityinabox.org/en/glossary#Tor>
[111] <https://securityinabox.org/en/chapter-8>
[112] <https://securityinabox.org/en/glossary#Circumvention>
[113] https://securityinabox.org/en/pidgin_main
[114] <http://www.skype.com>
[115] <http://jitsi.org/>
[116] <http://www.google.com/talk>
[117] <http://voice.yahoo.com/>
[118] <http://explore.live.com/windows-live-messenger>
[119] https://securityinabox.org/en/chapter_1_4
[120] https://securityinabox.org/en/gpg4usb_portable
[121] <https://securityinabox.org/en/glossary#VaultletSuite>
[122] https://securityinabox.org/en/vaultletsuite_main
[123] https://securityinabox.org/en/glossary#Digital_signature
[124] https://securityinabox.org/en/thunderbird_encryption

[125] <https://help.riseup.net/en/email-clients>
[126] <https://mail.google.com/support/bin/topic.py?topic=12769>
[127] http://email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[128] https://secure.wikimedia.org/wikipedia/en/wiki/Man-in-the-middle_attack
[129] <https://www.google.com/intl/en/privacy/privacy-policy.html>
[130] http://news.cnet.com/8301-13578_3-9962106-38.html
[131] https://securityinabox.org/en/glossary#Domain_name
[132] <https://securityinabox.org/en/glossary#Proxy>
[133] <http://opennet.net/>
[134] <http://www.rsf.org/>
[135] <https://securityinabox.org/en/glossary#Blacklist>
[136] https://securityinabox.org/en/glossary#Domain_names
[137] https://securityinabox.org/en/glossary#IP_addresses
[138] https://securityinabox.org/en/tor_main
[139] <https://securityinabox.org/en/glossary%23Proxy>
[140] <https://securityinabox.org/en/glossary#HTTPS>
[141] <https://securityinabox.org/en/glossary#Psiphon>
[142] <https://securityinabox.org/en/glossary#Peacefire>
[143] <https://securityinabox.org/en/glossary#Encrypted>
[144] https://securityinabox.org/en/chapter_8_5
[145] <https://help.riseup.net/en/riseup-vpn>
[146] <https://we.riseup.net/riseuphelp+en/vpn-howto>
[147] <http://www.hotspotshield.com/>
[148] <http://www.your-freedom.net/index.php?id=3>
[149] <http://www.your-freedom.net/index.php?id=170&L=0>
[150] <http://your-freedom.net>
[151] <https://www.your-freedom.net/index.php?id=172>
[152] <https://www.your-freedom.net/index.php?id=doc>
[153] <http://www.dit-inc.us/freegate>
[154] <http://www.addictivetips.com/windows-tips/freegate-lets-you-access-blocked-websites-at-optimal-speed/>
[155] <http://www.securitykiss.com/resources/download/>
[156] <http://www.securitykiss.com>
[157] http://psiphon.ca/?page_id=204
[158] <http://www.psiphon.ca/>
[159] http://psiphon.ca/?page_id=196
[160] <http://peacefire.org/>
[161] <https://www.howtobypassinternet censorship.org/>
[162] http://en.cship.org/wiki/Main_Page
[163] <http://citizenlab.org/guides/everyones-guide-english.pdf>
[164] http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf
[165] <http://advocacy.globalvoicesonline.org/tools/guide/>
[166] <https://www.eff.org/wp/locational-privacy>
[167] https://securityinabox.org/en/social_networking_tools
[168] <https://securityinabox.org/en/glossary#GPS>
[169] https://securityinabox.org/en/glossary#SIM_card
[170] <https://securityinabox.org/en/node/1777>
[171] <https://securityinabox.org/en/node/1778>
[172] <https://securityinabox.org/en/node/1779>
[173] <https://securityinabox.org/en/node/1780>
[174] <https://securityinabox.org/en/chapter-11>
[175] <https://securityinabox.org/en/glossary#Java>
[176] <https://securityinabox.org/en/glossary#rDA>
[177] <https://securityinabox.org/en/glossary#Bluetooth>
[178] <http://mobiles.tacticaltech.org>
[179] <http://mobiles.tacticaltech.org/security>
[180] <http://www.activistsecurity.org/>
[181] http://www.freebeagles.org/articles/mobile_phones.html
[182] <http://mobileactive.org/mobilesecurity-citizenjournalism>
[183] http://sw.nokia.com/id/5274b81c-12d0-43bb-8d89-26f6a1ae111f/A_Brief_Introduction_to_Secure_SMS_Messaging_in_MIDP_en.pdf
[184] <http://www.mysecured.com/?p=127>
[185] <https://securityinabox.org/en/chapter-10>
[186] <https://securityinabox.org/en/Glossary#GPS>
[187] <https://securityinabox.org/en/Glossary#FOSS>
[188] https://securityinabox.org/en/android_basic
[189] <http://f-droid.org>
[190] <https://securityinabox.org/en/glossary#apk>
[191] https://securityinabox.org/en/chapter_10_2_4
[192] https://securityinabox.org/en/chapter_10_2_2
[193] <https://securityinabox.org/en/Glossary#VoIP>
[194] <https://securityinabox.org/en/glossary#skype>
[195] https://securityinabox.org/en/chapter_7_3
[196] <https://securityinabox.org/en/chapter-7>
[197] <http://f-droid.org/repository/browse/?fdid=com.csipsimple&fdpage=4>
[198] <https://guardianproject.info/wiki/OSTN>
[199] <https://ostel.me>
[200] <https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone>
[201] https://securityinabox.org/en/chapter_10_2_3
[202] <https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms>
[203] https://securityinabox.org/en/textsecure_main
[204] <https://guardianproject.info/apps/gibber/>
[205] https://securityinabox.org/en/gibberbot_main
[206] <https://chatsecure.org>
[207] https://securityinabox.org/en/APG_main
[208] <https://code.google.com/p/cryptonite/>
[209] https://securityinabox.org/en/chapter_11_7
[210] https://securityinabox.org/en/Cryptonite_main
[211] https://securityinabox.org/en/KeepassDroid_main

- [212] https://securityinabox.org/en/chapter_7_1
- [213] https://securityinabox.org/en/K9_APG_main
- [214] <https://guardianproject.info>
- [215] <https://guardianproject.info/apps/obscuracam/>
- [216] https://securityinabox.org/en/Obскурacam_main
- [217] <https://securityinabox.org/en/www.witness.org>
- [218] <https://www.torproject.org/docs/android.html.en>
- [219] https://securityinabox.org/en/Orbot_main
- [220] https://securityinabox.org/en/Orweb_main
- [221] <http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox>
- [222] <https://guardianproject.info/apps/proxymob-firefox-add-on/>
- [223] <https://guardianproject.info/>
- [224] <http://www.cyanogenmod.com>
- [225] <http://www.cyanogenmod.com/devices>
- [226] <https://play.google.com/store/apps/details?id=com.nemesis2.luksmanager&hl=en>
- [227] <http://www.whispersys.com/whispercore.html>
- [228] <https://help.riseup.net/en/vpn>
- [229] <https://support.apple.com/kb/HT1424>