Information Security for Journalists

This handbook is a very important practical tool for journalists. And it is of particular importance to investigative reporters. For the first time journalists are now aware that virtually every electronic communication we make or receive is being recorded, stored and subject to analysis and action. As this surveillance is being conducted in secret, without scrutiny, transparency or any realistic form of accountability, our sources, our stories and our professional work itself is under threat.

After Snowden's disclosures we know that there are real safeguards and real counter measures available. The CIJ's latest handbook, ***Information Security For Journalists***, lays out the most effective means of keeping your work private and safe from spying. It explains how to write safely, how to think about security and how to safely receive, store and send information that a government or powerful corporation may be keen for you not to know, to have or to share. To ensure your privacy and the safety of your sources, ***Information Security For Journalists*** will help you to make your communications indecipherable, untraceable and anonymous.

Although this handbook is largely about how to use your computer, you don't need to have a computer science degree to use it. Its authors, and the experts advising the project are ensuring its practical accuracy and usability, and work with the latest technology.

Gavin MacFadyen, Director of the Centre for Investigative Journalism

By Silkie Carlo and Arjen Kamphuis

Acknowledgements

I would like to express my deep gratitude to Arjen Kamphuis for his truly brilliant, patient and generous teaching, for his excellent work and for his friendship.

Many thanks to Gavin MacFadyen and the CIJ for commissioning and trusting us with the responsibility of writing a handbook that aims to protect his journalists and their sources, and for his information security advocacy generally.

We collectively thank the whistleblowers, none more than Edward Snowden, for democratising the information that we now profit from in defending ourselves, our sources, and a free press.

With sincere thanks to the journalists who intend to use this manual,

Silkie Carlo

--

Thanks to the heroes of the Free Software Foundation who foresaw the problems we now have 30 years ago and moved to make sure we have alternatives.

Thanks to the developers and hackers who freely share their work with all humanity.

Thanks to Gavin, Juliet and Minal at CIJ for all their great work in support of journalism (including supporting us in making this book).

Thanks to the whistleblowers for their courage and sacrifice.

And thanks to Silkie Carlo, my co-author, for curiosity, drive, grace under fire and never settling for less than her best.

I dedicate this book to my parents, Ida & Andre Kamphuis, who raised me to stand up for principles and never bow down to authorities trying to destroy them.

Arjen Kamphuis

Contents

Foreword

Over the last 12 months all the most extreme paranoid fears of privacy activists and information security experts have turned out to be but cuddly little problems compared to the reality of industrialised espionage on the entire planet. Anyone who has kept abreast of the ongoing revelations as a journalist with the desire to protect their sources and their stories from government or corporate snoopers may have felt despair. Is everything with a chip and a battery spying on us? When considering most off-the-shelf computing devices such as laptops, tablets and smartphones, the situation is indeed dire. But there are steps you can take and those steps are not expensive nor do they require a Phd in computer-science. Using a computer system that can withstand all but the most advanced attacks by the most advanced nation state-level attackers is well within the reach of everyone.

That is, anyone who is willing to spend a few days learning to use software that is free of cost and hardware that is already available to you or that can be bought for under 200 Euros/Pounds/Dollars. This handbook can get you started on understanding how to secure your data and communications and those of your sources, and to use tools and methods that have been proven to work in the most extreme situations by experts all over the world.

Depending on your pre-existing computer skills this may be a bit of a learning experience, but trust that many have gone before you who also did not consider themselves experts and yet they managed to become comfortable with the concepts and tools described in this book.

If you are a journalist in the 21st century you need these tools. After all even William Randolph Hearst said decades ago: journalism is writing down what powerful people and institutions do not want written.

If you don't consider yourself to be a journalist but merely insist on actually having the right to privacy guaranteed to you under the UN Declaration Of Human Rights [1948] Article 12 - this book is for you too.

Like almost everyone who ever created anything we could only do so by standing on the shoulders of a thousand generations that came before us. Thus this book will be forever freely available in a range of electronic formats without any restrictions. If the format you would like is missing just let us know.

If you appreciate this work please spread it around as much as possible and help us make the next version better. Constructive feedback of any kind is most welcome. The problem will keep developing and so will our response. Please contribute to sharing this knowledge and promoting these tools in any way you can.

Arjen Kamphuis

Preface

Four weeks before Edward Snowden blew the whistle on extraordinary surveillance capabilities, I was fairly computer illiterate, raised on Microsoft and unable to do basic tasks on a Mac. About to embark on an investigative project and campaign, I was suitably paranoid and started my first encrypted email account, thanks to a lengthy walk-through over the phone with Arjen. Like many learning curves, the technology initially felt daunting. Worse still, only a handful of people I was communicating with used encryption.

This changed very quickly.

On June 5th 2013, the Guardian published Snowden's revelations of the PRISM program. I realised, with the rest of the sane world, that our Orwellian nightmare was now a reality. Only, the reality was far more bleak, chilling and stark than the nightmare we read about in fiction. The reality is that the nightmare develops in seemingly banal episodes, until you can no longer wake from it. Moreover, the reality is that there is the ability and responsibility to act. Thanks to Snowden, we know how critical this episode is and we are empowered with the information and the opportunity to act.

If journalism is printing what someone else does not want printed, and for investigative journalists it certainly is, you must assume that in the course of producing your best work, you have an adversary against whom you must protect yourself, your story, and your sources.

Since June 5th 2013, I felt it important to educate myself in the information security methods that protect freedom of speech and freedom of press – simple methods that are, without overstatement, essential to preserve and advance democracies, and essential to protect the individuals involved in doing so. As a total novice to computing, with no natural abilities in this area, I am testament to the fact that anyone who understands the importance of information security and has the patience to learn, can become an advanced user of 'infosec' methods in a matter of months.

This handbook is the product of a novice's year of learning (that's me) under an expert's teaching and guidance (that's Arjen), and is written in the plainest terms possible, with comprehensive instructions, to share with you a shortcut to this learning process – without compromising knowledge, teaching or security. The best way to learn is by doing – so I strongly advise that you use this handbook whilst also tooling up for infosec, and follow instructions as you go along.

Importantly, I hope that this handbook empowers a wide range of investigative journalists and especially their sources – including those facing the highest risks. Therefore, some information within is suitable for a 'Snowden scenario' – and I am quite sure there are many more would-be sources out there whose information merits a similar degree of security.

If this handbook relieves one victim of injustice or witness of criminality from the burden of their story; if it liberates one individual to securely communicate with the world and have their voice safely heard, then this handbook will have served its purpose very well.

Silkie Carlo

Introduction

Imagine opening your inbox to find an anonymous email from someone offering to share important, sensitive documents of international significance with you. The source, and the information, requires the highest level of protection. What do you do?

This manual is designed to instruct journalists and media organisations on how to practise information security in the digital age, protecting your work, your sources, and your communications at a variety of risk levels.

Information security, or "infosec", is the practice of defending information from unauthorized access. The information at stake may include a news report you are working on and any associated files, the identity of your source(s), your communication with them, and at times, your own identity.

You don't need to be an I.T. expert to practise infosec (although you will certainly learn a lot as you go along!). Using this manual, you could find yourself sending encrypted mail and documents from your own highly secure laptop within days!

The Threats: Who Poses a Threat?

Targeted threats

The Snowden revelations have exposed the extraordinary abilities of certain government intelligence agencies to intercept communications, and gain unauthorized access to data on almost any personal computer or electronic communication device in the world. This could pose an information security risk to investigative journalists working on stories concerning the interests of those governments, their agencies, and their private intelligence contractors.

Many states lack these sophisticated surveillance technologies – but all states do possess surveillance capabilities, some of which can be, and at times have been, used against journalists, with potentially severe consequences. Ethiopia, a less technologically advanced state, is alleged to have launched remote attacks against journalists stationed in US offices.

In the globalized age, some transnational corporations have greater wealth and power than many sovereign nation states. Correspondingly, some transnational corporations possess greater 'security' or surveillance capabilities than many nation states.

It is not only corporations, but sophisticated criminal organisations that have also been known to employ impressive surveillance technologies – and some criminal organisations may overlap with criminal elements in government. The Mexican army spent $350 million on surveillance tools between 2011-2012, and reportedly now possess technologies to collect text messages, phone calls and emails; to remotely automate audio recording on mobile phones; and even to

detect movement through walls using radar technology. Also between 2011-2012, 9 journalists were killed in Mexico in association with their work.

Unauthorised access to your data may entail its use, disclosure, disruption, modification, inspection, recording or destruction. You and your source could invoke legal or physical risks, and the information at the heart of your story could be compromised. In high risk situations, infosec may be as important as wearing a bullet-proof vest and travelling with bodyguards. However, because digital threats are invisible, complex and often undetectable they tend to be overlooked.

Dragnet threats

You may also wish to protect yourself from 'dragnet' surveillance programs, led by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ).

These are programs that sift through and collect the world's online and telecommunication data - potentially enabling "retroactive investigation." Should you become a person of interest to the government, for example through reporting of secret or controversial state activities, it would be possible to compile a record of your daily activity going back, under current law, as far as five or more years.

Practising Infosec

As an effective journalist, you may find yourself disturbing a few hornets' nests in the course of your career. Practising good infosec therefore means not only employing case-by-case protection strategies, but normalising several permanent strategies that easily fit into your everyday life. However, you will need to use stronger and more effortful infosec methods when working on sensitive topics, and with vulnerable sources.

The first step to practising good infosec is to be aware of the threats; the second, is to be aware of your hardware and software vulnerabilities. Understanding how and why unauthorized access happens is the first step in learning how to protect yourself from it. The threats will change, with time – but so too will the technologies available to protect journalists and citizens. So, it is important to understand infosec in theory, and to always continue learning about infosec in practice.

Chapter 1: Protecting the System

You security and/or encryption methods will only be effective if each level of your system is secure. You can send your emails with unbreakable encryption, or use the strongest conceivable passwords, but if your system is 'bugged', hacked, or vulnerable, your efforts may be futile.

Depending on your risk level, and the sophistication of your adversary, protection strategies range from simply keeping your laptop or phone on your person at all times, to using a second-hand, cash-bought, laptop and practising robust infosec, for some specific purpose.

Think of 'protecting your system' as building a house of cards. Without building security from the bottom up, the whole thing falls down.

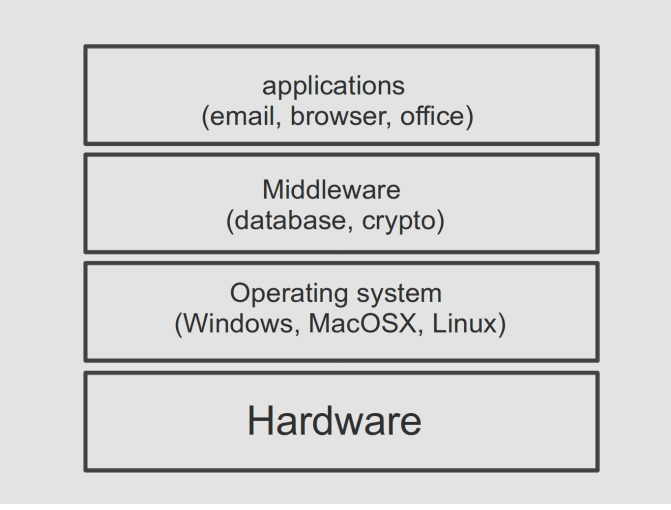
In this section, you will learn how to build a secure system, from the hardware to the middleware.

This chapter is the most important of the book. It is also fairly technical, and contains the most difficult information of any chapter in the book. The solutions here are many, and ultimate security is the outcome of only one. Here, we lay out the horrible reality of the number of hardware vulnerabilities, and leave the reader to decide what the appropriate security measures are for themselves. For several of the solutions described here (such as internal maintenance of the hardware, and certainly for replacing firmware) you will need expert help.

As lengthy, technical, and dis-spiriting much of this chapter is, please do read on. You should be aware of the vulnerabilities within your own system, even if you do not have the ability or need to currently solve them. This is important information that will guide your trust and use of your system, and prepare you for the future, simpler solutions that we hope will soon be developed.

Your computer model

Interface - screen
Applications – your programs
Middleware - *programming that "glues together"/mediates between two separate and often already existing programs: e.g. allows programs to access databases*
Operating System - Windows, OS X, Linux, etc.
Firmware – *software programmed onto hardware that provides instructions for how the device communicates with the other computer hardware*
Hardware – *the physical elements that comprise a computer system*



2.1 Hardware and firmware:

This refers to your physical machine. Desktop computers are not recommended for important journalistic work as they are immobile and as such not only impractical but vulnerable to physical intervention when you are not around. Laptops will be discussed here.

For our purposes "laptop" refers to all physical components, including the battery, hard disk drive, CD drive, wifi card, microphone, and webcam. Let's also consider additional hardware: any keyboard, mouse, scanner/printer, webcam, and so on that you connect to your laptop.

Threats to hardware

- Theft or damage
- Physical attack
- Virtual/remote attack

The main risks to your hardware are that it will be stolen, damaged, physically tampered with or 'bugged', or virtually/remotely accessed in order to transmit signals (ie. collect your information).

Five key measures are important for hardware protection:

> *Preventing physical attacks on your hardware*

1. Buy your laptop in person, with cash
2. Keep the machine on you
3. Consider detectability measures should you need to be separated from your laptop

> *Preventing virtual and physical attacks on your hardware*

4. Buy a machine that permits open source software
5. Remove and replace certain components

Although these five steps may sound confusing and even daunting at first, they are all entirely doable for journalists who are new to IT and infosec. How to obtain and maintain your secure hardware is explained in the five steps below – all you have to do is choose the risk level you want to prepare yourself for, and take the following steps.

1. How to buy your laptop

As you learn about infosec, you will want to purchase one or two new laptops. This is not only a wise decision when working with a new high risk source, or when working on a very sensitive story, but to prepare yourself for the possibility of such eventualities, and as a general measure to implement your new infosec learning.

The process of buying secure laptops should be as anonymous as possible, in order to prevent any adversary from pre-positioning surveillance tools in your hardware, or being alerted to your new hardware and thus being motivated to physically or virtually invade your machine after purchase.

If you are working with a high-risk source, such as an intelligence whistleblower, that person may already be under surveillance. You should assume that the surveillance risk that applies to your source also applies to you.

The Snowden documents revealed that intelligence agencies intercept devices to implant surveillance tools before factory sealing them and putting them back into transit – so you should avoid purchasing any hardware (even chargers) online. Most elements of hardware can be modified to act as surveillance tools.

You should decide what model of laptop you want to buy first (after reading this chapter), and be sure to do any research before buying using the anonymous Tor browser (see chapter 3). You should buy your laptop/s in person, with cash. You will likely be buying an older model so find an area, preferably some distance from where you normally shop, with several second hand electronics shops. To avoid arousing suspicion, you may wish to use several different shops to buy each laptop and accessory (e.g. USB sticks).

For media and campaign organisations, it is a good idea to pre-emptively tool up with secure laptops. For advice on ready made toolkits and training, contact infosec@tcij.org.

The risks:

- Interception and covert installation of surveillance tools
- Inadvertently informing adversaries of your intent to buy a new, particularly secure, machine thus arousing suspicion of this is 'out of character' behavior which would suggest contact with an important source or sensitive topic, and leading to increased surveillance or intervention of you and/or your source (high risk situations)
- A laptop being traceable back to you or your source, which may be unwanted in high risk situations

Infosec action:

- Research which model you will buy and/or where using the anonymous Tor browser
- Buy your laptop in person, with cash
- When buying your laptop, place any device that could locate you (i.e. your phone) in a Faraday cage or leave it somewhere safe at home
- Buy accessories such as Wi-Fi dongles and USB sticks separately to the purchase of your machine (also in person)
- Media organisations should prepare by tooling up training now and pre-prepared equipment (that should be stored in a safe until use) now – the CIJ can provide this

2. How to guard your laptop

Preventing theft, damage, and physical attacks or interventions on your hardware means adopting an important new behaviour: keep your laptop on you, near you, and within your sight at all times. Adopting such behaviour is called 'OpSec', or 'Operational Security'. If at any point your laptop is left unattended or should it find its way into someone else's possession (for example, checked-in baggage on a flight, or with the police/authorities), you must consider, depending on your risk level, the possibility that any part of the system may no longer be secure. If one part of the system is insecure, the whole system is.

Keep your system as simple, small, and light as possible – avoid connecting the laptop with a mouse, keyboard, printer, docking station, or other devices (which, for high risk targets, could conceivably be 'bugged') to limit the hardware you need to carry with you or be responsible for.

You need to consider the physical security of your hardware not only currently and from now on, but retrospectively. Could it have been physically attacked before? How was it manufactured – could the hardware already be compromised (see points 4 and 5)?

From the moment you order your laptop, you assign your person and thus your risks and responsibilities to it. Since we know that shipment may be a risk, we advised you to buy new hardware in person, with cash (see 'how to buy your laptop'). Not only is this a more anonymous way of acquiring a new laptop, but you can take responsibility for it immediately.

The risks:

- An adversary may steal your laptop
- An adversary/you may (accidentally) damage your laptop
- An adversary may physically tamper with your laptop when it is out of your sight (you leave it briefly in a café/you leave it at home or the office/you order it online and the shipment is intercepted)
- An intelligence agent may enter your offices and smash your machines

Infosec action:

- keep your laptop on you, near you, and within your sight at all times
- avoid connecting the laptop with other hardware (e.g. a mouse, docking station, etc)
- buy new hardware in person, with cash

3. How to detect a security breach

Detecting possible physical interventions with your laptop is extremely difficult, if not impossible. If you do need to securely store your laptop for some reason (for example, you wish to cross a border without your laptop) you should try to do so in a way whereby any disruption would be detectable. Be creative - but it is

unlikely you will outsmart a sophisticated adversary. Ideally, you will leave it under the close protection of someone you trust, if you cannot guard it yourself.

For technological defence against low levels of risk, and a general safety measure, you can download an **open source** application called Prey: see https://preyproject.com. This is tracking software that helps users find, lock and recover their computers. It also enables you to take screenshots of the stolen laptop's screen, and to activate the webcam to take a photo of its new owner. Downloading tracking software may feel counter-intuitive for a journalist who wants to strictly defend their privacy! Since the application is open source, it is fairly trustworthy. However, a sophisticated adversary will not be caught out by it. It is only recommended to use this application as a defence against less advanced adversaries.

The risks:

- physical tampering with your machine without your knowledge, resulting in a false sense of security

Infosec action:

- keep your laptop on you, near you, and within your sight at all times
- employ detection tactics, such as Prey (see https://preyproject.com)

4. What to buy

What laptop you buy determines the security level you will be able to achieve. As we learn more about extensive surveillance capabilities from the Snowden documents, we learn too what machines are and are not securable. Hopefully, with time, we will be able to develop more secure solutions. However, at the moment, very few laptops are entirely securable against the highest levels of threat.

This may not be a problem for you or your source, depending on who your adversary is. If you are defending your communications and data from a powerful government or an ally (which, in practical terms, may include significant banks and corporations), you will need excellent security for your laptop/s. How important you are to your adversary dictates whether you need high level security, or top security. Otherwise, whether you are defending against corporations, political, military, terrorist or rebel groups, private security firms, or specific individuals, you will have to estimate how sophisticated the tools of your adversary are, and thus, what measures you wish to take.

General advice on buying laptops at different risk levels:

Low risk: dragnet surveillance, low grade individual hacking, and theft

A good investigative journalist will outgrow this category before long! Most computer hardware is fairly securable against unsophisticated threats at the software level, and by keeping your machine on you at all times to defend against theft or covert interventions. Even MacBooks are suitable choices to defend

against low level threats because, whilst you cannot install a operating system of your choice, the inbuilt ones tend to be particularly resistant to malware. You can also avoid the digital dragnet, through software and application choices.

- You can start with any laptop.

Medium risk: targeted surveillance, by an adversary with relatively unsophisticated capabilities, or who is prepared or able to invest relatively limited resources

You will need to have a laptop that allows you to unscrew the casing and get inside the machine, so you can do some basic hardware 'maintenance', and choose which components to keep or disable; and a laptop which allows you to install the operating system of your choice (ideally, open-source). Many IBM/Lenovo, HP, and Dell laptops are suitable for this, and provide extensive hardware documentation on their websites that assists with DIY hardware modification[1]. MacBooks are unsuitable, as they do not allow you to switch operating systems (and their operating systems have flaws/potential backdoors).

- Start with, preferably an IBM/Lenovo Thinkpad or a HP or Dell laptop that allows you to open the casing.

High risk: targeted surveillance by an intelligence agency

Go for an older laptop (ideally pre-2009) that allows you to unscrew the casing and get inside the machine (IBM Thinkpads are ideal). You will want to do internal hardware maintenance, and use an open-source operating system. By buying a pre-2009 laptop, you are more likely defended against an adversary remotely controlling your laptop.

Expert info: why pre-2009? From around 2006, Intel started putting special components in their chipsets (combinations of chips that work together on laptop motherboards, i.e. the 'computer' within the casing) to allow the automated management of systems over a network. This is called 'Intel Advanced Management Technology', and means that an I.T. technician in a large office/university I.T. suite can update software, or do other things to machines, without having to be physically near them. The problem, of course, is that the same functionality can be abused to install spyware or manipulate the systems in other ways. All laptops made after 2008 contain these chipsets, and are therefore vulnerable to these types of attacks when they are on a network (e.g. the internet). It is thought that the 'Intel 945' chipset is the most recently made chipset without this automatable feature (hence lends itself to a securable motherboard).

- Start with an old IBM/Lenovo Thinkpad (preferably), or a HP or Dell laptop, (ideally manufactured pre-2009) and that allows you to open the

[1] Such hardware flexibility and documentation is also be available for other brands – the above suggestions are not endorsements of these brands or their products

casing

Top risk level: targeted, focused surveillance by an intelligence agency, possibly with a view to compromise the safety and freedom of the target/s, and the integrity of their data

Use two laptops: both should be old (pre-2009) machines, as above; one will be entirely offline ('air-gapped'), the other you will allow online.

Fact: Glenn Greenwald uses an air-gapped laptop to work on the Snowden documents.

In very high risk situations, you will have at least two laptops which have all the above security measures implemented – only, on one of those laptops, you will never connect it to the internet, even via a USB Wi-Fi dongle. This will be your 'airgap' machine – a laptop that never, ever goes online. This can be a very useful machine for storing files (for example, that you have on a USB stick), writing articles, and producing your reports on. You will need to be able to open this laptop to do some internal maintenance and remove connectivity devices, to ensure it truly is offline at all times (see point 5).

This adds an extra level of security to your source's data, because your important documents are stored not only on an incredibly secure machine, but also entirely offline. Even the most secure machine may be exposed to some degree of risk when it goes online, and is particularly likely to if you are the subject of a focused attack.

Advanced info: *At this risk level, you should also defend your laptop against firmware, or BIOS, attacks – another way in which your machine can be remotely accessed to steal your data. As usual, this means replacing closed source with open source solutions, but this should be done by an experienced infosec expert (see point 5). We recommend Coreboot, which is an open source BIOS. Although Coreboot is currently compatible with 230 motherboards, very few of those motherboards lack Intel's Advanced Management Technology chipsets, which have been almost ubiquitous since 2008. Currently, only a small handful of laptops have motherboards that are compatible with Coreboot, and also pre-Intel 965 chipsets (i.e. remotely accessible chipsets).*

At present, the ideal model to secure against top level threats is the IBM Thinkpad X60 (and X60s, including tablet forms), as it is one of the most modern models which lacks the remotely accessible chipset), and it is highly compatible with Coreboot – so, after all of the hard work securing your hardware, the machine will still function well.

- Buy two laptops: one to air-gap and one to go online
- IBM Thinkpad X60 (or X60s) is currently the most securable and functional machine
- If you can gain access to expert help, a laptop compatible with Coreboot is ideal.

What to buy, in summary

The risks:

- surveillance "backdoors", and vulnerabilities to backdoors inherent in the manufacture of many hardware components, firmware, and operating system
- inability to open, inspect, or replace hardware components (Mac, and other modern laptops)
- inability to replace a closed source with an open source operating system (Mac)
- *Advanced:* inability to replace closed source with open source firmware

Infosec action:

- avoid Mac, which prevents opening and inspecting hardware elements, or open source operating systems
- For medium risk, buy an IBM/Lenovo Thinkpad, HP or Dell laptop that allows you to open the casing
- For high risk, buy a pre-2009 IBM/Lenovo Thinkpad, HP or Dell laptop that allows you to open the casing
- For top security, use an air-gapped computer in addition to the 'high risk' laptop that you allow online, and also make sure your online laptop is compatible with Coreboot
- IBM Thinkpad X60 (or X60s) is currently the most securable and functional machine

5. Why, and how, to remove and replace certain components

Now that you have a securable laptop, you need to secure it!

Let's take a look at all of the internal components that could potentially be used to surveil you, your source and your work.

- Webcam
- Microphone
- Hard disk drive
- Wi-Fi card
- Bluetooth card
- 3G modem
- Ethernet port
- BIOS
- Chipset (post Intel 945)

Webcam:

Not only can webcams be remotely and covertly activated for specific targets, but webcam images have also been intercepted as part of dragnet surveillance

programs (see the Snowden revelation of GCHQ's OPTIC NERVE program). A simple solution is to place a sticker over your webcam.

Microphone:

Your laptop's microphone can also be remotely and covertly activated, to capture audio. You could try putting hot glue over the microphone input on your laptop casing, to muffle sounds. Better still, open your casing and cut the microphone wire.

Hard disk drive:

Some hard disk drives have been found to contain 'bad' firmware – that is, they could potentially be activated to compromise your security, should you become a target to an agency with a very sophisticated toolkit.

It is advisable to remove the hard disk drive, and instead work from USB sticks ('flash drives'). Flash drives are also ideal for storing the highly secure operating system, Tails (see chapter 2) – that is, they can hold a small, anonymising system for you to work from. USB sticks are highly portable, replicable (to share with colleagues/sources), and are easily protectable by high grade encryption (see chapter 4). This also means that, if your laptop is stolen or damaged, the data stored on your USB is still safe.

However, you may wish to keep the hard disk drive for your general day to day work, and work from USB sticks for specific projects (using Tails sticks, see chapter 2). This works too – but it is still good to practice removing your hard disk drive, should your risk level increase, or if you begin to distrust it.

WiFi card, Bluetooth card, 3G modem:

Any element that permits connectivity may be remotely and covertly activated to install surveillance tools, or indeed to send your data back to your adversary (high risk projects). Therefore, you should aim to have as much control over your laptop's connectivity as possible.

The best way to do this is to physically remove these components. This means opening the laptop casing, and unscrewing the WiFi card, as well as a Bluetooth card and 3G modem, should your laptop have these (consult your laptop's handbook if you are unsure – copies can often be found online). This may feel like a daunting task at first, but anyone with a steady hand and correct instruction can easily do this first-time.

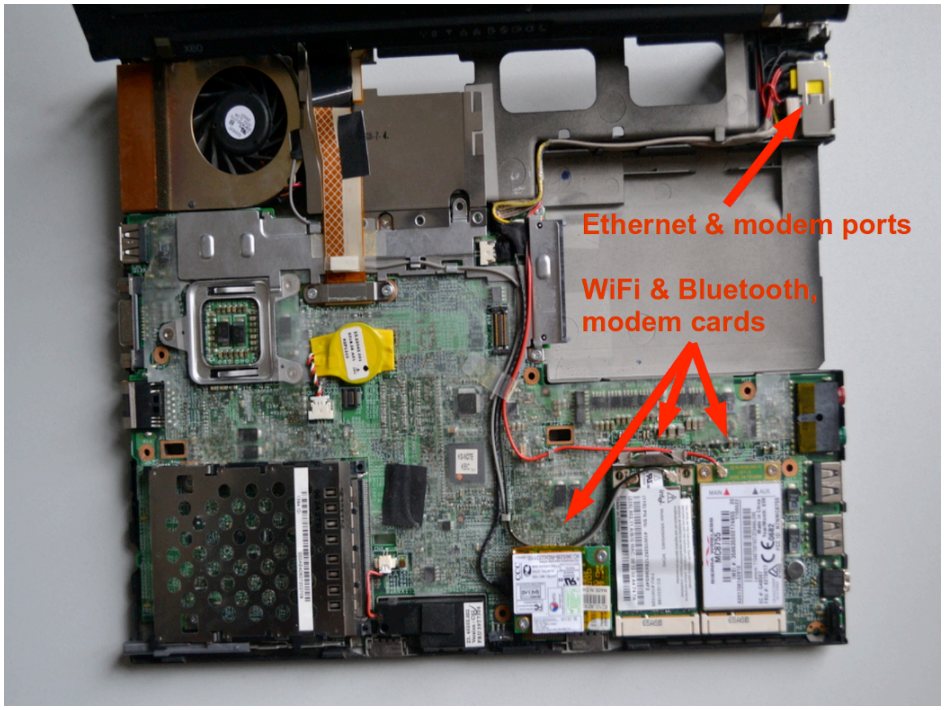
Then you can control when you are, and are not, online. You should buy a WiFi USB adapter, which functions in the same way as your WiFi card – it allows you to connect to the internet. The difference is, that you can easily connect and disconnect the adapter from the USB port, and so *you* decide when you go online and offline.

Ethernet port:

The Ethernet port is what you use to physically connect to a 'local area network' (LAN), which can be the anything from a network in a large office building or a home router box from your Telecom or Cable company. WiFi is more commonly used now, and an Ethernet port is no longer essential.

It is known that Ethernet ports have specific security vulnerabilities that can be exploited against high risk targets, although the extent is not fully known.

To defend your machine against Ethernet exploitation, you could fill the port with hot glue. Alternatively, you could disconnect the port wiring inside the laptop. However, if you have removed your WiFi card, you may wish to keep the Ethernet port as a means by which to connect to the internet.



BIOS
Basic Input/Output System - a set of computer instructions in firmware which control input and output operations.

At the top level of risk, you may also wish to defend your laptop against firmware, or BIOS, attacks – another way in which your machine can be remotely accessed to steal your data. Unfortunately, the Snowden documents indicate that, if you are a government target, a BIOS attack is a fairly easy, yet highly sophisticated, attack to employ.

As usual, this means replacing closed source with an open source solution – however, it is very tricky to do this with firmware. We would recommend that you seek a trusted and experienced infosec expert (contact the CIJ for advice) to help you do this. This is also why it is a good idea for an ambitious journalist

anticipating a highly sensitive story to obtain a prepared laptop well before one enters a situation where it is suddenly needed.

Chipset

See the 'expert info' box in 'What to buy' (point 4). There is nothing you can feasibly do to replace an undesirable chipset, so use the guide in the 'what to buy' to make sure you purchase a securable machine.

Why, and how, to remove and replace certain components – in summary:

The risks:

The remote, covert activation of the following elements, either due to a new virtual attack or pre-existing physical feature/intervention, to collect and/or send data to an adversary:

- Webcam
- Microphone
- Hard disk drive
- Wi-Fi card
- Bluetooth card
- 3G modem
- Ethernet port
- BIOS
- Chipset (post Intel 945)

Infosec action:

- Find the many helpful removal instructions and hardware manuals online, using the Tor browser, when working on securing your hardware
- place a sticker over your webcam
- hot glue the external microphone input; or better, open cut the internal microphone wire
- remove the hard disk drive, and instead work from USB flash drives
- unscrew the WiFi card, as well as any other connectivity devices present (e.g. Bluetooth card)
- connect your online laptop to the internet via a WiFi USB adapter
- fill the Ethernet port with hot glue, or better, disconnect the port's wiring inside the laptop
- with expert help or excellent training, replace closed source with open source firmware (Coreboot)

If you wish to continue using non-securable hardware, there are still measures you can take to protect you data and communications – so do read on. Just be aware that, if you become a surveillance target of someone with the resources, ability, and motivation to obtain your data, it is a fait accompli.

Chapter 2: Operating System

Now that the hardware is secure against automated and pre-positioned surveillance, it is vital to prevent the introduction of software that will make the system vulnerable again.

The most important software on a computer is the operating system. This is the software that takes control of the computer as it boots up, and is the interface through which you use the computer. In short, the operating system tells the computer what to do, and how to do it. Popular operating systems include versions of Windows (e.g. XP, Vista, 8), OS X (for Mac), and Linux.

Unfortunately, we know that intelligence agencies hide 'backdoors' in popular operating systems to enable covert access to users' data.

Threats associated with operating systems:

- malware, viruses
- surveillance 'backdoors' within an operating system, accessible to the intelligence community

Two key measures are important for protection against operating system threats:

- use an open source operating system (for medium risk)
- use Tails, an amnesic, incognito operating system (for high - top risk)

Open source: freely distributed software for which the source code is publicly available. (A full, ten-point definition is available at www.opensource.org/osd).

To be sure that your operating system does not have potential surveillance 'backdoors' (i.e. that it cannot be abused for surveillance purposes), it needs to be 'open source'. 'Open source' means that the source-code, the very fabric of the operating system, is 'open' and available online for public viewing. This allows independent experts to view the source code anytime, and verify that there are no security flaws in the makeup of the operating system.

Furthermore, open source operating systems are less susceptible to malware and viruses. This is because they are much less frequently used than proprietary operating systems, and they have a correspondingly low market share.

Open source software is known as 'free software' – not only for the freedom of access to its source code, but because it is also distributed on a free/donations-only basis.

It should be noted that open source software is only as trustworthy as the trust one puts in the expertise and frequency with which the source code is examined. However, open source software is widely trusted, and is clearly a preferable option (at least for infosec purposes) to closed source software.

Any variants of operating systems by Microsoft and Apple (e.g. Windows, OS X) are wholly unsuitable if you think you, or anyone you are communicating with,

could be (or become) a target of surveillance. These systems are closed source, and are expected to contain surveillance backdoors accessible to the NSA and allied interests. Microsoft's operating systems are particularly unsuitable, since more of its code is closed source than Apple's code, and their systems are more susceptible to malware and viruses.
Note: closed source mobile operating systems, such as iOS and Android, are ubiquitous on smart phones, which are therefore indefensible against targeted attacks – see chapter 7 for mobile infosec).

Linux

Linux is the leading open source, community developed, operating system. There are many different versions of Linux operating systems that you can use.

Ubuntu
Ubuntu.com

Ubuntu is the most widely used Linux operating system. It is easy to install, highly functional, and user friendly.

You can replace your Windows operating system with Ubuntu, or you can run both Windows and Ubuntu on the same laptop (which may help familiarize users with the new system before they commit). Ubuntu is very user friendly and not too dissimilar from other operating systems, so we recommend the former - that you replace your Windows operating system with Ubuntu. This removes the Windows operating system altogether, which is essential for infosec purposes (otherwise, the potential 'backdoors' remain). Note that removing your old operating system will also remove all files associated with it – so be sure to backup any files you wish to keep that are on that laptop.

It is not recommended that you try to install Ubuntu onto Mac, as this sometimes causes problems with a Mac's functionality. As discussed in 2.1, Macs are not securable machines anyway, as Apple prevent their customers opening and modifying their hardware, so whilst handy for limited use, and indeed compatible with secure communication methods, they do have fundamental security vulnerabilities that make them ultimately unsuitable for serious infosec purposes.

It should be noted that a few elements within Ubuntu are currently closed source – it is assumed (though not definitively known) that these do not pose a security risk. However, other popular variations of Linux include Debian, and Trisquel, which are entirely open source. Note that they may be slightly less intuitive for those new to Linux to use and maintain.

Tails
tails.boum.org

Use an amnesic, incognito operating system for the greatest security: Tails

Tails stands for 'The Amnesic Incognito Live System'. It is an open source, Linux-based operating system that protects users' privacy and anonymity.

Amnesic: because no trace of your computer use is left on the system after shut down
Incognito: because it is privacy and security orientated, accessing internet anonymously by default, and thus circumventing any censorship

Tails is purposefully designed as an anti-surveillance system, and comes with several built-in (entirely open source) security-oriented applications:

Built-in online anonymity: The in-built web browser Iceweasel uses anonymous web browsing technology from Tor (see chapter 3). The browser also includes popular security extensions like HTTP Encryption and HTTPS Everywhere which encrypts your browsing data; Adblock Plus to block ads; and NoScript to block Java and Flash (as they can compromise anonymity). This does mean some web features won't work via Tails – but it is a worthwhile compromise for a incomparable privacy gain when working on sensitive projects. *Note: if you attempt to log in to an online account that is clearly linked to your person, you will compromise your anonymity for that entire session of computer use. Shutdown and restart Tails every time you're using a new contextual identity. Files and documents can also contain metadata which may indicate your location via GPS – see chapter 4 for tips on removing such metadata.*

Built-in encrypted email and chat: Tails offers in-built encrypted and private messaging. Tails includes the Claws email client with OpenPGP for email encryption (see chapter 5) and the instant messaging client Pidgin (see chapter 6) which keeps your messaging private and anonymous.

Built-in file encryption: Tails comes with LUKS, which can encrypt files. If you want to store files on the same USB stick you are running Tails from, you can create permanent storage space, or a 'persistent volume', on the USB stick (the second installation method we explain further on does this for you). Tails will encrypt the persistent volume by default, requesting your password to view or access any of the files stored

Expert info: Whilst the persistent volume is useful for storing relatively unimportant information and documents, you should not use it to store or transport the most sensitive documents. This is because the persistent volume is not 'hidden'. That is, should an adversary obtain the USB stick, they will be able to see that an encrypted volume exists on the device, and they may force or trick you into giving them the password. You should create a 'hidden' volume for the most sensitive documents (perhaps on a different USB stick), which appears to take up no memory – only you know it is there. This is done simply with an application called TrueCrypt – see chapter 4.

Built in password protection: Tails comes preloaded with KeePassX, a password manager that stores usernames and passwords in an encrypted, local

database, protected by your master password. It also comes with PWGen, a strong random password generator.

Tails is designed to be used from a USB stick independently of the computer's original operating system. This means that you can remove your laptop's hard disk drive (recommended for high risk work), and still boot up the laptop through a Tails USB stick. Alternatively, you can put a USB Tails stick into a computer with the hard disk drive intact, and boot it up via Tails – the machine can ignore the original hard disk and operating system, and run from the USB with Tails instead. Again, it is not recommended that you try to use Tails on a Mac, as Mac does not work well with non-Apple operating systems (the Mac may cease to boot, or wipe your files); and the hardware is fundamentally unsecurable (see chapter 1).

The provision of a 'mini system' on a Tails USB stick makes it ideal for sensitive journalistic projects. Your machine can essentially be 'clean' with no trace of your work on there, and your documents can be stored on the highly portable, inexpensive USB stick. Tails even comes preloaded with open source editing software such as Openoffice for creating, reading and editing documents, Gimp for editing photos, and Audacity for editing sound.

The USB stick is ideal for travelling, and you can plug it into any (non Mac) computer, if you set the computer to boot up from USB (explained within instructions below). It is wise to have separate Tails USB sticks for separate projects, to spread the risk (should you lose the USB stick) and to spread your identity trace. If appropriate, you could also give a prepared Tails USB stick to your source, with a few instructions, so they have secure means of communicating with you.

Operating Systems: Summary:

Using Ubuntu is a good option for day to day, non-sensitive work. However, it is wise to also create a Tails USB stick and switch over to Tails when working on sensitive projects – particularly when working with important documents, communicating with high risk individuals, or researching for sensitive projects online. Furthermore, taking serious infosec measures pre-emptively can prolong your anonymity and thus the time you, and most importantly your source, have before you become targeted for surveillance.

You have now learnt how to robustly protect your system. However, if you feel attached to a Windows system, or a Mac, you should still read on and employ the strategies described in following sections to protect your communications, anonymise your browsing data, and encrypt and transport sensitive documents. Applications that encrypt your email and chat, for example, are excellent anti-surveillance tools, even on a Windows or Mac system. However – if you become a surveillance target by someone with the resources, ability, and motivation to obtain that data, consider it a fait accompli, as Windows and Mac systems are fundamentally vulnerable to surveillance.

Step-by-step instructions

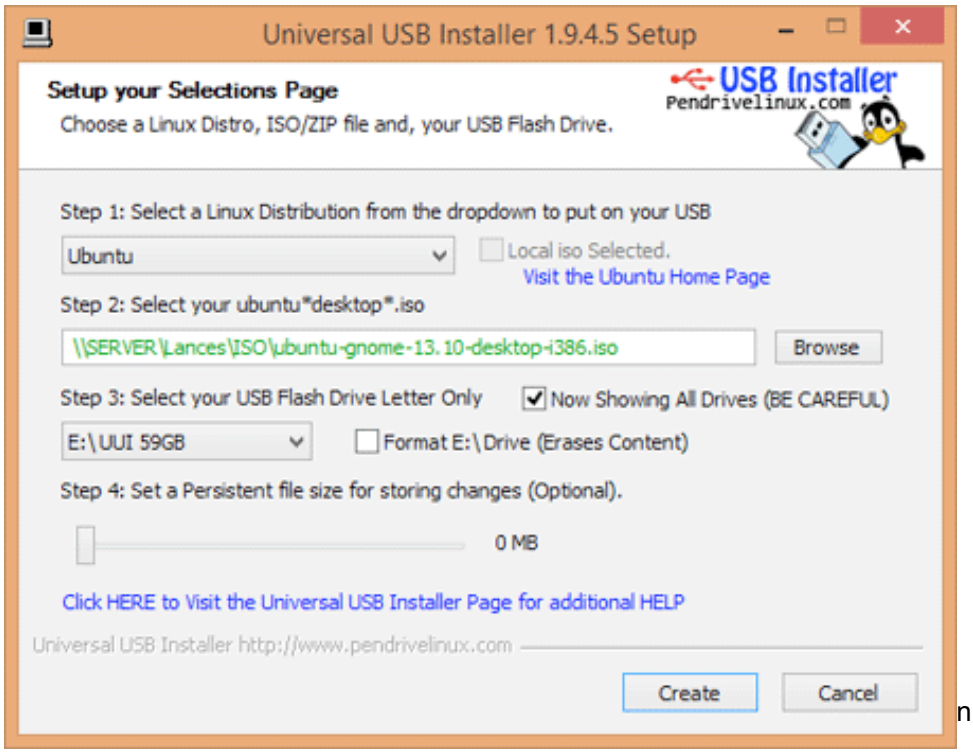
Ubuntu

Note: all Windows documents, programs, files, etc will be deleted if you replace Windows with Ubuntu (recommended).

1. **Download Ubuntu**
   Go to http://www.ubuntu.com/download/desktop and download Ubuntu.
   You will need to know how much RAM your laptop has, and download either 32-bit (for older machines, such as the recommended Thinkpads, with 2GB or less RAM) or 64-bit (for newer machines with 4GB or more RAM). The download may take 20-60 minutes.

2. **Download Linux's USB Installer**
   Go to http://www.ubuntu.com/download/desktop/create-a-usb-stick-on-windows and click "Download Pen Drive Linux's USB Installer ›". This will download the USB installer, allowing you to store Ubuntu on a USB drive, from which you will use to install Ubuntu.
   Expert info: During the OS installation, the hard disk cannot run any other software – so you need another source, in this case a USB stick, to run the install software.

3. **Put Ubuntu on the USB Installer**
   When both downloads are complete, insert a clean USB stick and open the USB Installer.
   Select the Linux Distribution from the dropdown menu (Ubuntu); use the 'Browse' button to locate the Ubuntu downloads; and select the USB Flash Drive Letter (where the computer has located your USB stick). Click 'Create'.



When this is complete, safely remove the USB stick, and shut down the computer.

4. **Install Ubuntu**
   Insert the USB to the laptop, and press the Power button to turn the machine on. Hold down the Enter key during bootup, to reach the BIOS setup utility. Go to 'Startup' > 'Boot', and make sure your USB stick is top of the priority order (if an item on the list has a '+' it means it has a submenu, where your USB listing may be hiding!).

   You may be prompted to set up WiFi, but you don't have to worry about setting up WiFi now, especially if you have removed your WiFi card.

   Under 'Installation type':
   - Select: Replace Windows with Ubuntu
   - Select: Encrypt the new Ubuntu installation for security
   - Select: Use LVM with the new Ubuntu installation

   Choose a strong password (see chapter 8 for guidance).

   The software will ask you to register your name (but you don't have to enter anything here). Pick a computer name and username for your log-in. Choose a strong password, and tick "require my password to log in" and "encrypt my home folder".

   Ubuntu will now install. Once installed, turn off the laptop and remove the USB. Turn the laptop on and Ubuntu should launch!

   When you connect to the internet, go to top left Ubuntu icon on the desktop and search 'updates'. Click to accept any updates.

Ubuntu privacy tweaks

- Select 'System Settings' on the desktop > Security and Privacy
- Under 'Files and Applications' you can control whether records are kept of your file and applications usage.
- Under 'Search' you can disable online search results when searching in the Dash. This stops Ubuntu's Amazon integration, and prevents your Dash searches being sent back to Ubuntu servers and Amazon. You may as well right-click the Amazon icon on the desktop and select 'Unlock from Launcher' to remove it from the desktop.
- Under 'Diagnostics' you can opt out of sending 'error reports' and 'occasional system information' to Canonical.

Tails

There are three ways we recommend installing Tails:

1. Via a pre-installed/cloned Tails USB stick gifted from a trusted friend (contact infosec@tcij.org if you require help finding a cloned Tails stick)

2. Manually via Unetbootin (which allows you to create a persistent volume on the USB stick)
3. Manually via your Linux system (which does not allow you to create a persistent volume on the USB stick)

We highly recommend starting with Tails via a pre-installed/cloned USB stick. Manual installation is not very easy, and as such does not have a perfect success rate.

We would also recommend installing Tails in a way by which you can create a persistent volume (hence easily access the same email address, instant messaging address, and documents for each install). This means method two is preferable to method three.

Instructions for installation methods 2 and 3 follow.

You will need:

1. A **clean** USB stick (explained next) which is 4GB or bigger (ideally 16GB if you intend on storing documents on it too)
2. The latest download of Tails
    a. Open the Tor browser. Go to https://tails.boum.org/download/ , click on "2. Download the ISO image", and under Direct Download, Latest Release, select 'Tails I.0 ISO image'. Save the file on the laptop you wish to use Tails on.

Clean and prepare the USB stick

Perhaps you have used this USB stick before, or perhaps it came with pre-installed software. Either way, opening the USB drive on a computer and moving the files to Trash only stops them being visibly listed, and does not really 'delete' them. For your new Tails USB stick, you want to start with a totally clean device.

We also need to change some settings on the USB stick, so that it is prepared to boot up the computer and can host Tails.

1. **Install GParted**
   Go to the Ubuntu Software Center on your computer, and search for 'Gparted'. Install.
2. Insert your USB stick into the laptop.
3. Open GParted. Go to GParted > Refresh Devices
4. Your USB should appear as a drive in the top right drop down menu (e.g. listed as /dev/sdb or dev/sdc) and will display the size of the USB stick)
5. Now at the top of the box is a long green rectangle, outlined green, possibly with some space on the left of the rectangle shaded yellow. Right click, select 'unmount', and then 'delete'.
6. Any colours in the rectangle are now gone and replaced by grey. Right click, and select 'New'.
7. A screen titled 'Create new Partition' appears. Under 'File System' select 'fat32', and under 'Label' type 'TAILS'. Click 'Add'.

fat32 = File Allocation Table 32 bits

8. Click the green 'tick' (just under the 'Partition' option on the menu)
9. In the pop up box, select 'Apply' to apply operations to device, and 'Close' when the message appears: "All operations successfully completed".
10. Now, right click on the long green rectangle and click "Manage Flags" > select 'boot', and close.

This will tell the computer that this is a drive that can be used to start the system from.

You can safely remove the USB stick – it is ready for Tails!

2. ***Installing Tails Manually via Unetbootin (allows persistent volume)***

1. **Download Unebootin**
   Download Unetbootin 494 for Linux here: .
   http://sourceforge.net/projects/unetbootin/files/UNetbootin/494/
   When the Download is complete, right click the Unetbootin file and select 'Properties' > Permissions tab > tick the box next to 'Execute' to 'Allow executing file as program'

2. **Launch Unetbootin**
   Open the 'Terminal' (use the Ubuntu search tool, the top left icon on the screen, if you cannot find the Terminal). It is a black box with a command prompt saying: user@<name of your computer>: $

- Type:

  ```
  cd Downloads
  ```

  (assuming Tails and unetbootin are in Downloads) and press Enter.
  Note: commands are sensitive: be sure to leave a space after 'cd' and that the D on Downloads is a capital.

- Type `sudo ./` followed by the file name of your Unetbootin download. So it will likely be:

  ```
  sudo ./unetbootin-linux-494
  ```

  and press enter (be sure to leave a space after 'sudo').
  You may be prompted for your password – enter it (your password-typing may not be visible in the terminal, but type it in anyway and press enter).

  Unetbootin should launch.

3. **Do the copy**
   Plug in the prepared USB stick. In Unetbootin, select the round button to the left of 'Diskimage'. Open the search box by clicking the ellipsis (…) . Open Downloads (assuming that is where your Tails download is saved), and select the Tails .iso file. Under 'Type' select 'USB drive', and under

'Drive', select the USB device name (it is probably /dev/sdc, or similar, but it is very important that you get this right). If nothing shows under 'Drive', wait a moment, or try ticking and unticking the 'show all drives' box. Press OK.
Exit UNetbootin rather than reboot, and close the Terminal too. Safely remove the USB and shutdown.

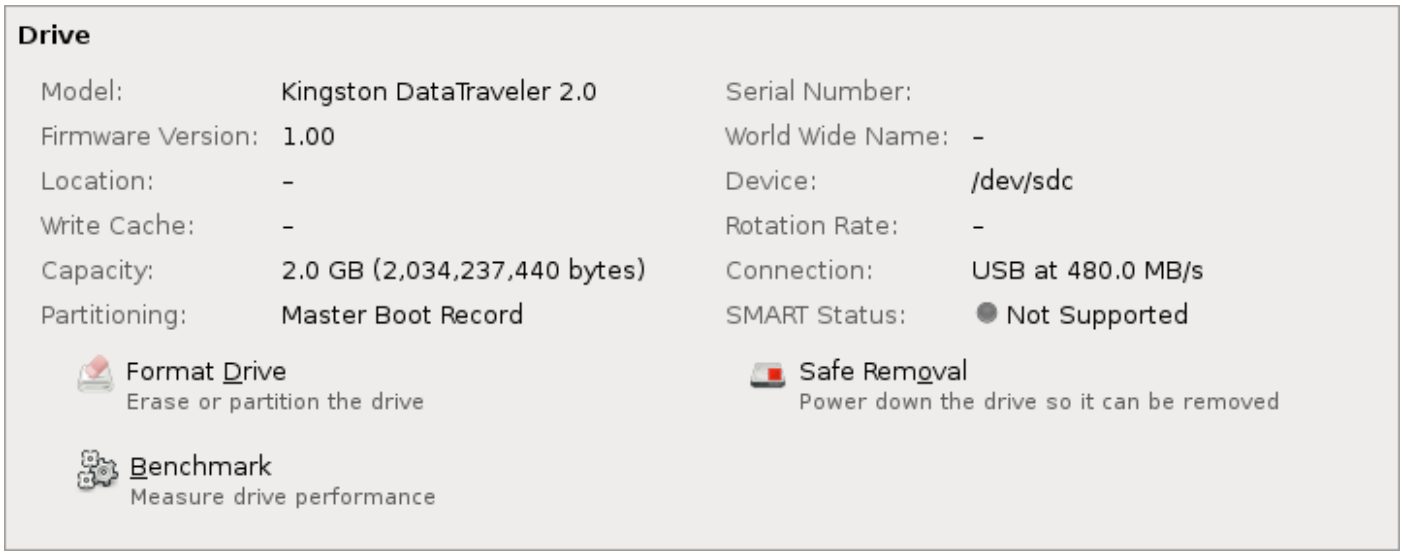
You're done! You can now start Tails from your USB stick.

Put the USB stick in the laptop and then start the laptop - it should begin with Tails.

Alternatively it may go to a blue screen menu – use the arrow keys to select Live and press Enter to boot up (or if that doesn't work, select 'Live failsafe' and press Enter).

3. ***Installing Tails Manually via your Linux system (does not allow persistent volume):***
See also:
https://tails.boum.org/doc/first_steps/installation/manual/linux/index.en.html
To install Tails manually via your Windows system see here:
https://tails.boum.org/doc/first_steps/installation/manual/windows/index.en.html

1. **Find out the device name of the USB stick**
   The 'device name' refers to how your computer has identified the USB drive, and should be something like /dev/sdb, /dev/sdc1, etc. If you are not sure about the exact device name, do the following:
   1. Make sure that the USB stick onto which you want to install Tails is unplugged.
   2. Open GNOME Disk Utility from the menu Applications ▸ System Tools ▸ Disk Utility (use Ubuntu's search function, the top left icon, to search for 'GNOME' if you cannot find it)
   3. 'Disk Utility' lists all the current storage devices in the left pane of the window.
   4. Insert the USB stick onto which you want to install Tails. A new device appears in the list of storage devices. Click on it.
   5. In the right pane of the window, verify that the device corresponds to your device, its brand, its size, etc.



On this screenshot, the USB stick is a Kingston DataTraveler of 2.0 GB and its device name is /dev/sdc. Yours will be different.

If you are having any trouble finding or using GNOME, search online (ideally via Tor) for solutions to your problem, including the type of operating system you are using.

If you are still unsure about the device name, you should stop proceeding or you risk overwriting any hard drive on the system.

2. **Locate Tails**
   Find the Tails download, right click, and select properties. You should see the file location (e.g. /home/amnesia/Desktop/tails-0.6.2.iso) – keep a note of this.

3. **Plug in the USB stick**

4. **Install isohybrid**
   If you are using Ubuntu, the 'isohybrid' utility should be included in your package. To check, or indeed install it, open the 'Terminal' (use the Ubuntu search tool, the top left icon on the screen, if you cannot find the Terminal). It is a black box with a command prompt saying: user@<name of your computer>: $
   Type the following very carefully into the Terminal, before pressing Enter:

   ```
   sudo apt-get install syslinux
   ```

   Note: Terminal commands, such as the one above are case sensitive, and must be typed exactly.

5. **Do the copy**

In the Terminal, type the following command, replacing [tails.iso] with the Tails location you found in step 2, and replacing [device] with the device name of the USB stick that you found in step 1.

```
isohybrid [tails.iso] --entry 4 --type 0x1c dd if=[tails.iso]
of=[device] bs=16M
```

Here is an example of the commands to execute (the bold type signifies the sections that will be different for you).

```
isohybrid /home/amnesia/Desktop/tails-0.6.2.iso --entry 4
--type 0x1c dd  if=/home/amnesia/Desktop/tails-0.6.2.iso
of=/dev/sdc bs=16M
```

If you don't see an error message, Tails is being copied onto the device. The whole process might take some time, generally a few minutes. Once the command prompt reappears, you can shutdown your computer, and start Tails from this new device.

Troubleshooting

dd: /dev/sdx: No such file or directory
Double-check the name of the device you found in step 1. If you are not sure about the path to your Tails download or if you get a No such file or directory error message, you can first type dd, followed by a space, and then drag and drop the icon of the Tails download from the file browser onto the Terminal. This should insert the correct path to the Tails download in the Terminal. Then complete the command and execute it.

dd: /dev/sdx: Permission denied
You might have committed a mistake in the device name, so please double-check it. If you are sure about the device name, this could be a permission problem and you could need to gain administration privileges before running the commands in the terminal.

dd: tails.iso: No such file or directory
You might have committed a mistake on the path to the Tails download in step 2.

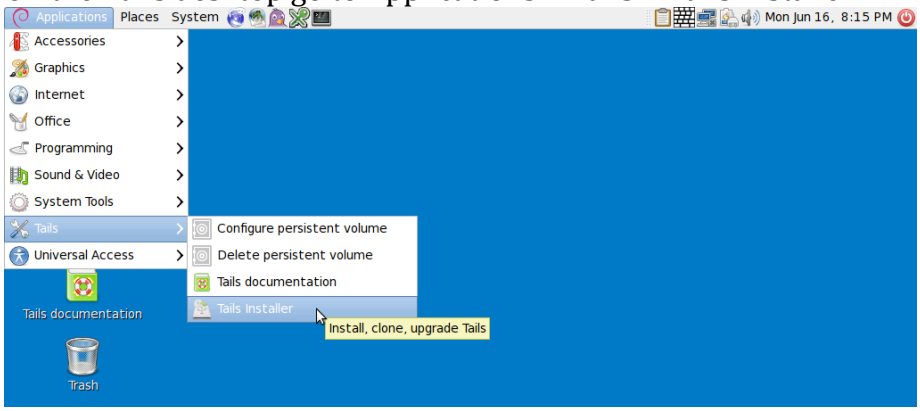
Clone a USB stick for a source

You can use your Tails USB stick to create a new Tails USB stick – this can be particularly useful for equipping sources and colleagues.

1. Start the Tails system and login with password (giving administrative options).
2. Make sure your Tails installation is updated and perform an update if needed (restart afterward to make sure update takes effect).
3. Insert a clean USB-drive into one of the free USB-ports on the computer. This drive needs to be 4 GB minimum to contain a Tails installation, but

ideally 8GB or more.

4. On the Tails desktop go to Applications > Tails > Tails Installer.



5. A new window will open. Select: Clone & Install

6. The Tails Installer window should list your clean USB stick. Click 'Install Tails' on the bottom of the window and click 'Yes' on the pop-up window to confirm your device selection. A clone of your Tails installation will now be made to the other USB-drive.
   When done the Tails Installer will tell you: Installation complete!
7. When completed shutdown the system and try to start from the newly created drive to make sure it works properly.

Using Tails for the first time

When you use Tails for the first time, you will see a screen load up with options 'Live' and 'Live failsafe'. You can hit Enter to choose Live immediately if you like, or it will be chosen automatically after 5 seconds.

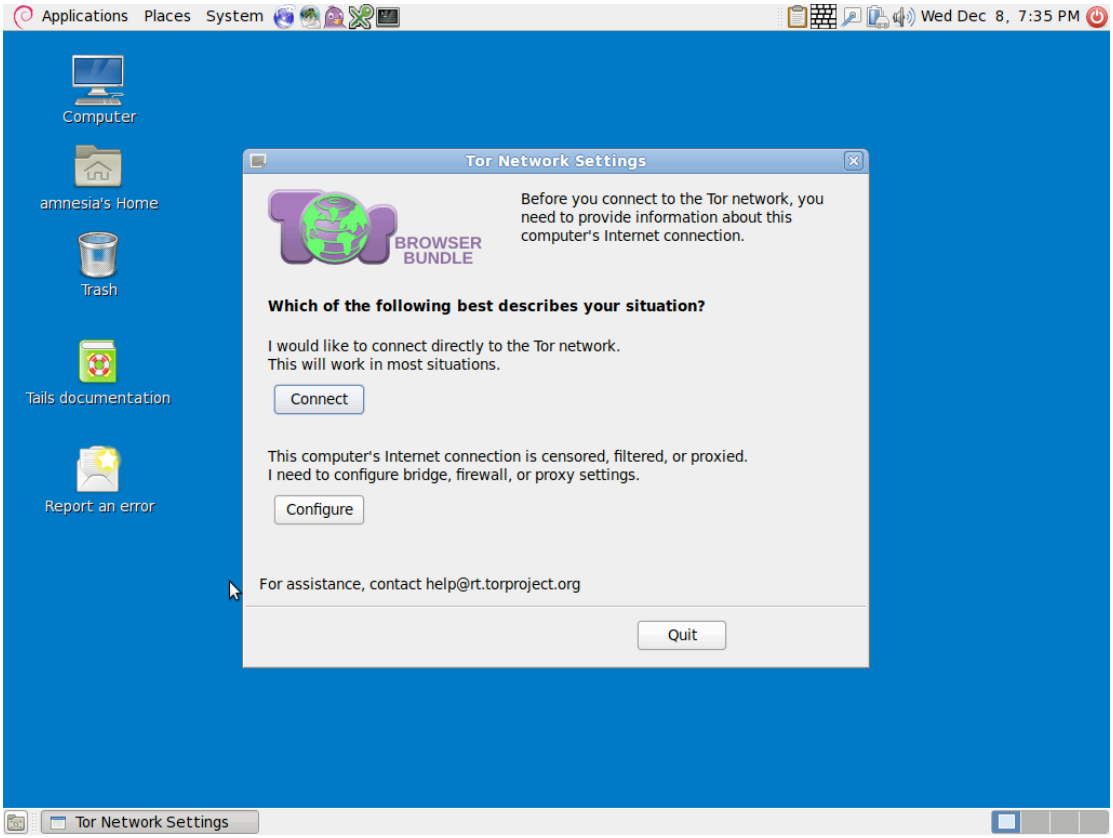
When you boot up via a Tails stick for the first time, you will be asked one question: 'More options?'. It is not essential that you enter this menu, unless you need to configure Tails to circumvent Tor censorship. Otherwise you can select no and 'Login'.
If you do select yes for more options, you will see:

- '*Administrative password*'. It is unlikely you would need to create one unless you want to access the internal hard disk of the computer (which is not recommended, and can lead to unnecessary security risks).
- '*Windows camouflage*'. If you activate '*Microsoft Windows XP camouflage*', Tails looks more like Windows XP. This may be useful in public places if you think the Tails OS may be recognised or attract suspicion.
- '*Spoof all MAC addresses*', which should be automatically selected. This is a good option to hide the serial numbers of your network cards, and thus is another function which helps to hide your location.
- '*Network configuration*', under which you have two options: *connect directly to the Tor network*, or '*This computer's internet connection is censored, filtered or proxied. I need to configure bridge, firewall or proxy settings*'.

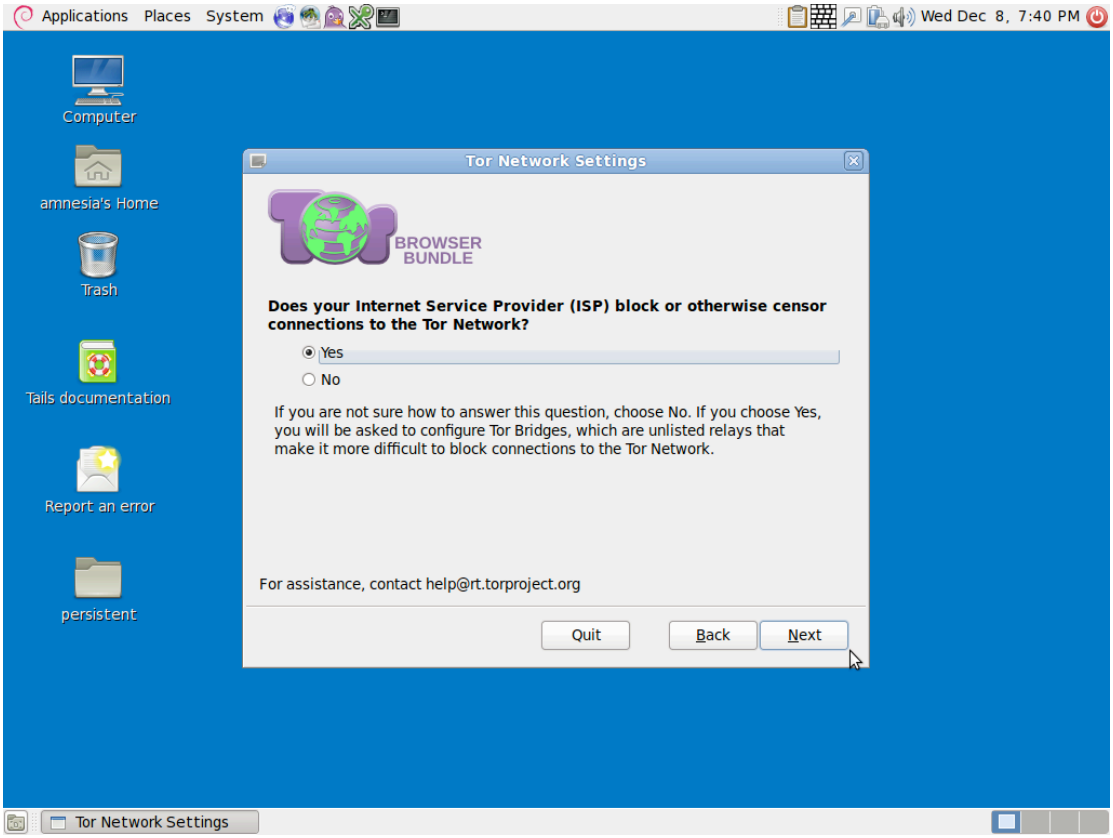
Using Tails via bridges/circumventing censorship
Bridges are Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that help circumvent censorship.

When you boot up using the Tails USB stick and are offered 'More options?', select 'Yes' and continue.

Under '*Network configuration*', select '*This computer's internet connection is censored, filtered of proxied. I need to configure bridge, firewall or proxy settings*'. Then, when you connect to the internet the Tor browser bundle window will appear asking the same question.



If the latter option applies, click 'Configure'. You'll be asked if you need to *use a proxy to access the internet* – select 'No'; then if your computer's *internet connection goes through a firewall that only allows connections to certain ports* – select 'No'; then, if your *ISP blocks / censors connections to the Tor network*. If you need to configure bridges, select 'yes' here and press next.



You now have a box to enter one or more 'bridges', strings of numbers that identify a Tor relay. To get bridges, go to https://bridges.torproject.org or if you cannot access that site, send an email to bridges@torproject.org , from a gmail.com or yahoo.com email address, with the line 'get bridges' by itself in the body of the message, and some should be sent back to you. Using a bridge can be an extremely slow way of connecting to the internet – but if you need it to circumvent censorship, it works very well.

Creating a persistent volume in Tails
Creating persistent storage space on your Tails USB stick.

To create a persistent volume in Tails, go to the swirl icon in the top left hand corner of the screen > Tails > Configure persistent volume. Once you have entered a (very strong, see chapter 8) password, you can choose what types of files you will save in the persistent volume. You can select all of these, to keep your options open.

Now, every time you boot up with the Tails USB stick, you wil be asked two questions: 'Use persistence?' and 'More options?' (as before). If you click 'Yes' to 'use persistence' and enter the password, you can access any data (e.g. configured email client, IM client, password manager, or files) you have stored in previous sessions.

Using KeePassX
KeePassX is a password manager that stores usernames and passwords in an encrypted, local database, protected by a master password. It also comes with PWGen, a strong random password generator.

To create a new password database:
File > new database
Groups > new groups (e.g. 'Jabber' group, for your Jabber usernames and passwords)

To add a new password:
Click on a group > Entries > Add new entry. Here you have the option of entering a password, or generating a random one. If you click on the eye icon, you can see the text of the password – otherwise, it will remain obscured.

To retrieve a password:
When you have added a password to a group, you can right click on the desired password and select 'copy password to clipboard'. You can then paste it in to a log-in form.

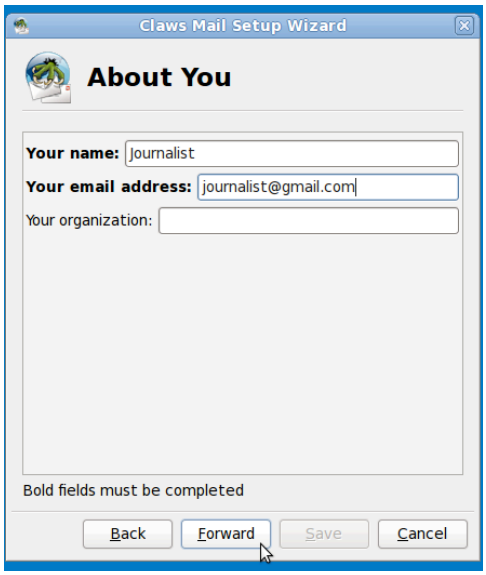
Email in Tails
You should read chapter 5 on email encryption before continuing to read the rest of this chapter.

Claws

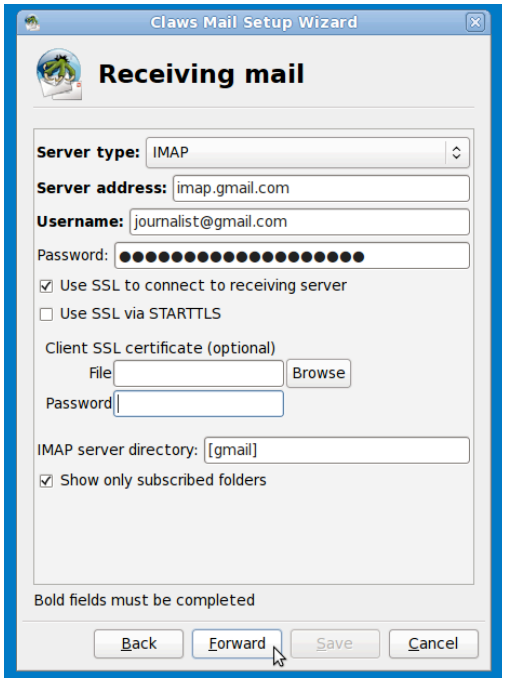
Tails comes with a pre-installed desktop email client, Claws. You can use this to configure your email account with a GPG plug-in to send encrypted mail, in much the same way that you can configure Thunderbird on your regular operating system (see chapter 5).

Configure your email account with Claws

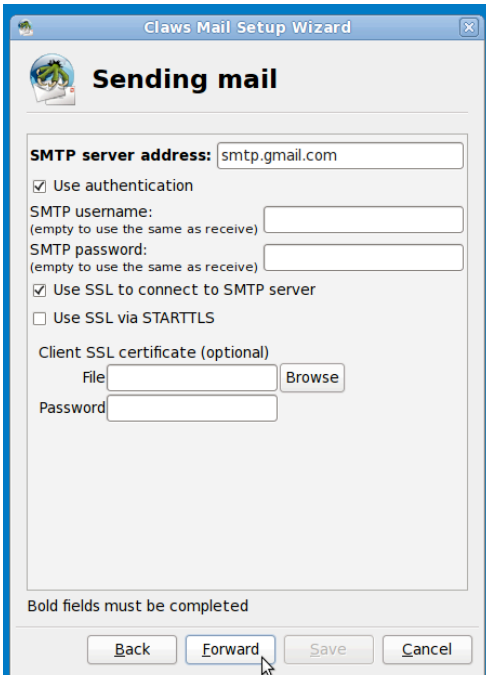
1. Enter your name (if you wish) and email address



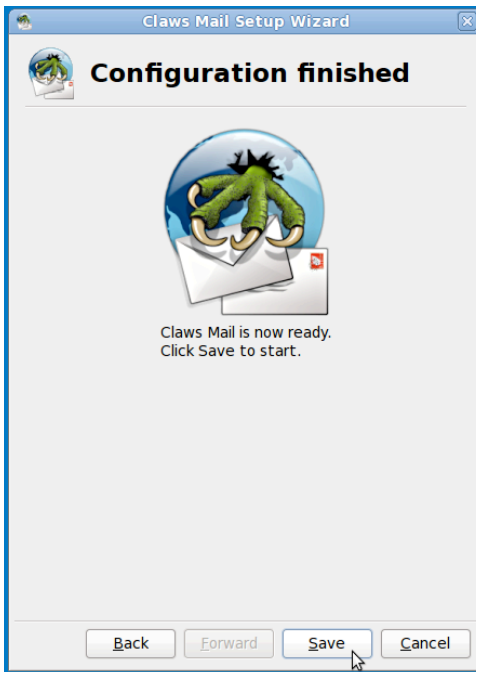
2. Receiving mail
   For receiving mail, the server type should be IMAP.
   You will need to search online for the correct IMAP server address for your particular email provider.
   Under 'username' type your whole email address.
   Enter the account password.
   The 'IMAP server directory' is optional and can be left blank.



3. Sending mail
   You will also need to search online for the correct SMTP server address for your particular email provider, and enter it here.



4. Configuration finished!



Now you can open Claws, configure encryption, cut a keypair and change your settings.

Configure Claws for encryption

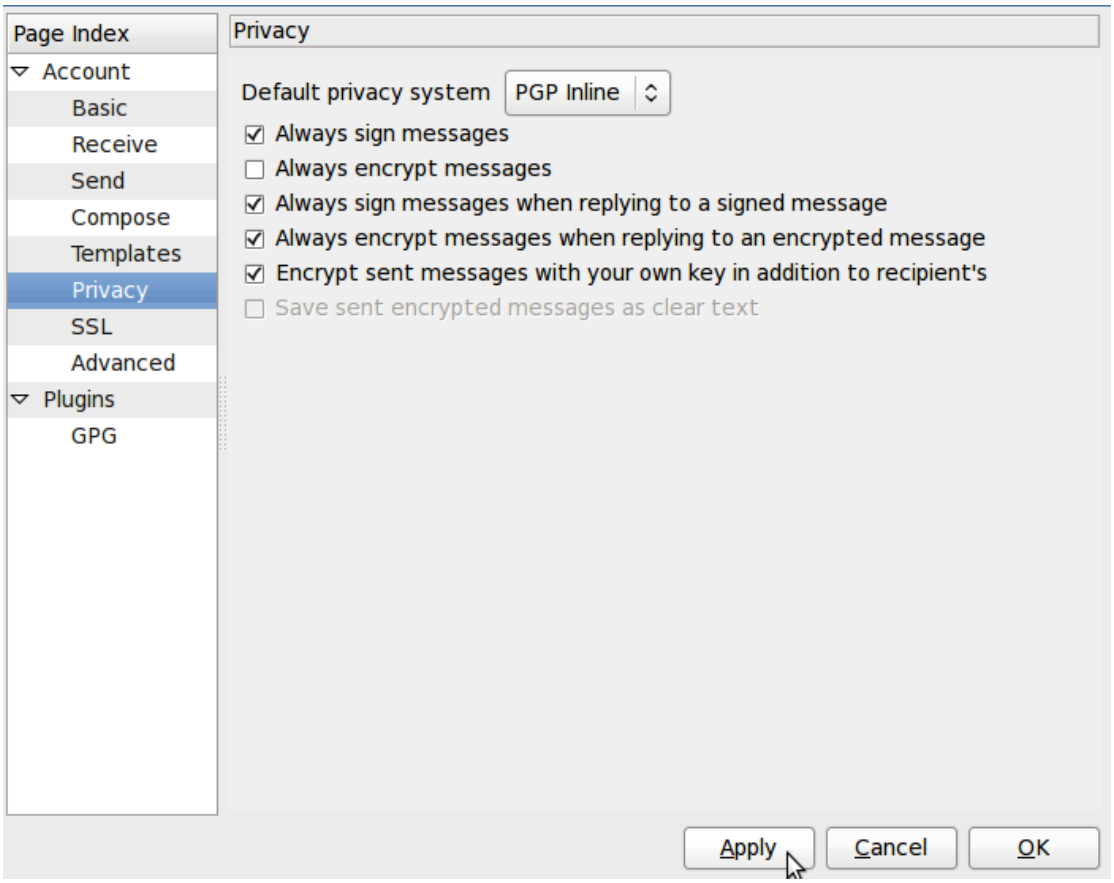
Claws should be already have plugins installed for encryption, but to check:
In Claws, go to Configuration > Plugins > PGPcore > Load
A new window appears, "Select the plugins to load": select both PGPcore and PGPinline, and click Open.

In Claws, go to Configuration > Preferences for current account > GPG (under Plugins).

- Choose 'Select key by your email address'.
- If you haven't yet created a key pair for the email address, click 'Generate a new key pair'.
    - You will be asked to enter the passphrase for the email account (twice) and then the key will begin to generate
    - Move your mouse around the screen as your new key pair is generated to aid randomisation.
    - Once completed, a window will pop up saying 'Key generated' and asking 'Do you want to export it to a key server?'. If you do want the key to be publicly accessible (like listing your number in a phone book), so people can find your key and send you encrypted emails, select Yes.

Check your encryption and signing options.
In Claws, go to Configuration > Preferences for current account > Privacy (in the menu in the left hand side).

- Set the 'Default privacy system' to 'PGP Inline'
- You may want to tick "Always sign messages'.
- You should also tick 'Encrypt sent messages with your own key in addition to recipient's' so you can decrypt and read your sent messages.
- When you have made your selections, click 'Apply'.



All other default general settings in Claws should be fine. You may wish to change how often Claws searches for new received messages. You do so here by going to:
Configuration > Preferences > Mail handling > Receiving.

Other ways to encrypt emails on Tails - OpenPGP encryption applet

Because *all* internet connections on Tails run through the Tor network, connections to your email provider via your email client will also be run through Tor. Users of some email providers sometimes have problems configuring their email accounts with Claws through Tails, because the connection is re-routed through the Tor network to disguise your location.

Tails offers an alternative method to encrypt email and email attachments. Rather than using an email client to encrypt the entire email, you can highlight

text and encrypt it to the desired recipient's key, before pasting it into an email (e.g. when composing an email on the web browser).

Import contact's public key

Go to the OpenPGP encryption applet (the clipboard icon in the top right of the toolbar) > Manage keys > then either

> Remote > Find remote keys. Enter the contact's name, and click search.
> Or
> File > Import (if you have the key saved in a file – e.g. if you have the key on a USB, or if your contact has their key saved on a website, you can save the text as an .asc file and then import).

Encrypt the text

Applications (left on the top toolbar) > Accessories > gedit Text Editor. Type your message. Then select (Ctrl + A) and copy (Ctrl + C) the message. Go to the OpenPGP encryption applet > Sign/encrypt Clipboard with Public Keys > select the recipient of your email (you need to have already imported their key), sign the message as the email address from which you will be sending the email, and click OK. Then paste the message (Ctrl + V) into the composing window in your email account, and send.

Note that you have encrypted the message to only allow decryption by the desired recipient. This means that once encrypted, you cannot decrypt it to read it yourself. Therefore, if you use this method, it is a good idea to select your own public key, as well as that of the recipient of the email, when you encrypt the message. You will then be able to decrypt it if you want to read your sent messages.

Encrypting email attachments

It is easy to encrypt files using public keys, to send as email attachments, with Tails. Right click the desired file > Encrypt > tick the recipient's email address (sign the message as the address from which you will send the email) > OK. You will now see a duplicate of the selected file, with the '.pgp' extension – this means it is an encrypted file. Attach the .pgp file to your email, and it can only be decrypted and opened by your chosen recipient.

Chapter 3: Safe Browsing

Web browsing risks:

- Being blocked from accessing certain sites
- Being blocked from using anonymous browsers
- Data collection of your identity
- Data collection of your browsing behaviours – the pages you have visited, and when
- Data collection of your passwords and autofill information
- Data collection of your location (and previous locations)
- Man-in-the-middle attacks, often for the purpose of malware (surveillance) injections

Infosec action:

- Use a general purpose browser, with privacy-enhancing extensions, for daily activities
- Use the Tor browser for anonymous browsing, for censorship resistance, and to hide your real location

A web browser is the software you use to access the World Wide Web. For many of us, web-browsing *is* 'The Internet', and in many senses it is a window to the world. Because of the huge opportunities in web browsing, some states impose restrictions on access to certain websites, which can be very debilitating for people's freedom, and of course a problem for local journalists, researchers, and foreign correspondents.

Whilst web access is largely unrestricted in the West, we have serious privacy issues with our web browsing. It remains that most browsers collect vast amounts of data about their users, which are often made available for marketing, intelligence agencies, and other nefarious purposes.
This chapter gives a range of options to minimize the impositions on freedom and privacy in web browsing, under a range of circumstances.

What browsers to use

Many people are unaware of the privacy issues with browsers, and use whatever browser is already on the system as they take it out of the box. In practice, this means Safari on Macs and Internet Explorer on Windows systems. Both of these are insecure in terms of privacy and data protection. There are several alternatives that are more integrally secure, and that can be vastly improved by further adding 'extensions' – extra software that improves the functionality of your browser.

While there are dozens of browsers with specialised purposes, this chapter recommends three open source browsers:

- Firefox as a general purpose web browser for Linux and Windows
- Chromium as a general purpose web browser for Mac
- Tor, as a secure browser that anonymises your location and identity, and

overcomes web censorship (suitable for Linux, Windows and Mac).

Expert info: The reason we recommend Firefox for Linux and Windows but not Mac, is that Firefox sometimes conflicts and does not work with Tor on a Mac (because Firefox and Tor are based on the same code).

A general purpose browser

Your daily web browsing centres around generally unrestricted sites and sites that you log in to, such as social media platforms, LinkedIn, newspapers, YouTube, shops, and so on. It doesn't make sense to use Tor for sites you are logging into with your real identity, unless your primary concern is to shield your real location (in which case you should make sure all the other software on your computer, such as your email client, App store or software centre, etc., are blocked from going online – or more realistically, use the Tails operating system).

Firefox
A popular open source web-browser

For Windows, download Firefox for your operating system and language at www.getfirefox.com.
On Linux distributions/Ubuntu, Firefox should already be installed.

Chromium
An open source clone of Google Chrome

Download Chromium for Mac at
http://www.macupdate.com/app/mac/36244/chromium (or go to www.macupdate.com and search for Chromium)

Extensions

A general purpose browser is certain to make your identity and location available. However, there are some extensions we can use to prevent it from:

- tracking your browsing behaviours
- saving and leaking your passwords and autofill information
- allowing man-in-the-middle attacks and malware injections

You can find a range of privacy enhancing extensions at https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/ , which should be suitable for both Firefox and Chromium.

We particularly recommend the following open source extensions:

HTTPS everywhere: forces all connections between your web browser and the webserver you are visiting to encrypt the connections. This is a useful defence against man-in-the-middle attacks.
https://www.eff.org/https-everywhere

NoScript: blocks JavaScript. JavaScript is an essential element of many websites, but can be exploited by adversaries to track your browsing behaviour, leak your passwords, and to inject malware. NoScript is very effective but you will need to grant or deny privileges on a per website basis depending on how much you trust them, as JavaScript is essential for many sites' functionality.
https://noscript.net/

Ghostery: blocks a wide range of trackers in its database, which track your browsing behaviour. Do make sure to switch off 'GhostRank' under Settings > Options, as this itself reports back data for marketing purposes.
https://ghostery.com

Web Of Trust: is a database of website rankings. It will tell you if a website is considered (un)trustworthy by many other web users.
https://www.mywot.com/

Lastpass: is a password generator and manager for Firefox.
https://lastpass.com/

Tor
https://www.torproject.org/

About Tor

The Tor browser was especially designed for anonymity by routing all its traffic through the Tor ('The Onion Router') network.

This is a global network of computers called Tor nodes that have encrypted connections with each other. When the Tor browser starts it will connect to one of these nodes. This node will connect to a second node that will in turn connect to a third node. All these nodes can be anywhere in the world and the first and third node will not be aware of each other. The third node will connect to the wider internet and fetch webpages from the sites you're visiting. Those sites will not be able to see where you are or who you are (as long as you do not identify yourself by logging into services associated with your real identity).

Since the Tor browser runs all its traffic trough several other places around the world it is slower than 'normal' browsing but this is a price well worth paying for being online anonymously.

In order to ensure the safety of the browser, Tor automatically enables HTTPS-Everywhere, and automatically avoids extensions such as Flash, Realplayer, Quicktime. Because of this, and the speed-limitations, services such as YouTube will not work on the Tor-browser – you will use your general purpose browser for that.

Overcoming restrictions

If the network provider you are using (this may be the entire country or just a University network) blocks access to the Tor network, you can use 'bridges' to achieve access.

Bridges are Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that help circumvent censorship.

Launch the Tor Browser Bundle. In the Vidalia Control Panel, go to Settings > Network > tick 'My ISP blocks connections to the Tor network'.

You now have a box to enter one or more 'bridges', strings of numbers that identify a Tor relay. To get bridges, go to https://bridges.torproject.org or if you cannot access that site, send an email to bridges@torproject.org , from a gmail.com or yahoo.com email address, with the line 'get bridges' by itself in the body of the message, and bridges should be sent back to you. Using a bridge can be an extremely slow way of connecting to the internet – but if you need it to circumvent censorship, it works very well.

Warnings

Don't open documents (such as .doc and .pdf) downloaded via Tor while still being online. These document formats can contain elements that independently connect to the internet, thereby revealing your real IP-address. Make sure you are offline first or use a separate computer for working with such documents.

Don't run bittorrent over Tor since this may betray your real IP-address and will consume disproportionate amounts of capacity on the TOR-network.

Install Tor
Every time Tor starts it will check if there is an update available – you should upgrade immediately when notified of any updates.

Mac, Windows:
Download and install the Tor browser for your operating system at https://www.torproject.org/ following the installation instructions on the site.

Linux/Ubuntu:

1. Download and Tor browser for Linux at https://www.torproject.org/
   To complete the install, you need to
2. Save the download (note whether you were guided to a 32 or 64-bit version; 32-bit suits older machines, and 64-bit suits newer machines).
3. Open the 'Terminal' (use the Ubuntu search tool, the top left icon on the screen, if you cannot find the Terminal). It is a black box with a command prompt saying: user@<name of your computer>: $
   In the Terminal, run one of the following two commands to extract the package archive:

`tar -xvJf tor-browser-linux32-3.6.2_`***`LANG`***`.tar.xz`
(substitute LANG for the language listed in the filename).
Or
`tar -xvJf tor-browser-linux64-3.6.2_`***`LANG`***`.tar.xz` (for the 64-bit version,):

4. Once that's done, switch to the Tor browser directory by running:
`cd tor-browser_`***`LANG`*** *(where LANG is the language listed in the filename).*

To launch the Tor browser on a Linux OS, at any time, you must use the following command in the Terminal:

```
./start-tor-browser
```

This will launch Tor Launcher and once that connects to Tor, it will launch Firefox.
Unfortunately, there is no Tor launcher for your desktop. Every time you wish to use Tor, you must use this command in the Terminal.

Chapter 4: Data

Risks:
- Loss
- Corruption
- Interception
- Theft
- 'Deleted' data recoverability
- De-anonymising/compromising metadata

Infosec actions:
- Backup data
- Encrypt data
- Securely share files
- Securely delete data
- Delete metadata

When storing or transporting data there are several types of risks that require attention: interception/theft, loss, corruption and incrimination. The difference between interception and theft is detectability for the original owner. Interception will usually mean a copy has been made while theft would suggest the taking of the storage device (laptop, USB-drive or hard-disk) containing the data. The latter case would be detectable, whereas the former might not be.

If sensitive data falls into the hands of adversaries, there may be severe consequences for sources or the journalist.

To protect digital files there are several options. Simply storing the material on a small device (USB-drive, memory-card or external hard disk) and hiding it may be effective in certain cases. In such a scenario the entire security of the material is dependent on the hidden device not being found.

To protect your data from unauthorised access, it is important to encrypt it. TrueCrypt is an easy-to-use tool for encrypting files and entire disks, and can even hide their very existence from adversaries.

TrueCrypt
TrueCrypt is open source encryption software.
Download: https://truecrypt.ch/

In June 2014 the website of TrueCrypt was suddenly changed – it stated the product was no longer safe to use and advised people to switch to Microsoft's Bitlocker (which only runs on MS-Windows, a known insecure platform). All previous versions of the software were removed and replaced by a new version, 7.2, that can only decrypt existing TrueCrypt files.

Discussion on what actually happened, who made the changes to the website and why, continue but among most experts the consensus is that the previous version of TrueCrypt (now online at the new site https://truecrypt.ch/) is trustworthy. If, as

some people speculate, TrueCrypt had a NSA backdoor built into it then why do anything to cast doubt upon it? An untrustworthy system with a backdoor being used by many people is after all a spy's dream.

With Truecrypt, an encrypted 'container' can be made that can act as a digital strongbox for files locked by a password. Once this box is created and filled with files it can be moved to an external storage device such as a USB-drive, or indeed sent over the internet to others. Even if the file is intercepted, the strongbox will not reveal its contents to anyone who does not have the password (for choosing a good password see chapter 8).
Important! Do not forget your password, there is no other way to get to your data once it is encrypted. Losing you password means losing your data!

Encrypt a file with TrueCrypt

1. **Download**
   Download TrueCrypt from truecrypt.ch and install on your system like any other application.
   TrueCrypt works the same on Windows, Mac and Linux systems and the encrypted containers are cross-compatible between these systems. This allows you to work securely with other people without having to know what system they use.

2. **Create an encrypted volume**
   To create an encrypted 'volume' (like a folder) start the program and click:

- 'Create Volume' > 'Create an encrypted container' > select 'Standard TrueCrypt volume' > select the location where the container will be stored on your computer (it can be moved later) and give the container an (innocuous) name.
  To encrypt an entire external hard drive such as a USB stick, select 'Create Volume' > Create a volume within a partition/drive'

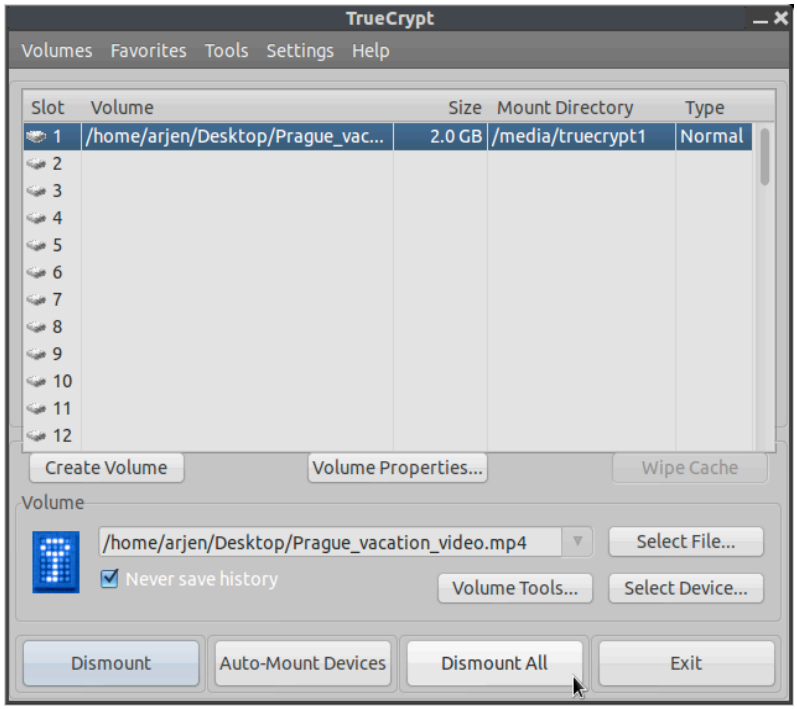
- The next screen is titled 'Encryption Options'. The default selections are fine. For the strongest encryption (encrypts multiple times): under 'Encryption Algorithm, select 'AES twoFish-Serpent', and under 'Hash Algorithm', select SHA-512.
- The next screen is titled 'Volume size'. Select the size of the container (obviously, this will determine the maximum amount of data that can be put into it).
- Set the volume password on the next screen. Make a good one (see chapter 8) and Do. Not. Forget!
- The next screen is titled Format Options. Select FAT.
  Expert info: FAT is compatible with all systems but is limited in the maximum size of files it can contain (individual files cannot be larger than 4 GB). Usually this should not be a problem. If you need to be able to store larger files and are certain that choosing something other than FAT will not

create problems with the sharing of the files, you could choose one of the other options.

- The program will now generate a random dataset to encrypt the volume. Randomly move your mouse around for a moment, before clicking 'Format'. The program will now create the volume. Depending on the size, chosen encryption algorithm and speed of your computer this will take a few seconds to hours (for very large volumes).
- Once the system is finished pres 'Exit' to return to the main program screen. Congratulations - you have created your TrueCrypt secure volume!

3. **Put the files you want to encrypt into your new encrypted volume**
   Now the volume can be 'mounted' (i.e. activated). Click 'Select File' > locate and select the volume you just made > click 'Mount'.
   Now enter the password and click 'OK'.
   The TrueCrypt container will now appear on your system as a separate drive (much like a USB-drive or external hard disk). You can put files into it in the same way you would use such external media (go to My Computer or Finder and click and drag files into the container).

   Once you have put the desired files in the container, 'close' the container by clicking 'Dismount' in TrueCrypt. The container will now appear to be just a file on your computer.



Create a hidden encrypted volume

Hidden volumes are encrypted volumes that sit undetectably within a regular TrueCrypt volume. The purpose of this is to provide an extra layer of protection should your password be forced from you, and plausible deniability.

You will create a password for the regular TrueCrypt 'outer' volume – the container that is visible in your directory. Inside this container you will put sensitive files that you could plausibly want to encrypt and keep secret (otherwise the adversary may keep pushing for the 'real' password) – but that, if worst comes to worst, you are prepared to share with an adversary, should you be subjected to pressure.

However, within that volume is a hidden volume. No one can see it, and as far as we know, even the most sophisticated examination cannot reveal the existence of TrueCrypt's hidden volumes. Only the creator knows it is there. You access it by entering an alternative password that you create specifically for access to that hidden volume. This is a password that you would be prepared to withhold much longer than the outer volume password.

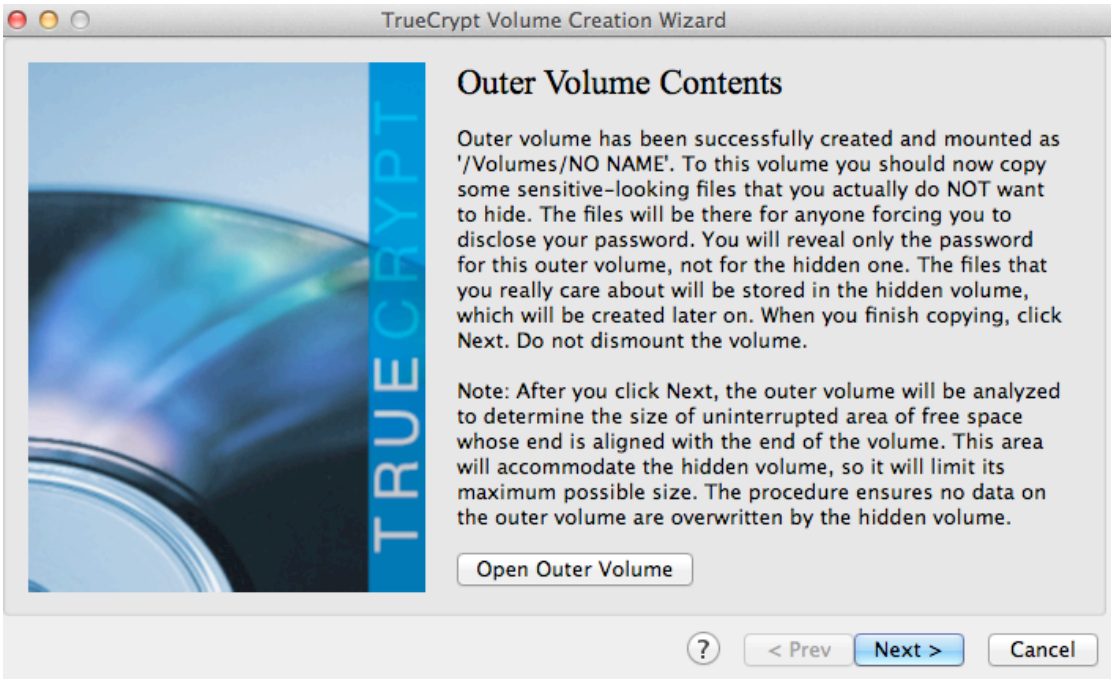
1. **Create the outer volume**
   Start the program and click:

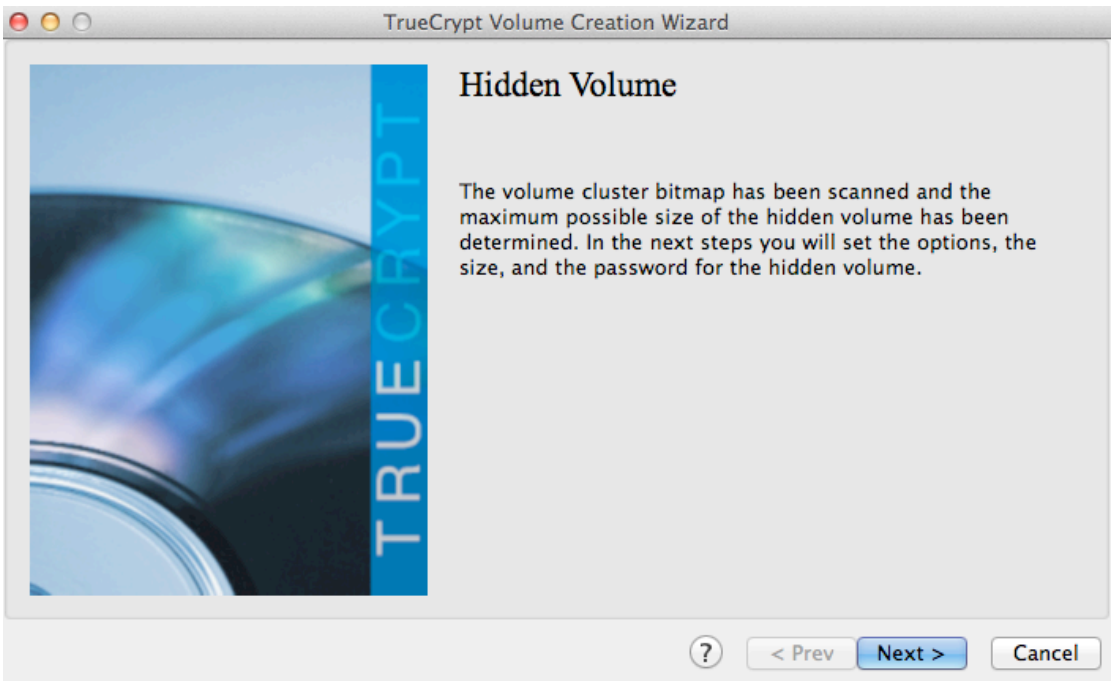
- 'Create Volume' > 'Create an encrypted container' > select 'Hidden TrueCrypt volume' > select the location where the container will be stored on your computer (it can be moved later) and give the container an (innocuous) name.
  To encrypt an entire external hard drive such as a USB stick, select 'Create Volume' > Create a volume within a partition/drive'

- The next screen is titled 'Encryption Options'. The default selections are fine. For the strongest encryption (encrypts multiple times): under 'Encryption Algorithm, select 'AES twoFish-Serpent', and under 'Hash Algorithm', select SHA-512.
- The next screen is titled 'Volume size'. Select the size of the container (obviously, this will determine the maximum amount of data that can be put into it).
- Set the volume password on the next screen. Make a good one (see chapter 8) and Do. Not. Forget!
- The next screen is titled Format Options. Select FAT.
  Expert info: FAT is compatible with all systems but is limited in the maximum size of files it can contain (individual files cannot be larger than 4 GB). Usually this should not be a problem. If you need to be able to store larger files and are certain that choosing something other than FAT will not create problems with the sharing of the files, you could choose one of the other options.
- The program will now generate a random dataset to encrypt the volume. Randomly move your mouse around for a moment, before clicking 'Format'. The program will now create the volume. Depending on the size,

chosen encryption algorithm and speed of your computer this will take a few seconds to hours (for very large volumes).

- The next screen is titled 'Outer volume' – read this carefully. You must now copy some sensitive looking files into this volume (i.e. copy-paste some files into the TrueCrypt container 'drive' which now appears in My Computer/Finder). Then click 'Next'.
- The next screen is titled 'Hidden Volume'. Read this, and click Next.





2. **Create the hidden volume**
   Now the outer volume has been created, you will be guided through the creation of the hidden volume. This will take you back through the previous step, but for your hidden volume. You will go through the screens for 'Encryption Options', 'Hidden Volume Size' (the space availability will depend on the size of the files you used as your decoy in the outer volume), 'Hidden Volume Password' and 'Format Options'. **Importantly,** you must choose a different password for the hidden volume to that of the outer volume. It is with these two different passwords that you gain access either the outer or the hidden volume.

3. **Put the files you want to encrypt into your new encrypted volumes**
   Now the volume can be 'mounted' (i.e. activated). Click 'Select File' > locate and select the volume you just made > click 'Mount'.
   Now enter **either** the password for the outer or hidden volume, depending on which you would like to access (it should be the hidden volume), and click 'OK'.

   Note that if you add more data to the outer volume, it may overwrite space/data in the hidden volume. Ideally, you will not change or add any more data to the outer volume after the creation of the hidden volume.

   The TrueCrypt container for that volume will now appear on your system as a separate drive (much like a USB-drive or external hard disk). You can put files into it in the same way you would use such external media (go to My Computer or Finder and click and drag files into the container).

   Once you have put the desired files in the container, 'close' the container by clicking 'Dismount' in TrueCrypt. The container will now appear to be just a file on your computer.

Encrypting entire hard drives

Mac and Linux systems have inbuilt options to encrypt the entire hard drive.

Linux/Ubuntu:
You will notice in our guidance on Ubuntu installation (chapter 2), we instructed you to opt to 'encrypt the Ubuntu installation' and 'encrypt the home folder'. These options encrypt the entire hard drive and the home directory with separate passwords.

Mac:
Go to System Preferences > Security and Privacy > FireVault > Turn on FireVault

Windows:
The most secure way to encrypt a hard drive on a Windows system is using TrueCrypt.

The method is much the same as those described above, except to begin the process: click 'Create Volume' > select **'Encrypt a non-system partition/drive** > 'Standard Truecrypt volume' > **Select the hard disk drive.**

Full instructions can be found here:
http://webapps.lsa.umich.edu/lsait/admin/HowTos/Encrypt-w-TrueCrypt-Win-FDE.pdf

Data: sharing securely

Risks:
- Interception
- Intervention
- Destruction of source documents
- Identification of source
- Identification of journalist

Infosec action:
- Exchange encrypted USB drives or hard drives (if you can meet in person)
- Exchange small volumes of data via encrypted attachments with encrypted emails
- Exchange large volumes of encrypted data via a file-sharing service

Physical exchange

The safest way to share large volumes of data is to physically exchange a storage device (ideally a USB-drive or hard disk) with the data on it in encrypted form.

The entire device can be encrypted, or several folders stored on the device can be encrypted with separate passwords so that access to them can be given in a controlled manner by the source (who can release passwords over time through secure channels such as encrypted email or OTR-chat – see chapters 5 and 6).

So, all you need to securely exchange data in person is encryption software (such as TrueCrypt) and a USB drive. You can currently buy USB drives with large storage capacity (256GB) for under £30.

Digital exchange

If you cannot physically meet face-to-face with your source to collect the documents, you will need to exchange your documents securely online.

Small volumes of data can be shared as encrypted email attachments, if both of you are using encrypted email (see chapter 5).

Large volumes of data should be encrypted using TrueCrypt, for example, and given an innocuous file name that does not relate in any way to the nature of the

data or specifics of the contents. You should then upload this file to a recommended file-sharing service, and send the recipient a link to the online file and the password(s) to decrypt via a separate, secure channel.

We would recommend 'Mega' (https://mega.co.nz/) as an alternative to popular file-sharing platforms such as Dropbox and Google Drive. Mega runs some encryption inside the browser before the file is uploaded to protect the user against low-level snooping and to legally protect Mega against accusations of facilitating copyright infringement (since they then cannot know the contents of the files being shared). While their encryption should not be considered 'government-proof' it does add a thin layer of protection against snooping on data as it is being transmitted over an open Wifi connection in your favorite anonymous upload café/station/library. Like most providers of online file storage Mega will provide 50 Gigabytes for every unique email-address you can make an account with. As with any other aspect of infosec compartmentalisation of data over several accounts that are not relatable to each other is advisable.

**Again, note here how you need a secure system for this to be a safe option. If your hardware or operating system is insecure, the files you exchange and passwords you share may also be insecure – an adversary could potentially have remote access or even control of your computer. Ideally, you will exchange documents between secure hardware and both using Tails to obscure your locations. For top security, you will only access the documents on an air-gapped machine.*

SecureDrop

Some journalistic organisations with considerable resources and IT capabilities have implemented their own systems to facilitate the secure sharing of files – namely, SecureDrop. SecureDrop is an open source whistleblower submission system, and it is great news that organisations are using it. However, setting up such systems properly and keeping them secure is not a trivial matter and should not be done without involving specialists with extensive experience and a proven track record. It is not a realistic solution for an independent investigative journalist.

**For questions on these matters, contact your organisation's IT-service provider who may be able to help (but ask them if they have done something like this before, and if not, seek help elsewhere). While the CIJ is not an IT-consultancy, it can provide some proven and trusted contacts to get started.*

OnionShare

OnionShare is an open source tool that lets you securely and anonymously (over the Tor network) share a file of any size.

The concept of OnionShare *is* a realistic solution for an independent investigative journalist – but it has only just been launched, and needs a little more testing and

improvement before we can recommend it to general users. Hopefully, this will be ready for general use soon.

Securely deleting files

On most systems, deleting a file does not actually remove the data from the computer's hard disk (or the USB drive, if that is where it is located). The file still exists but the space it occupies is simply labeled as 'no longer in use', and will eventually be re-used and displaced by other files. However, until then, the 'deleted' files can still be retrieved with the proper forensic tools and expertise.

To securely delete files, you can use specific tools that overwrite files with random data several times. This method is very secure, but may take a significant amount of time for large data volumes (e.g. several hours for multi Gigabyte USB-drives).

Mac

Securely deleting individual files:
After putting a file in Trash, go to Finder (left on the top toolbar) and select 'Secure Empty Trash'. The file will be removed from the Mac's directory, and the hard drive space it occupied will be overwritten with random data.

Securely wiping a USB drive (or any external hard drive).
Insert the USB drive. Launch 'Disk Utility' > Select the drive you wish to erase (see menu on the left) > select 'Erase' tab. Select 'Security Options' and set the slider to 'Most Secure'* > 'OK' > "Erase'.

Securely wipe all 'free' space on the Mac's hard drive:
This seeks out any areas of the drive marked as available for new data and overwrites them with random data.
Launch 'Disk Utility' > Select the drive you wish to erase (see menu on the left) > select 'Erase' tab > click 'Erase Free Space'. A window will appear with 'Erase Free Space Options' – set the slider to 'Most Secure'* and click 'Erase Free Space'.

*(On some Mac OS versions, this will be a button rather than a slider, and labelled '35-Pass Erase of Deleted Files').

Windows, Linux/Ubuntu

On Linux and Windows systems BleachBit (http://bleachbit.sourceforge.net/) is the premier, open source tool that is considered highly trustworthy.

Tails

The Tails system has a Secure Erase feature that can be easily accessed by right clicking on a file.

Physical erasure
If an entire disk needs to be wiped there is also the option of physical destruction of the storage device. To be certain that no data can be retrieved afterwards the device needs to be ground up into very small parts no bigger than 1 mm. Do not assume that specialised forensic techniques can be defeated by simply breaking a disk with a hammer or immersing the device in water. While this will almost certainly break the functioning of the device, data may still be retrieved if the adversary has the means and time to use more advanced methods of data recovery.

Opt for USB drives
Since storing data on the internal disk of a laptop exposes the data to additional risks and possibly makes it harder to securely erase, storing sensitive material on an external storage medium such as a USB-drive or external hard disk (for large volumes) is strongly recommended. Encryption of such devices or the files on them is also important to protect against loss or theft by adversaries.

Metadata

Meta-data is data about data. Metadata could include the author of a Microsoft Word document, or the GPS co-ordinates of where a photo was taken. Audio, video, and PDF files also hold metadata and hidden data (such as comment or tracking history, file names, etc.). Most colour laser printers will print their type and serial number in tiny invisible dots on every square centimeter of paper so that those pieces of paper are traceable if the serial number of the printer is in any way connected to you (such as by ordering the printer online).

Each program used may have specific metadata settings, so you should do some research online (or consult an expert) on whatever program and file you plan to use, to be sure you are aware what information is being stored, how you can remove it and how to make sure this information is harmless.

LibreOffice
LibreOffice is a free, open source office suite.
https://www.libreoffice.org/

In LibreOffice, user data can be viewed and cleared by going to:
File > Properties > General tab

- click 'Reset' to reset general user data (e.g. total editing time, revision number)
- uncheck 'Apply user data'

Then check the 'Description' and 'Custom Properties' tabs and clear any data you don't want disseminated. Under the 'Security' tab, uncheck 'Record changes' if not already clear.
Under Edit > Changes > Accept or Reject: you can clear these if the recipient doesn't need them.

If you use the Versions feature, go to File > Versions and delete any older versions of the document that may be stored there.

(Just for Writer) View > Hidden Paragraphs, check that all hidden paragraphs are visible.
(Just for Calc) Format > Sheet, check that there aren't any hidden sheets.

Chapter 5: Email

Email is very likely the means by which you most frequently contact colleagues and sources. Vitally, it is the means by which a new source is likely to contact you. Therefore, having secure email, not only for everyday use with colleagues but as a secure channel for initial contact, is important for any investigative journalist.

The risks to your email communications may include an adversary doing any of the following:

- Reading email content
- Reading subject header
- Seeing who you are contacting, how often and when
- Intercepting email attachments
- "Man in the middle" attacks (an impersonator intercepting communications)
- Seeing where you are emailing from (location)

Infosec action:

- Use strong passwords
- Use a trustworthy email provider
- Encrypt your email
- Verify your keys
- Put minimal information in your email subjects
- Email from Tails, or a public WiFi connection (if/when you need to)
- Use anonymous email addresses for select purposes

The risks

For protection against most non-state level actors, using a very strong password is a good defence against unauthorised access. However, for state level actors, it may be no defence at all.

An email provider that is 'trustworthy' is one who has a good basic security infrastructure, and who won't hand over your data to an intelligence agency in a hurry. If you don't trust the country where the email provider is based, it is best not to use an email address there. For example, we know that the default position of the US and UK intelligence agencies is to record and store all of our email communications. Even if you don't feel your email communications to be of relevance to these agencies now, they will be retroactively accessible should you and/or your work become relevant in the future. So, if you don't trust the US approach to email privacy, assume that the email providers based there (Outlook, Gmail, Riseup, etc…) are subject to that approach. Some are thought to be more co-operative than others, but unless you run your own server (or the organisation you work for runs their own server in a country with good privacy laws, like Switzerland or Iceland), we should assume that your emails and email

metadata is not secure with *any* email provider. Other considerations are whether you have to hand over your mobile phone number, a postcode/address, or another of your email addresses in order to register an account with a provider, as you may want to avoid donating that information (and especially if/when you use an anonymous email address).

Metadata: is data about data. Email metadata includes both the sender's and recipient's names, emails and IP addresses, server transfer information, date, time and timezone, unique identifier of email and related emails, content type and encoding, mail client login records with IP address, priority and categories, subject of email, status of the email, and any read receipt request.

Example: US government authorities requested access to the metadata of an unnamed user of Lavabit, a secure email provider, as well as the company's private encryption keys (allowing access to user's passwords) in the summer of 2013. Presumably, they asked for this because they were unable to covertly gain access themselves. The attempted breach was thought to be because NSA whistleblower Edward Snowden had an email account with Lavabit. The founder of Lavabit was legally restricted from discussing the exact requests of the US government – as is anyone approached in this way (which makes evaluating the security of our email providers all the more difficult). Rather than allow a breach of users' privacy, the founder suspended Lavabit altogether, in August 2013.

Email encryption

It is important to encrypt as many of your email communications as possible, using 'public key cryptography'. Public key cryptography scrambles the content of your email into (thus far) unbreakable code using your 'keypair', and then sends the encrypted message to be received and decrypted only by the keypair of the intended recipient.

We recommend the GNU Privacy Guard, 'GPG' (an open-source implementation of Pretty Good Privacy, or PGP).

Using GPG, whilst very different to normal emailing, is not difficult and you will get used to it very quickly. Understanding exactly how it works, however, is slightly more challenging.

Keypairs

Keys are essentially unique long sets of numbers, and each user of email encryption has a key pair – a public key, and a private key.

Your public key is like your listed phone number in the phone book. It is public and openly available so that anyone can contact you securely. To make sure people know the public key really does belong to you, you should keep a copy of it on your website, and/or a 'fingerprint' of the key (a unique code coupled with your public key) on your business card.

Although your public key is freely available, the private key in the keypair ensures that no one else can have unauthorised use of it.

Unlike your public key, your private key is exactly that – private! A private key is what allows you to decrypt emails from others who have contacted you using your public key.

Using the phone analogy, lets say someone calls your phone using a number they found listed on your website (your public key). However, this is a very secure phone, and when you answer you can only begin hearing one another when you provide an entirely secret code (your private key). When you call someone else, you do so using their publicly listed phone number (their public key), and their phone has a call reader so they can see who's number it is that called (your public key 'signature') – so they know it is definitely you. To begin hearing one another, however, the recipient provides their entirely secret code (their private key).

The length, randomness, and sophistication of public key cryptography is such that the encryption is much stronger than a 'secret code' as described in the analogy above. In fact, even you will probably never see your private key – it lives and works under the bonnet of your GPG software. This type of encryption remains, as far as we know, unbreakable.

Verifying keys

Importantly, you should always verify the keys of the people who you send encrypted mail to. Although the email address belongs to the person you want to contact, the public key might not. This is known as a 'Man-In-The-Middle' (MITM) attack – the covert interception of communications by the impersonation of a target. You need to make sure that both the email address *and* the public key definitely belong to the individual concerned. See 'verifying keys' later in this chapter.

What email encryption can't do

Note that email encryption does not hide metadata such as who you are talking to, the email subject, or your location. For people at all risk levels, it is a good idea to be minimalistic or obsfucatory in your subject line.

Protecting your identity and location when emailing

At higher risk levels, for those who wish to hide the real identities of themselves and/or others communicating, anonymous email accounts should be used, unassociated with any other aspect of your online identity - it should not be connected with you in any way. Gmail and Hotmail tend to request a phone or alternate email address, so these providers are not ideal for anonymous accounts. In many countries, GMX allows users to create accounts without giving personal information.

However, if you create an anonymous email address from an internet connection that is associated with you, your anonymity may already be compromised. Furthermore, when you send and receive emails, you are doing so by connecting to the internet – thus your location is known by the internet provider (and intelligence agencies). If you want your identity *and* location to be anonymous, you can use an anonymous email account with the Tor browser (see chapter 3) for webmail (i.e. unencrypted mail) and any machine you trust; or the Tails operating system, which hides the real location of *all* of your laptop's communications with the internet (see chapter 2). If you are working on a Tails system, when he desktop email client (which supports encryption) sends and receives information/mail to and from the internet, it does so through Tor, thus hiding the real location of the connection.

More commonly, you might just want to protect your location in the field rather than identity per se. For this, using the Tails operating system is the only answer.

Basic notes about email encryption

You can't encrypt or decrypt email from your smart phone. Whilst it is possible to set up on some Android phones, it is highly inadvisable because mobile phones are fundamentally insecure anyway (see chapter 7).

Neither can you encrypt or decrypt mail in your web browser (unless you are using the Tails operating system, where things work a bit differently) – you will use the Thunderbird email client on your desktop, with the added GPG encryption software and the Enigmail security extension, in order to encrypt and decrypt mail.

Finally, as is hopefully clear at this point, you can only send encrypted emails to other people who also use encrypted email. This used to be a rather small community of people and especially of journalists - but in a post-Snowden world, it is growing exponentially.

Installation instructions for encrypted email

1. UBUNTU/LINUX: Thunderbird email client and GPG encryption software

Ubuntu comes pre-loaded with Thunderbird (email client) and GPG encryption software.

Use the Ubuntu search tool on the top left hand of the desktop to find it.

1. MAC: Download Thunderbird email client and GPG encryption software

You will need to download:

- An **email client**/mail manager for your desktop - we recommend Mozilla's open source 'Thunderbird'
    - http://www.mozilla.org/en-US/thunderbird/
- **GPG** – Gnu Privacy Guard, which is encryption software

- https://gpgtools.org/ The first pink download box, 'Download GPG suite' will be the latest version – click on it to download.

When the downloads are complete, open Thunderbird from your Downloads and drag the Thunderbird icon into the Applications folder.

1. WINDOWS:

You will need to download:

- An **email client**/mail manager for your desktop - we recommend Mozilla's open source 'Thunderbird'
  - http://www.mozilla.org/en-US/thunderbird/
- **GPG** – Gnu Privacy Guard, which is encryption software
  - http://www.gpg4win.org/download.html . The first green download box will be the latest verion of GPG – click on it to download.

Open Thunderbird. If you are opening Thunderbird for the first time, it may prompt 'Integration' or a 'Set up wizard' – skip both of these. Thunderbird will also prompt you to configure your email account, and offer you a new email address. Click 'Skip this and use my existing email'. Enter the email address you would like to use for encryption and the password. You should decide whether you select 'Remember password' or not – if you don't remember password, you will need to enter your email account's password every time you access the account on Thunderbird. Click 'Continue'.
Note – if you are using an anonymous email address, obviously, do not enter your real name!

You should see, 'Configuration found in Mozilla ISP database'.

You now have the option to choose between IMAP or POP3. Choose IMAP, and click 'Done'.
Expert info: Unlike POP, IMAP offers two-way communication between your online email account and your desktop email client – so any changes you make in your email client are communicated back to your online account (e.g. if you mark an email as 'read' on Thunderbird, with IMAP, it will appear as 'read' on your online email account too).

2. Enigmail security extension

At the top of the Thunderbird window, and click on Tools > Add-ons > Extensions. If you see 'Enigmail', you already have Enigmail. If not, go to the search bar in the upper right of the window, and search for 'Enigmail'. Click 'Install', and restart Thunderbird.

3. Keypair

At the top of the Thunderbird window, click on OpenPGP > Key Management. Back up to the top toolbar, click > Generate > New key pair.

- the email address you wish to use for encrypted mail should be selected
- Tick 'Use generated key for the selected identity' Select key to expire in 5 years.
- Enter a passphrase (this is the passphrase for your encrypted mail – not just your online mail account – it should be very strong)
- Under 'Key expiry', the Key should expire in 5 years.
- Click the 'Advanced' tab, and select the maximum key size of 4096, and Key type 'RSA'
- Click 'Generate key' and move your mouse around the screen whilst it generates your key (this aids the 'randomness pool' from which the key is configured). This may take a few minutes.
- A box will appear informing you that the key generation is completed. Click 'Generate Certificate' in this box (this creates a revocation certificate that you will need when you wish to invalidate your key, for example, if the key is lost or compromised). Save the revocation certificate somewhere safe. You will now be asked to enter your passphrase in order to complete this action.

Configuring Thunderbird

Go back into Thunderbird to change some settings.

Expert settings

Open PGP > Preferences > Display Expert Settings

- Sending: Tick
  - 'Add my own key to the recipients list'
  - 'Re-wrap signed HTML text before sending'
  - 'Always confirm before sending'
    - *N.B. this is a very useful tool that tells you every time you send an email whether the email is signed and encrypted – so you are much less likely to accidently send an unencrypted email*
- Sending: Untick
  - 'Always trust people's keys'
- Key Selection: Tick only 'By email addresses'

Click 'Ok'.

Saving folders locally

This is particularly useful for saving drafts – you don't want your draft, unencrypted emails being saved on your online mail folders. Rather, you can save them locally on your hard disk, where you have more control over their security.

In the menu bar on the left hand side of the Thunderbird window, you will see all your email folders. At the bottom, are 'Local Folders' – right click and select 'New Folder'. Creating 'Sent' and 'Draft' local folders may be helpful.

Click Edit (Linux) or Tools (Mac) > Account Settings > Copies & Folders. You can select where to store your messages here. For example, under 'Drafts and Templates', select 'Local Folders' as the location to keep your message drafts.

Email in plain text
HTML does not encrypt well, so you will write messages in plain text instead.

Edit (Linux) or Tools (Mac) > Account Settings > Composition & Addressing
Deselect 'Compose messages in HTML format'

Share your PGP signature with contacts
Sharing your PGP signature with the people you email, even when the email is not encrypted tells the recipient you have PGP encryption and (technically) allows them to verify your identity.

Edit (Linux) or Tools (Mac) > Account Settings > OpenPGP Security
'Enable OpenPGP support (Enigmail) for this identity' should be ticked
Tick both 'Sign non-encrypted messges by default' and 'sign encrypted messages by default'. Click 'OK'.

Publicly list your public key
Uploading your public key to the keyserver is like listing your phone number in a phonebook. It allows people to search for your name/email address, and locate your public key in order to send you an encrypted email. This is very useful for journalists who invite encrypted mail and wish to protect source confidentiality. However, if you are setting up encryption for an anonymous email address that you will use only to communicate with specific, high risk individuals, of course there is little to gain from uploading your public key to the keyserver.

Open PGP > Key management.
Tick 'Display All Keys by Default'. Right click your email address, and select 'Upload Public Keys to Keyserver' if you want people to be able to contact you. The default keyserver (pool.sks-keyservers.net) is fine.

To search for anyone's public key
Search for a name/email address to see if a person has a public key listed, so you can send them encrypted mail (like searching for a number in a phonebook).

Open PGP > Key management > Keyserver (in the top toolbar) > Search for keys.
Tick the email address of anyone whose key you'd like to import and press ok.

Verifying keys

Make sure that the person you think you are communicating with is certainly who they say they are

In Thunderbird, go to OpenPGP > Key management > right click a selected email address > View Properties. Here you will see the person's key ID and fingerprint. You can verify that the key does indeed belong to the person by exchanging fingerprints by another communication means (in person, on the phone, on their business card/website), and checking they match exactly. In the same window you can then click Select Action > Set Owner Trust > and select how much you trust that the key does in fact belong to the individual concerned.

Add a regular email signature
With your name, job title, website, email address/es, PGP fingerprint, etc…

Edit (Linux) or Tools (Mac) > Account Settings
Here you can enter signature text to attach to your emails.
Edit (Linux) or Tools (Mac) > Account Settings > Composition & Addressing
Select 'Include signature for replies'

Receiving new mail
You can decide how frequently the mail client searches for new messages.

Edit (Linux) or Tools (Mac) > Account Settings > Server settings

Send an email!

When you have completed the set up, send a test email to someone else who has encrypted mail. Find their key on the keyserver, and be sure to verify it and sign your trust of their key before you try to send an email (otherwise the email client might not actually let you send them encrypted mail – Thunderbird will encourage good infosec in this way!).

Choose a recipient whose key you have already imported, verified, and set owner trust for. Write your email, and before you click 'Send', go to OpenPGP within the email compose window and tick 'Encrypt Message'. Press 'Send', and the confirmation box should tell you that the email is both signed and encrypted (if not, go back and check you ticked to encrypt). Click 'Send Message', and your encrypted email will be sent!

Sending/receiving attachments
You can encrypt and decrypt attachments to your emails with GPG too

When sending a file as an attachment to an encrypted email, you can choose whether or not to encrypt the attachment too. Write the email and attach a file as normal. Click 'Encrypt Message' as usual and then 'Send'. Before the email sends, you will be given three options, of which the first two are relevant. The first option is to just encrypt the message but not the attachments. The second is to encrypt the message, and to also individually encrypt attachments. Opt for the second choice ('Encrypt/sign each attachment separately and send the message

using inline PGP'), and click OK. Then your confirmation box will pop up as usual, telling you the message is signed and encrypted – click 'Send Message', and the email and attachment will be sent.

When someone sends you an encrypted email attachment, right click the attachment and click 'Decrypt and Save As'. Save it in your chosen location, and then go to that location to find/open the attachment.

Of course, if you are mailing an attachment that has already been encrypted by other means (e.g. TrueCrypt), you don't need to encrypt it again using GPG.

Chapter 6: Instant Messaging

Instant messaging is a great way to start and maintain conversations with a source, and it is very quick and easy to set up encrypted, 'off-the-record' (OTR) instant messengers (IM) – especially compared to setting up encrypted mail. Using an OTR IM, you can discuss necessary security protocols before you continue conversing, meeting, emailing, sharing documents/information, and so on. It is also a useful tool for talking to colleagues if you are collaborating on a project.

Off-the-record (OTR) messaging allows you to have private conversations over instant messaging that are not only encrypted messages between verified contacts (like your encrypted email), but that are also 'deniable'. That is to say, it is plausible that a chat purportedly including a chat account associated with you, is not actually you.

Expert info: Like encrypted emailing, OTR IM uses public keys by which you can verify that your contact really is who they purport to be. However, every time you begin a new chat with a contact, the chat is encrypted using a new, throwaway set of keys. Don't worry – you don't have to do or even see this yourself – this is under-the-bonnet encryption that the messenger client does it for you.

If you are using Linux or Windows, you will use an IM client called Pidgin, with an OTR plug-in.

If you are using Mac, you will use an IM client called Adium.

Users of Pidgin and Adium can communicate easily with one another. However, in the current versions, the verification methods for the two messenger clients are different. See 'Verifying contacts'.

Adium instructions for Mac:

1. **Download Adium**
   Download and install "Adium" for Mac – http://adium.im/

2. **Create and configure an IM account**
   Once downloaded, open Adium and go to (at the top) "File">"Add account">"Jabber". Under "Jabber ID" choose a name and add @jabber.ccc.de or @jabber.cryptoparty.is to the end of it, e.g. kissinger@jabber.ccc.de Under "password" choose a strong password
   - Don't choose "register account" just yet – click the "Options" tab first (in that same window)
   - In "options" tick "Require SSL/TLS" and tick the "Do strict certificate checks"
   - Now go to the "Privacy" tab and in the "encryption" drop down menu click on "Force encryption and refuse plain text" (last one on the list)

   Go back to the Accounts tab and click "register account". In server type jabber.ccc.de (or @jabber.cryptoparty.is if you went for that) then click

"Request new account". In a moment it should tell you that your account has been successfully created.

3. **Configure Adium**
   Go to Adium > Preferences > General > untick 'Log messages'

Pidgin instructions for Linux (Ubuntu)/Windows

1. **Download Pidgin and OTR plug-in**
   Download and install Pidgin at www.pidgin.im (Windows); if you're on Ubuntu, you will be directed from that page to the Pidgin PPA package, so download that.
   For Windows, then download the OTR plug in from https://otr.cypherpunks.ca. On Ubuntu, go to the Ubuntu Software Centre, search Pidgin OTR, and install the 'Pidgin Internet Messenger Off-the-record Plug-in'.

2. **Configure Pidgin**
   Open Pidgin. If this is the first time you are opening Pidgin, you will not have an account configured and will be prompted to 'Add an account'. Click Add (if you are not prompted, you can find this at Accounts > Manage Accounts > Add).
   a. Under 'Protocol' select XMPP/Jabber (NOT Facebook XMPP)
   b. Choose a (fairly anonymous) username
   c. Under domain, type jabber.ccc.de or jabber.cryptoparty.is
   d. Make a strong password
   e. Click on the 'Advanced' tab and for 'Connection security', ensure 'Require encryption' is selected
   f. Click back onto the Basic tab and be sure to tick 'Create this new account on the server' at the bottom of the window before you click 'Add'
3. **Create an IM account**
   Your Jabber address should appear in an 'Accounts' window. Tick the 'Enabled' box and then click 'register' in the 'Register New XMPP Account' window that appears.

4. **Configure OTR**
   In Pidgin, go to Tools > Plug-ins > tick 'Off-the-record messaging'. Then click 'Configure plug-in'. Tick all the default OTR settings: Enable private messaging; Automatically initiate private messaging; Require private messaging, and Don't log OTR conversations. Now click 'generate' to generate a key for your account.
   Go to Tools > Preferences > Logging and untick all logging options – you do not want to log chats.

Congratulations! You now have a configured OTR IM and can enjoy off-the-record, encrypted chat.

Test your OTR chat

Add a contact

Pidgin

In Pidgin, go to Buddies > Add a buddy and type in their full address before clicking 'Add'. When your contact is next online, they will receive an authorisation request from you.

To start a conversation with an online contact, double click on a buddy/contact in your list, and click OTR > 'start private conversation' in the chat window.

Adium

In Adium, go to Contact in the top toolbar > Add contact. Under 'Contact type', assuming your contact is also using Jabber, select XMPP/Jabber, either their full address in 'Jabber ID', and click 'Add'.

Authenticating/verifying a contact

Ideally, you will use fingerprint verification and if you know the person well enough, you will also ask a question of each other, that only the other person would know the answer to.

Pidgin

If you have not yet authenticated your contact, double click on their address to open a chat window with them, go to OTR in the chat window and click 'Authenticate buddy'. You can authenticate either by

- A question and answer
  - A good, personalised method
- A shared secret
  - Has to be pre-arranged via a different communication method so this is less useful
- Manual fingerprint verification.
  - A useful and strong method
  - The only method by which Adium and Pidgin users can authenticate one another

In that window, select 'Manual fingerprint verification' as the method, and you will then see your contact's purported fingerprint. Check the fingerprint – if it is ok, select 'I have' verified that this is in fact the correct fingerprint, and click 'Authenticate'.

Adium

If you have not yet authenticated your contact, double click on their address to open a chat window with them (even if they appear to be offline – they will appear offline and 'not authorised' until you verify them). Click the lock icon and select 'Initiate Encrypted OTR chat'. The lock should close. With the chat window still open, go to the top toolbar in Adium, click Contact > Encryption > Verify. You will then see your contact's purported fingerprint.

Checking fingerprints

You should ideally check one another's fingerprint by a communication method other than IM (email, phone). If there is not a secure means by which to do this, a mutual friend/third party on IM can pass on a partly redacted version of your fingerprint to the contact (e.g. 0---A7-0 D—706-D 2—65--1 --3D-9C2 0-57B—1), and the contact's fingerprint to you, for you both to check alongside the purported fingerprint shown.
Note: you should redact parts of your fingerprint to prevent an easy 'man-in-the-middle impersonation attack.

Finding your own fingerprint

Adium users can find their own fingerprint in Adium > Preferences > Advanced (horizontal tab) > Encryption (tab on the left hand side column).

Pidgin users can find their own fingerprint by opening a chat window with a contact, clicking the small buddy icon (right of 'OTR') > Re/Authenticate buddy > Manual fingerprint verification.

Chapter 7: Phones and Voice/Video Calling Over Internet

7.1 Phones

Many of us find our smart phones to be great importance and value in our everyday life and work. The benefits of being constantly connected to our email accounts, web browsers, social media, calendars, and also having easy access to a high quality camera and voice recorder, do indeed make them valuable tools. However, they are basically redundant for infosec purposes.

The only serious solution for information security is to use burner phones, with diligence and caution.

Phone risks:

- Automatic logging of your current/past locations
- Automatic collection of metadata, i.e. the phone number and location of every caller; unique serial numbers of phones involved; time and duration of call; telephone calling card numbers
- Theft and loss of data
- Remotely accessing data when phone connects to public WiFi
- Remotely accessing all data at any point the phone is on
- Phone/voicemail tapping, intercepting, or recording
- Covert remote automation of microphone to record audio
- Covert remote automation of camera to capture images

Dragnet phone surveillance

All phones leak an enormous amount of information about us to intelligence agencies, and we know from the Snowden revelations that programs collecting the full audio of every single call within a nation are, at the very least, already in place and being trialled in some countries. This type of surveillance is extremely dangerous for democracy, let alone journalism, and may permit 'retroactive' investigation of your work or your person, should you become of interest to intelligence agencies at some point in the future.

Therefore, it is worth using any phone with this in mind, whether you, your sources or colleagues may be targets of intelligence agencies now, or years in the future. They are not secure communication devices, and should be used sparingly, for only the most banal of your communications activities.

Targeted phone surveillance

Low risk

At a low risk level, the threat is mainly physical – someone gaining access to the handset. If this happens, even a fairly unsophisticated hacker/the police can crack your password (if you use a password lock) so this only provides minimal protection. If you are at a low risk level, just be sure to back up your data, and

stream or send any video or audio being recorded on the device to a secure storage cloud as soon as possible.

You can also use applications to track your device, should it be stolen in the field. For iPhone, for instance, Apple offer a free app called 'Find my iPhone' which tells you the current location of your phone. Another free anti-theft app is 'Prey' which, once you report the phone as stolen, will record not only the current location of the phone, but any other locations of the phone registered since you reported it stolen.

Medium risk

At a medium risk level, you may encounter an adversary trying to gain access to your data, not just physically, but remotely. When you connect a phone to a public WiFi connection, for example, a fairly unsophisticated hacker can intercept lots of information about you and connected accounts such as email and social media. Therefore, at a medium risk level, you may already be thinking about avoiding a smart phone as a work tool, or at least guarding it closely, closing applications after use, turning off WiFi in public, and using flight mode when you don't need to be connected.

- A note about smart phones: the vulnerabilities of smart phones are numerous, with some existing in the hardware, and they are not fixable. You can use open source software on smart phones, and even applications for encrypted chat. However, as we discovered in 'Protecting the System', when hardware is vulnerable, the software cannot provide you with real security. Therefore, we will not discuss such apps for the purpose of this guide.

As the recent phone hacking scandal in the UK demonstrated, unsophisticated hackers working for unethical journalists were able to listen in on people's voicemail. Private investigators often also have the ability to 'phone tap' (i.e. eavesdrop) not only voicemail but general phone calls made and received by a number. Therefore, you shouldn't discuss anything sensitive on your (mobile or indeed landline) phone.

High risk

At a high risk level, a phone basically *is* your adversary. At the very least, it locks your location and all associated metadata with the device is in the hands of a Five Eyes intelligence agency. At worst, it can be used to covertly collect the content of all of your phone calls, let alone all other data on the phone, and can covertly automate your microphone and camera to record audio and images (if it has a camera) too. This type of phone surveillance is very easy and basically comes at zero-cost to Five Eyes intelligence agencies, so you may not necessarily be an important target for them to justify this type of privacy invasion.

Infosec action

The only serious infosec action for phone communications is to use burner phones.

Ideally, your burner phone and regular phone will never both be emitting signals, since (if you are a target), your regular phone may pick up on the signal of the burner phone, making that a target too.

Before you use a burner, make sure the phone usually associated with you (e.g. your smart phone) is not emitting signals. Switching the phone to flight mode, removing the battery (don't bother trying to do this to the iPhone), and turning it off is good but is not enough. Do all of these things and then put it in a Faraday cage – popular solutions are biscuit tins, some fridges, or even a stainless steel cocktail shaker! The phone has to be completely sealed in metal (check it is working by trying to call the phone). It is a good idea to find and carry a small tin around with you to put your phone in, and in an important meeting, make sure all attending have done the same (a larger biscuit tin works well here).

A burner phone is a cheap, cash-bought, throwaway, low-tech phone, with a prepaid SIM card not registered to your person, to be used only for specific purposes. It can be hard, in some countries, to buy a SIM card without registering it to your personal details. Therefore, buying second-hand, or having a contact who can obtain such SIM cards, is ideal.

After some use of the phone, the phone may become associated with you and attract surveillance, so you should destroy it and use a new one. Changing the SIM card is not enough – each phone handset also has an IMEI (International Mobile Equipment Identity) number that identifies the phone. If the SIM has been identified as being yours, the IMEI will be too – so you will need to destroy the phone.

Due to intelligence agencies rolling out full audio recording of all phone calls, let alone the ease with which they can record a target's phone calls, you should avoid sharing particularly sensitive information - even on a burner phone.

7.2 Internet voice and video calling

Software that provides voice and video calling over the internet (Voice over Internet Protocol, VoIP), such as Skype, is enormously popular and useful, with Skype having over 700 million users itself. However, Skype does not offer full security, and there is not yet any user-friendly, secure alternative.

Among the Snowden revelations are details of the NSA's ability to intercept and store Skype communications. We should assume that all Skype communications are not just between us and our contacts, but with intelligence agencies too.

Example: Glenn Greenwald tells a story of when he used Skype in Hong Kong to call his partner back in Rio, David Miranda, to tell him he would receive some encrypted documents by email, and to store them securely. Greenwald never did send those files – but 48 hours later, Miranda's laptop was stolen from their Rio home.

We should also assume that it is not only the most sophisticated agencies that have covert access. For example, Egypt's secret police are known to have purchased Skype penetration tools, and man-in-the-middle Skype attacks have been reported by environmental campaigners working in Asia.

Secure internet voice and video calling is being worked on (by providers such as Jitsi) but it is currently rather inaccessible for non-experts.

So currently, we advise that voice and video calling is not suitable for any infosec purposes.

Chapter 8: Passwords

All of the systems and tools in this book use passwords as a method to correctly identify authorised users and secure against unauthorised access. Strong passwords are a key line of defence at all levels of information security.

However, bear in mind that passwords to online accounts are mainly a defence against non-state hackers (who are also able to obtain increasingly sophisticated commercial password cracking programs). There may be backdoor access at a state level to your online accounts, ultimately rendering a password irrelevant. That is one good reason to encrypt your emails – you may have an incredibly strong Hotmail password, but it doesn't stop intelligence agencies forcing Hotmail to handover all of your emails anyway (or more likely, covertly intercepting and collecting them without permission). If your emails are encrypted, all Hotmail can hand over is a pile of (thus far) uncrackable code.

So, whilst strong passwords are always a good idea, passwords that protect your system (e.g. hard disk encryption) and your encryption programs are far more important than passwords to online accounts.

Risks:

- Forgetting and losing passwords
- Overriding passwords by backdoor access (online accounts)
- Hacking (relatively unsophisticated password hacking)
- Password cracking (sophisticated)
- Key logger
- Being coerced into revealing a password

Infosec action:

- Learn how to create strong passwords
- Use KeePassX password manager (if you trust your system)
- Store the most important passwords in your head only
- Use hidden volumes for important encrypted files

Password cracking: understanding the risk

If your system is insecure, password cracking in a targeted attack is simple. An adversary could physically or remotely insert a key logger into your system, to record every keystroke. This would mean that an adversary captures every thing you type, including your passwords. This is not a hugely sophisticated attack and yet totally invalidates other security measures. Therefore, it really is important to secure your system in the very first instance, as described primarily in chapters one and two.

However, if your system is secured and your adversary does/can not use key logging tools, an attacker may try to crack the passwords that protect your system, software and accounts (and this may be either in a large scale hack of thousands of users, or in a targeted attack against an individual).

Password cracking programs are used by authorities across the world, but sophisticated versions are also available as commercial products. A password cracker can automatically test at least eight million passwords per second and may run for days, on many machines simultaneously. For a high-profile target, a password cracker could run on multiple machines, for months.

Password crackers try the most common passwords first. A typical password consists of a root plus an appendage. The root isn't necessarily a dictionary word, but it's usually something pronounceable. An appendage is either a suffix (90% of the time) or a prefix (10% of the time). A cracking program would typically start with a dictionary of about 1,000 common passwords, such as "letmein," "temp," "123456," and so on, and then test them each with about 100 common suffix appendages: "1," "4u," "69," "abc," "!," and so on. It is thought that about a quarter of all passwords can be cracked with just these 100,000 combinations.

Crackers use different dictionaries: English words, names, foreign words, phonetic patterns and so on for roots; two digits, dates, single symbols and so on for appendages. They run the dictionaries with various capitalizations and common substitutions: "$" for "s", "@" for "a," "1" for "l" and so on. This guessing strategy quickly breaks about two-thirds of all passwords.

The attacker will feed any personal information available about the password creator into the password crackers. A good password cracker will test names and addresses from the address book (post codes are common appendages), meaningful dates, and any other personal information it has.

A particularly comprehensive attack can be launched if your hardware is insecure (the root of all problems!). An attacker can index a target's hard drive and create a dictionary that includes every printable string, including deleted files. If you ever saved an e-mail with your password, or kept it in an obscure file somewhere, or if your program ever stored it in memory, this process will grab it and aid the process of cracking your password.

How to create a strong password

A strong password is one that the cracking process described will miss.

Password manager

One option is to use open source password management software such as KeePassX to generate a random, long, alphanumeric password (with symbols too, if they are permitted for the particular password), and then save it in your own encrypted password database. If you trust the other layers of your system, this is a fairly robust option.

Furthermore, this is a good way to store multiple complicated passwords for multiple accounts, with KeePassX also having entry fields for URLs, account names and comments for each password stored, so you can securely store all the

information you need. The random passwords generated are unmemorable, which fulfils a security function in itself. However, KeePassX allows you to easily copy and paste passwords from the database, so you don't even have to type them.

There is some debate as to how good such programs are at effectively randomising, but the human brain is pretty awful at randomising too, so it remains one of the best options we currently have.

You will need to create a master password for KeePassX, which must be very strong. You should aim to store this password only in your own head.

Schneier scheme

You should use manually created passwords to encrypt your whole system, any encrypted USB stick or highly important file (e.g. source documents), and your password manager. These important passwords should be stored in your human memory only, and therefore need to be memorable.

Of course, to minimalise any damage should a password be compromised, you should avoid re-using passwords.

To manually create a password, we recommend the 'Schneier scheme', a method advocated by Bruce Schneier, the internationally renowned cryptographer and security expert.

Schneier advises taking a memorable sentence and initialising, symbolising, and numbering the words to turn it into a password.

For example, "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary. Choose your own sentence - something personal, but not obviously related to you through public data.
Here are some examples:

- WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.
- Wow...doestcst = Wow, does that couch smell terrible.
- Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all.
- uTVM,TPw55:utvm,tpwstillsecure = Until this very moment, these passwords were still secure.

(Of course, do not use any of the above examples – now that they have been used, they are invalid as strong password options).

You get the idea. Combine a personally memorable sentence with some personally memorable tricks to modify that sentence into a password to create a lengthy password.

Being coerced into revealing a password

Let's hope that you are never in this situation. However, let's say a malicious group or agency has intercepted you, carrying an encrypted USB stick (with your most important files, or source documents), and they are prepared to go to extreme lengths to obtain the password in order to decrypt. What do you do?

In these instances, it may be helpful to have a hidden volume on your USB drive. A hidden volume is not visible to anyone and does not appear to take any space on a drive. As such, it can be overwritten easily. However, it means that the visible encrypted volume can act as a decoy, and provide you with plausible deniability. In the visible encrypted volume, you can store files that could reasonably warrant security and encryption, and this volume has its own password. However, the hidden encrypted volume sits undetected beneath the visible volume, and has a separate password.

You can create a hidden encrypted volume with TrueCrypt. This method may help protect the information from interception, but not from loss – it can be easily destroyed or overwritten so you should always back up important files.

(Much of this chapter is adapted from Bruce Schneier's blog, https://www.schneier.com/ . We thank Mr Schneier for allowing us to use his work).

Glossary

Term	Definition
Air-gapped	A security measure whereby a laptop is kept entirely offline, separate from other local networks and the internet
Backdoors	Covert security vulnerabilities that allow a system's known security mechanisms to be bypassed, allowing undetectable access to the computer or its data
BIOS	Basic Input/Output System - a set of computer instructions in firmware that control input and output operations
Bridges (Tor)	Bridges are Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that help circumvent censorship
Dragnet	A mass surveillance system operated through programs that sift through and collect the world's online and telecommunication data
Faraday cage	A metallic enclosure that prevents the entry or escape of an electromagnetic field
Firmware	Software programmed onto hardware that provides instructions for how the device communicates with the other computer hardware (includes BIOS)
Hardware	The physical elements that comprise a computer system
Malware	Malicious software, typically spyware, designed to disrupt or damage a computer system
Man-in-the-middle attack	The covert interception of communications by the impersonation of a target
Metadata	Data about data

Middleware	Programming that "glues together"/mediates between two separate and often already existing programs: e.g. allows programs to access databases
Open source	Freely distributed software for which the source code is publicly available
Operating system	The software that takes control of the computer as it boots up, tells the computer what to do and how to do it, and is the interface through which you use the computer

About the authors

Silkie Carlo is a London-based journalist, activist, and a campaigner at the Courage Foundation (https://couragefound.org). She graduated in Politics, Psychology and Sociology from the University of Cambridge in 2012, where she conducted the first ever research into the possibilities of reversing system justification, using WikiLeaks as a stimulus. Since 2012, Silkie has written features on whistleblowers for VICE, and occasionally teaches Politics and Psychology in addition to her work on Information Security.

Arjen Kamphuis is co-founder and Chief Technology Officer of Gendo (http://www.gendo.ch/en/blog/arjen) since 2005. Previously he worked for IBM as IT architect, trainer and IT strategy advisor. As CTO of Gendo he advises several national governments, non-profits and Fortune-500 companies on technology-policy. Since 2009 Arjen has been training journalists, politicians, lawyers, human rights workers and whistleblowers to defend their communications and data from government or corporate intrusions or manipulation.

--

If you can offer any feedback about this book, we would be most grateful to receive it.

Please email infosec@tcij.org.
KeyID :0x7EF8DE32
FP: D0C5 A200 A49B E194 7AE4 A7C8 4DD6 A68E 7EF8 DE32

You can also use this address for technical queries and advice.

This handbook is a very important practical tool for journalists. And it is of particular importance to investigative reporters. For the first time journalists are now aware that virtually every electronic communication we make or receive is being recorded, stored and subject to analysis and action. As this surveillance is being conducted in secret, without scrutiny, transparency or any realistic form of accountability, our sources, our stories and our professional work itself is under threat.

After Snowden's disclosures we know that there are real safeguards and real counter measures available. The CIJ's latest handbook, ***Information Security For Journalists***, lays out the most effective means of keeping your work private and safe from spying. It explains how to write safely, how to think about security and how to safely receive, store and send information that a government or powerful corporation may be keen for you not to know, to have or to share. To ensure your privacy and the safety of your sources, ***Information Security For Journalists*** will help you to make your communications indecipherable, untraceable and anonymous.

Although this handbook is largely about how to use your computer, you don't need to have a computer science degree to use it. Its authors, and the experts advising the project are ensuring its practical accuracy and usability, and work with the latest technology.

Gavin MacFadyen, Director of the Centre for Investigative Journalism

This handbook is being translated into Arabic, Chinese, French, German, Portuguese, Spanish, and other languages.