



PRACTICAL DIGITAL PROTECTION

defense beyond technology



PRACTICAL DIGITAL PROTECTION

A guide for practical cybersecurity in hostile environments

practicaldigitalprotection.com



Copyright 2017

CC BY-NC 4.0

Creative Commons Attribution-NonCommercial 4.0 International License

TABLE OF CONTENTS

PREFACE	4
INTRODUCTION	6
■ PART I: RISKS	8
CHAPTER 1: Know Your Threats	9
Insert: Basic Protection Behavior	14
CHAPTER 2: Preparing Your Computer	18
Insert: A Note on Passwords	25
■ PART II: COMPUTER SECURITY	27
CHAPTER 3: Core Rules	28
CHAPTER 4: Getting Information	33
<i>Story: Zero-inbox, Autodestruct Saving the Day</i>	40
Technical solution: FireFox and Extensions	42
Technical solution: TOR	47
Insert: The Dark Net	50
CHAPTER 5: Storing Information	51
Technical Solution: Basic Encryption	56
Technical Solution: Advanced Encryption	59
<i>Story: Hidden Encryption and File Recovery</i>	65
CHAPTER 6: Sharing Information	67
Technical Solution: ProtonMail	74
Insert: Sending Information to People at Risk	77
Insert: MetaData, Publishing and MS Office	79
CHAPTER 7: Deleting Information	83
Technical Solution: CCleaner	89
<i>Story: MetaData and McAfee</i>	94
■ PART III: PHONE SECURITY	95
CHAPTER 8: Phone Security	96
CHAPTER 9: Using Your Phone	101
<i>Story: How a Phone Almost Destroyed it All</i>	106
CHAPTER 10: Setting Up Your Phone	108
Insert: A Note on Location Tracking	114
CHAPTER 11: Secure Apps for Use	115
Insert: A Day in the Life	121
■ PART IV: PREVENTATIVE SECURITY	123
CHAPTER 12: Preventative Protection	124

PREFACE

If you are reading this you are likely already aware of basic cybersecurity threats. This manual is designed to show you the key cybersecurity problems and how to take steps to prevent them. It demonstrates why it's important to do so, with real cases of proper or improper cybersecurity being the difference between freedom and imprisonment for you, your friends, sources or coworkers. More than just a manual on technical cybersecurity, it's a manual on safer digital behavior.

One of several reasons for this manual is to provide a resource that responds to real needs concerning cybersecurity for journalists, lawyers, NGO workers and others in China.

“Many of the threats you face are more physical than digital.”

Everyone has heard of Edward Snowden and his revelations about the U.S. NSA and U.K. GCHQ and probably seen American movies about electronic surveillance, or discussions on how government agents and private hackers break encryption to steal data. Unfortunately, none of this is really relevant for human rights defenders in China, or most of the world. The key problems you will face are not the U.S. or other governments using massive resources to break the encryption that comes with almost all emails or mobile chat programs these days. The real problem lies in what happens when you are detained or your phone or computer is confiscated. This manual will focus more on a behavioral approach to digital security.

This is one of many areas where the threat to operating in China is vastly different from what is usually talked about in terms of cybersecurity. Many of the threats you face are more physical than digital. This manual, based on input and ideas from a wide range of journalists, NGO workers and others inside China, aims to remedy the misunderstanding by providing a guidebook for navigating and counteracting the most common risks.

Secondly, most of the material you will have seen online or been presented during trainings you may have attended, is usually a compilation of various technical solutions, many of them unnecessarily advanced. These often lack a thoughtful discussion on how improvements in your security will often come not from advanced technical solutions (although they are sometimes needed), but from relatively minor changes in behavior.

Finally, creating a manual on cybersecurity without taking into account real people's behavior and limitations would be a waste of time. If a manual focuses on the most sophisticated security solutions without taking into

account how it affects daily use and efficiency, then it is likely to be abandoned after time, practice used at first before slowly being ignored and leaving you less secure than when you started. A manual to actually help must find a middle ground.

“...improvements in your security will often come not from advanced technical solutions, but from relatively minor changes in behavior.”

This manual builds from the three issues above and presents a stand-alone text for step-by-step, self-guided study in recognizing and addressing the security risks you are most likely to face.

INTRODUCTION

Welcome to this practical, self-study manual on cybersecurity. In as little time as one day it will help you both understand the risks to your safety and allow you to greatly increase your security concerning your use of computers and phones. We advise you to read this manual sequentially chapter by chapter, as each chapter builds on knowledge presented in the previous.

Please have your laptop and phone with you as you read. Before you start making changes, make sure you created a backup or saved any data, documents, or other files you want to be sure to keep. You can move them onto a USB, another hard drive or your cloud storage for now. Later in this manual we will address protecting portable data storage such as USBs.

All chapters are written with your laptop in mind (Win10 and OSX), but many issues also apply to smartphones. Many of the apps are likewise available for both iOS (iPhone) and Android. Smartphone security is presented in its own chapter.

The manual is written with readability in mind and for most chapters the layout will be similar. Most chapters will begin with a general introduction to the issues and concepts of the chapter. It then presents behavioral changes to limit these risks, and concludes with technical solutions. In most cases you should be able to find technical answers online, so only the more difficult or important aspects are presented step-by-step with screenshots.

The technical sections of the manual are color-coded. Sections with light blue backgrounds behind the text are for OSX (Mac computer) and iOS (iPhone). Sections with light purple backgrounds concern Win10 (PC computer) or Android phones.

In between the chapters are stories. These stories are based on real cases and show how using, or not using, the solutions offered have had a direct impact. The cases come from NGO activists, journalists and lawyers but all stories are presented anonymously or with pseudonyms.

The manual is divided into four parts, broken up into 12 chapters.

Part I focuses on knowing your risks. It is designed to provide you with the tools to analyze your own situation and what the most likely threats against you are. It also includes some steps to take with your computer before getting started, such as changing basic settings.

Part II, the core, consists of chapters 3 through 7. Each chapter focuses on one specific issue, for example hard drive encryption, secure browsing, or deletion. Each chapter starts with an overview of the issue. This is followed by suggestions for changes, both in your behavior and in technical solutions, and where needed, step by step instructions on how to make such changes.

Part III covers Phone-specific security. Much of what has been taught in chapters on computers will apply to Phones (and tablets), but this section deals with specific phone-related threats and solutions.

Part IV covers preventive security. It is aimed at helping you take practical, non-cybersecurity related steps to ensure your safety, and how to be prepared for the worst.

In between the chapters are a number of stories. These are real stories by journalists, lawyers and activists who have been detained, kidnapped or imprisoned, and how Cybersecurity issues affected them. Specifically, the stories show how using, or not using, the advice given here helped or hurt them during interrogations.

PART I

RISKS

CHAPTER 1

Know Your Threats will present information on different types of threats that exist, and show you to assess your risks and needs, to allow you to focus on what is most important to you.

CHAPTER 2

Preparing Your Computer shows you how to take the first steps towards better digital security, and teaches you about your operating system's basic settings, and how to change those to correspond to your needs.



CHAPTER 1 KNOW YOUR THREATS



By reading this chapter you will familiarize yourself with the different kind of threats that exist against you concerning cybersecurity. Knowing these basics will help you understand and use the rest of the manual better.

There is little point in taking steps to secure yourself if you don't understand the threats you face. This chapter briefly outlines some of the most common threats. If any threat strike you as being very relevant to you, or of interest, please take the time to search for more information online. If you have trouble finding good resources or the issue is not clear or too technical, you can contact us for assistance.

BEING FORCED TO DISABLE YOUR OWN SECURITY

This is largely the reason behind this manual, as those working in China face far greater threats to their Cybersecurity than hacking. The key threat is being forced by police, state actors, criminals or others, to disable your own security, by providing passwords to your emails, your cloud storage or your encrypted data storage. This is a guiding concern for the whole manual, and the reason the manual focuses on behavior, and not just technology, as that is the only way to counter this threat. Of course, we also look at technical threats and offer solutions to those.

ALLOWING ACCESS THROUGH THE BACKDOOR

You wouldn't spend a month salary on a new strong door and then forget to buy a lock would you? Or install a safe front door and lock, but still leave the backdoor wide open? Unfortunately, when it comes to Cybersecurity this is exactly what many do. Going to great length to use strong passwords and wipe their browsing traces, only to allow an App on your smartphone direct access to the same service, requiring not even a PIN code. Or by accessing the same service on your phone's browser, leaving it wide open to anyone who gets either physical or online access to your phone. Proper security means you have to analyze your situation, and how

you use services and functions properly, completely, and then shut down your vulnerabilities.

LOCALIZATION / TRIANGULATION / TRACKING

These days' smartphones are more like computers, and computers more like smartphones. Through GPS, wireless connections, and radio (phone) signals, there are many types of connections that leave your computer and smartphone an easy target to track. Without precaution, always assume someone can easily track you, and the equipment required is not expensive. It need not be a government anymore to do this. Your phone never stops to send out location signals, even without a SIM card. Apps installed often require location access, opening up for more ways for people to track you.

INTERCEPTING SMS, CALLS, CHATS, EMAILS

Without encryption for your chat messages, emails, phone calls and SMS, the content is sent in plain text for not only the service provider to read, but anyone on your network. Most services today fortunately use encryption, and if you stay away from Chinese services, these companies are unlikely to hand out information they have to the Chinese state. Again, the main problem is not the sending of emails or SMS, but what happens when your phone or computer is taken and you are coerced into giving up your password (also called login credentials).

SECURITY HOLES AT START UP

Most operating systems (OS) for computers and phones come with selected settings for easy use, not for security. As such, a first step should always be to go over the settings for your devices and make changes to improve the security.

BREAKING PASSWORDS

Running an entire dictionary against a password can be done in minutes. Using brute force (running millions of attempts per minute) cracking a 4-6 character password can be done in an hour. Consider this when choosing passwords for those services that truly matter to your safety, like your work emails or encrypted storage. A short password might stop a random person finding your phone on the street from getting access, but will not help if you become a target for police or organized crime. Passphrases, longer randomized passwords, should be used.

VIRUSES, HACKING, ROOTKITS AND MORE

This manual will not focus on advanced hacking threats, because it is unlikely. However, do understand that viruses and rootkits (viruses hidden from you that allow others to access your computer) are common threats. Ensure that you have enabled your Firewall and have an antivirus program running in the background, and that they are set to update automatically. Updating regularly ensures that the application is equipped to recognize the newest threats. Expired anti-virus programs provide virtually no security.

NETWORKS

If someone did not want to detain you or confiscate your equipment, but instead secretly access your information, your network is the natural point of attack. Have you ever changed the password and username to access your router in your home? Chances are, like almost everyone, you have not. Login and password to routers are published online, and is the same for almost all routers. If someone can access your router,

they have access to your computer. It is also important to be aware that public Wi-Fi networks are inherently vulnerable and you should be extra cautious when doing anything over a public network.

FILE RECOVERY

When you delete a file, or empty the trash bin, or move a file from your computer to a USB or other external drive, nothing is deleted. Nothing. It's all there and might remain there for years to come. It is easily accessible by anyone with even just a small amount of IT skills. Free programs can be downloaded and with those you can find everything on your computer that you have deleted in the past with a single click of a button. The section on deleting files in this manual might be one of the most important ones.

Do you understand these general concepts and how they can pose problems? If not, please go online and search for more information before you continue. A key aspect to understand is how location on your phone (or computer) can allow others to track you, and how file recovery poses perhaps one of the most serious threats against your computer should it fall into the wrong hands.

ASSESSING YOUR RISKS AND NEEDS

Before you continue with this manual, you need to understand how it applies to you and your situation. The stories presented in this manual should make it clear to you that as a lawyer, journalist or NGO worker, there are significant risks. Even if your work is such that you do not fear prosecution or serious persecution, you will nonetheless be monitored at times, and if something happens to others, such as coworkers or friends, you are likely to be brought in for questioning, interrogated or have your computer or phone monitored. If you have not already taken steps to protect yourself, this could create a whole new security issue for you. As such, do not let your lack of security thinking allow a small problem to become a big problem.

“Proper security thinking will keep small problems small.”

STEP 1. WHAT DO YOU NEED TO PROTECT?

What kind of information do you work with, and if released or provided to either criminals or police, how could it affect you. More importantly, how could it affect others? If your entire hard drive is compromised, what would an outsider learn about you and your work? What would they learn about others, such as sources, funders, coworkers or partners? Be aware how your ignoring basic security thinking would affect you as well as others.

STEP 2. WHAT DEVICES ARE AT RISK?

You have only one phone? Perhaps you had another one you gave or sold to a coworker. You only access one computer, in your own care, or also use an office computer? Perhaps you use friends' computers to read your emails sometime? Make a list of all devices you use or have recently used for any work.

STEP 3. WHY ARE YOU A THREAT?

Are you a journalist? Is it likely that if actions are taken against you it's primarily to find your sources? Are you an NGO worker, and police might take actions against you to map how you work, or who funds you? A lawyer who provide legal aid to clients the state would rather did not receive proper legal counsel?

STEP 4. WHO IS YOUR THREAT?

Is it the local police, is it mafia? Perhaps it's State Security Police? Figuring out who the likely persecutor is will go a long way for you to decide on your security policy. Perhaps you are not a target at all, but you work for a newspaper often a target. If so, who is the attacker, and how could you become involved even though you are not an active target?

These are some questions you need to think about before continuing to read this manual. These questions are also further developed under Chapter 12: Preventive Security, the end chapter for this manual. Starting to think about this now will make this manual far more meaningful to you, and make it easier for you to understand why and how the different chapters apply to you.

BASIC PROTECTION BEHAVIOR

Once taken by police, state security or criminals, there is little room to protect yourself. The impunity with which police and state actors can act in countries like Vietnam, China, Pakistan and elsewhere will leave you with little protection. Chances are they will get you to do what they want, whether through threats to you, coworkers or loved ones, or through direct physical or mental torture. The only way to protect yourself once this happens is to have already taken steps to protect yourself. Luckily, there are easy ways to achieve this, and those steps can mean the difference between freedom and imprisonment for you, or putting others at risk.

There are too many services, emails, and other online systems for the police to effectively use random methods to get your information. They need to have an idea what they are looking for, or where to start. If they are to force you to give up login information or a password, most of the time, they need to know what to ask for. In China, they can assume you have a WeChat account, in Vietnam they will assume you have Facebook. However, besides a few such widely used services, they will need to find out what to ask for.

Solutions for the most common issues shown below are offered in the manual.

LIMITING POSSIBLE DAMAGE CAUSED BY THIRD PARTIES AND OTHER PEOPLE

First, your accounts could be known because of what happens to other people. The partners, coworkers or sources you communicate with could have already been detained and have given that information up, or they could potentially have sold you out. This means, for sensitive work exchanges, you need to consider not only what you say and how you store information. To begin with, always have a specialized email or chat identity for your most sensitive work. This should not be your regular work email or accounts.

These accounts should not use your full name, nor should you, as part of email or chat exchanges, include details on your exact identity, or location. Avoiding this at least gives you some deniability, even if a third party finds an exchange from this account in someone else's communication and this other person states that this account belongs to you.

This issue is one of the biggest concerns, but also the one you have the least control over, because it depends on other people.

The safest way to limit this risk is to, for your most sensitive exchanges, use emails and chat programs with an autodestruct function. Such a function means that the logs or emails are automatically destroyed, on both ends (sender and receiver) based on an agreed amount of time, destroyed after one hour or one day for example. The identity of the user can still be compromised, but any actual information or "evidence" shared will not be available to anyone, including you and the other person, as it will be regularly destroyed automatically, with no way to recover.

Autodestruct emails are particularly useful when communicating with someone you do not fully trust, or someone you know has very limited skills with IT issues. It is also very easy to use. The same

applies to certain chat programs.

DAMAGE CAUSED BY TRACES AND EVIDENCE ON YOUR COMPUTER

As soon as you are detained or your equipment is confiscated the authorities are likely to initiate technical forensic analysis. This is how the police can track down what accounts you use, and with that knowledge, more easily force you to give up access to such accounts. Once they have succeeded, the information they find can and likely will be used against you, as well as against others. The important of this cannot be stressed enough. There are ways to address this.

Your browser, for example, will save and store a wide variety of data. The most obvious type is bookmarks to an email provider, or cookies showing which websites you go to, but also more advanced data, as well as login information and even passwords.

You can set your browser to automatically delete such information, but that means you will need to re-sign in for everything each time you open your browser, including social media, shopping sites, etc. You also would not be able to save bookmarks. This makes general computer use rather inefficient. It also looks suspect.

Instead, the first thing you need to do is use a dual browser strategy. One browser for your normal day to day surfing and use. Another browser for accessing your most sensitive email and other accounts, or use for more sensitive research. This second browser should be set to wipe every trace automatically when you close it. It should also add certain security extensions that complement the browsers own wiping, to better remove more traces.

OPERATING SYSTEM TRACES AND EVIDENCE

Like your browser, your operating system collects traces on everything you do. This includes internet access. It also includes word documents opened and edited, temporary copies of data and documents, and logs of more or less everything. Accessing such information requires much greater technical skills than analyzing your browser, but is not very hard for police or governments with lots of resources.

To deal with this problem, you need to use a program designed to wipe these traces and this temporary data off your computer. Again, luckily, it's easy to use.

"DELETED" MATERIAL

One of the most misunderstood concepts is what it means to delete something from your computer. Police know this, and use it. In short, when you "delete" something, or empty the recycle bin, nothing is actually deleted. The only difference is the computer or phone marks it as 'available space', that can later be over-written with new data. It's still there. In many cases, it remain there for years to come. In other cases, only part of the "deleted" data is over-written by new music, files, videos or whatever, while the rest remains.

Even though you cannot see it or search for it, there are easy to use and freely available programs

that can identify all such data, restore it and read it as if it had never been “deleted” in the first place. Such programs are so easy to use - in fact even someone with no computer skills can do it, in as little as five minutes. If you are detained, this will be used on your USBs, phones, computer and devices. Keep this in mind.

YOUR DATA

A key issue of course is all the files, from documents to videos to photos, which you keep and store, whether on USBs, phones, external hard drives or your computer. The only way to really protect such information is to store it in one highly secure place. This should be an encrypted, hard to find, drive on your computer.

However, if encrypted, police will notice, either directly or through data forensics. With that in mind, to truly protect such information, you need to use a “hidden” encryption, so they can’t even see that you are encrypting information in the first place. They can’t demand, threaten, or torture you into giving access to something they don’t know exists.

Again, this is actually easier to do than it sounds.

You should also simplify everything. This means not only storing all relevant work files in one place, but only storing only that which is needed. A quick look at all your old work files will likely show you that most of those files are no longer needed. Drafts, earlier versions, supported files later incorporated into the main documents, etc., these can and should all be deleted. Only store such things that you actually need.

You can also move old files you need to keep, but are unlikely to need to use, to a safe cloud storage. Such a cloud storage needs to be safe, and you need to use one that does not have servers in your country. You also need to consider the point about browsers, to ensure police cannot identify your use of such cloud storage or access it easily.

PHONES, PADS AND APPS

You need to separate your work use between computer and phones. You should not let it overlap. All the steps you take for safety and security can be undone by careless phone use. What good is it to auto-destroy log files, keep your browser traces cleaned, if police can find that information even easier on your phone?

Everyone uses Apps on our phones to access accounts and services. Having mobile Apps not only gives the police direct, although limited, access to our accounts, for example emails, but also, even if you protect those Apps with additional passwords, will tell them what services you use. Your phone can literally destroy all your computer security. It has happened many times.

Make sure to specify how you use your phone, and make sure to avoid using Apps that are allowed to identify what services you use online. Usually when downloading or configuring your mobile Apps you will be asked whether to grant it access to location, camera, or contacts, for example. Furthermore, do not use the browser on your phone to access sensitive webmails, as traces are impossible to remove on a phone. Also, proper deletion is likewise much harder on a phone, and

you should never use your phone to store any work documents, or download any work documents for later transfer to your computer.

YOU

Finally, You. You are the biggest threat to yourself, and to others. Protecting your information, your knowledge and data requires you to plan ahead. Besides doing a risk assessment, you need to plan how you will act should you be taken, and share this plan with several trusted people who are unlikely to be taken. What information can you share (and some you must share, or they will know you are hiding something), and what information must you protect? Likewise, if you work with partners, you need discuss and make agreements so everyone agrees on the same strategy. You need to have a good idea what information others are likely to give up?

There is a saying in the world of politics: Never lie about something the public will find out about anyway. For you, do not hide information the police will likely find anyway. There is no technical solution for this, only your own precaution and intelligence.

BUT

These days, registering a SIM card in places like Thailand, Vietnam or elsewhere, without providing your ID, is hard. With that, and the fact that all Internet Service Providers (ISP) requires ID when setting up internet connections, you have a problem. In China or Vietnam, no probable cause is needed for police to access the phone company or internet company logs. And these companies are required to store information on how their customers use their services, i.e., they record how you use your phone, including your location, as well as your internet use.

The above means that all the steps you have taken to protect your data, to hide your internet use and what services you use, like emails for example, can be undone. Luckily, you can also easily hide much of this information from your internet operator by using a VPN or TOR. It's harder against your phone operator, so again, we advise you to use your computer more than your phone for work.

CHAPTER 2 PREPARING YOUR COMPUTER

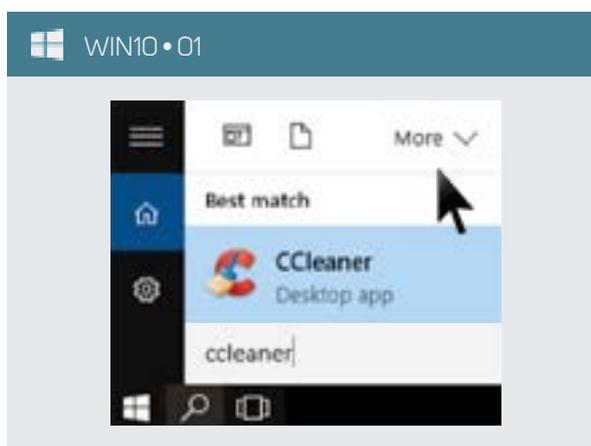


This chapter will show you some settings on your PC that need to be considered. By going over this chapter, you will have a greater understanding of the basic settings and setup of your computer, and how and what you can change and control.

For the remainder of this manual, for the technical instructions, we will be using the search functions. As such, when technical changes need to be made, we will provide the search term to locate the specific setting. You are likely familiar with the search functions, but to be sure, below is a screenshot showing the location of the search area (WIN-01).

These search terms will be given in English, and the search terms will look like this: Search Term.

Technical instructions sometimes come with screenshots. For PC's, these are numbered WIN - X and for Mac's OSX - X. If a screenshot applies to both Win10 and OSX, they are referenced as WIN + OSX X).



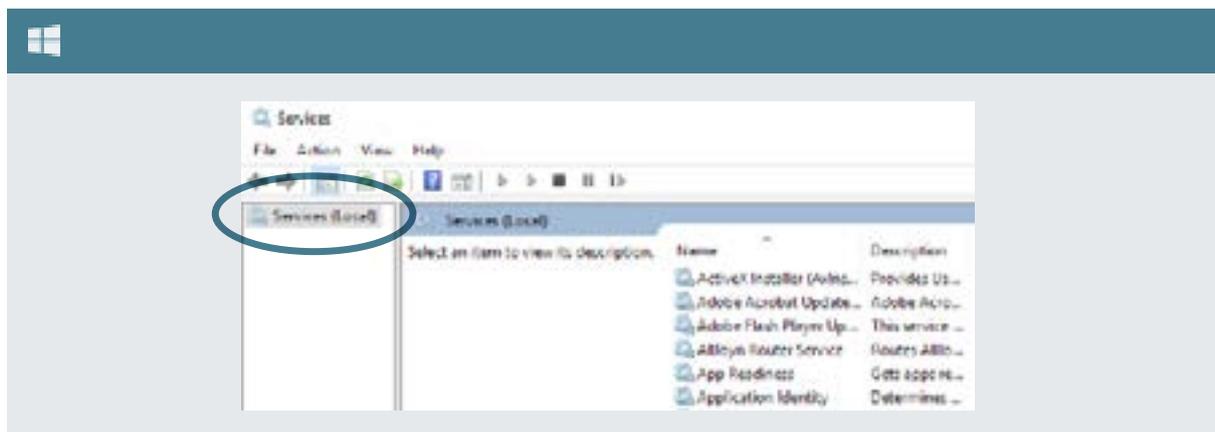
For Win10, the issues we need to look at before starting with the core part of the manual are divided into three areas; Services, Local Security Policy, and Settings.

“If you are using Windows HOME edition, some of these settings will not be available.”

SERVICES (SERVICES)

Services run in the background of your computer and determine what the computer can do. For example, to deny remote access to your computer, the service allowing remote access must be disabled. We will identify some key services that you must turn off (disable) to improve security.

For Win10, open the services window by entering Services into the search bar. In the window that will open (WIN10 • O2), find the services listed below by going through the list, and double-click on each one of them. In the new small window (WIN10 • O3) that opens, find Startup Type, and change it to Disabled and click OK or Apply.

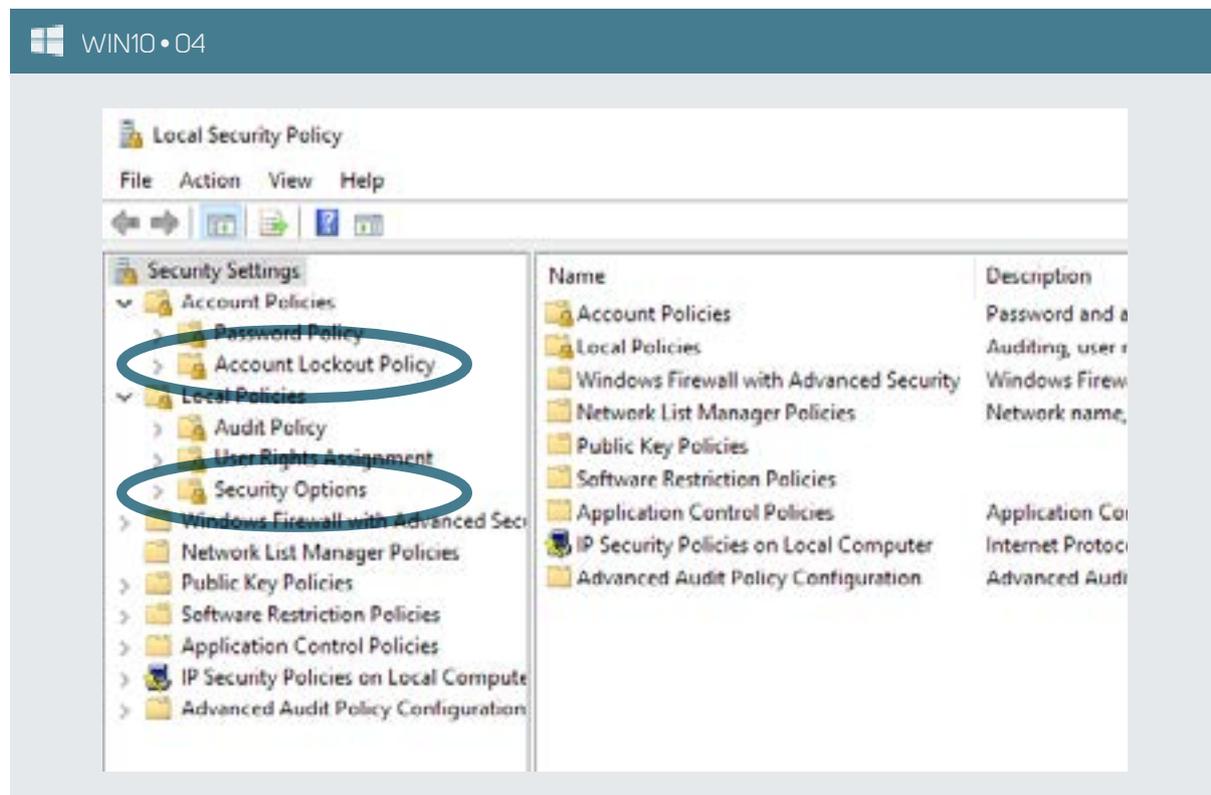


WIN10 • O3

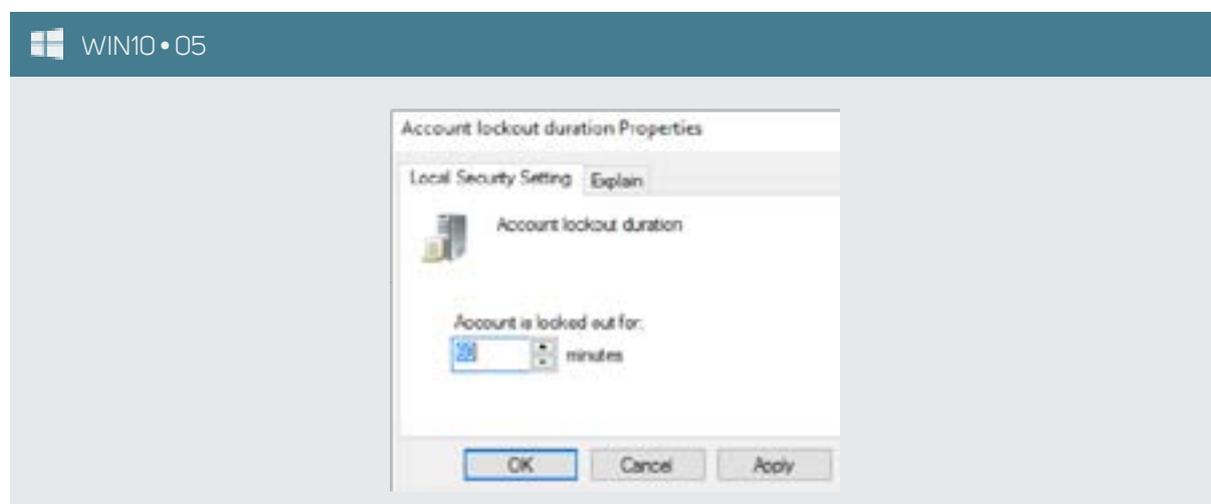
- Remote Desktop Configuration
- Remote Desktop services
- Remote Registry
- Routing and Remote Access
- UPnP Device host
- Volume Shadow Copy
- File History Service

SECURITY POLICY (LOCAL SECURITY POLICY)

Security policy area allows you to set a policy for security related issues. For example, you can set it so that if someone enters the wrong password to open your operating system 5 times in a row, the computer will freeze for 1 hour. Some security policy changes you should consider making are presented. Open the Local Security Policy window (WIN10 • 04) by writing in the search term Local Security Policy in your search bar.

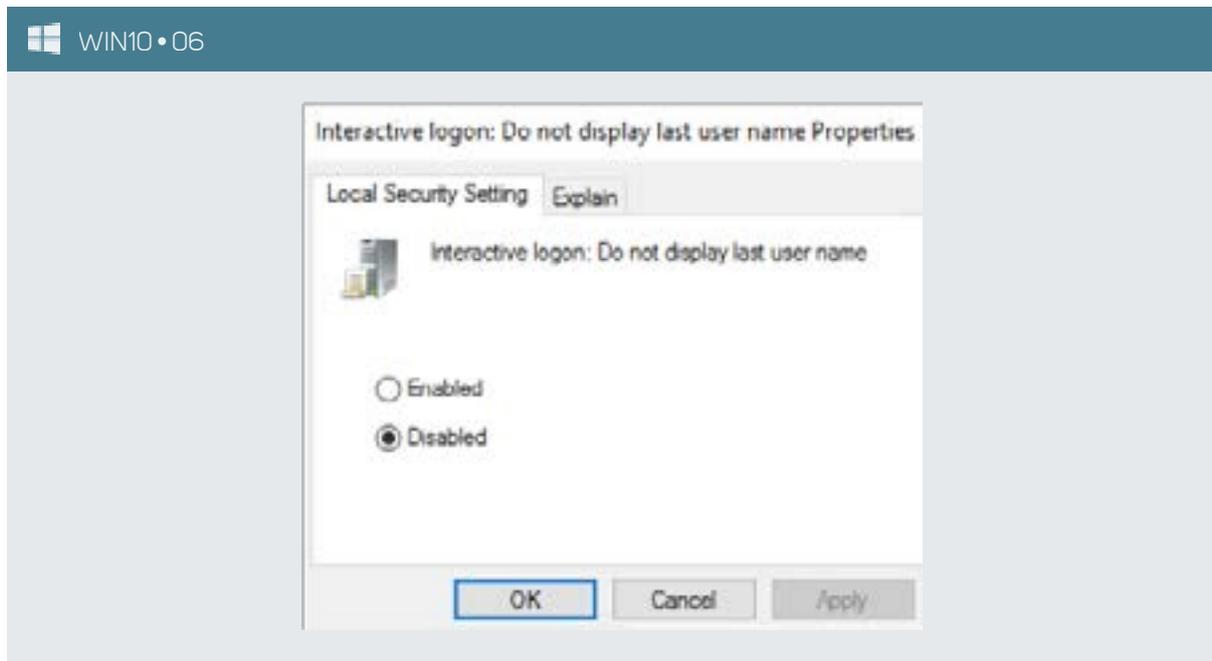


Click on Account Policies > then on Account Lockout Policy. Double-click Account lockout duration and in the new pop-up window (WIN10 • 05) select a time, say 1 hour and click Ok. Then double-click on Account lockout threshold and select 3 or 5. This means if the incorrect password is enter 3 or 5 times in a row, computer will lock for 1 hour or whatever time you set.



Note: Before the next step, make sure you know your username/login name for Win10, write down if needed, along with the email attached to your Win10 account. You will need to know your login/username to login after making this change.

Go to Local policies > Security Options. Double-click Interactive login: Do not display last user name and select Enabled. Double-click on Interactive login: Display user information when the session is locked and select Do not display username. (WIN10 • 06)



This means that your username will not be shown when the computer start, and to open Windows you will need to enter both your username and password. This adds security, as both need be known to open, not just your password.

Finally, and importantly, locate in same Local Security Policy window as above (Local policies > Security Options) Shutdown: Clear virtual memory pagefile and select Enable and click Ok. This issue is discussed under Chapter 7: Deleting information.

SETTINGS (SETTINGS)

These concern basic settings (WIN10 • 07), like whether to allow applications and programs to use location service or to allow the webcam or microphone to function. It also allows us to make some other changes to increase your security.

Updates (Windows Update settings). Click on Advanced Options, select Automatic updates, and Give me updates for other Microsoft products when I update Windows.

Windows Defender (Windows Defender). Turn on Real-time protection, Cloud-based protection. If you are using another, third-party Anti-Virus program Windows Defender will automatically be turned off and you can skip this setting.

Backup (Backup Settings). Make sure that Back up using File History is not selected.

Location ([Location privacy settings](#)). Ensure Location is turned off. While you are here, click Clear history on this device. Unlike for a smartphone, there is no need to allow your computer to use location.

Web camera ([Webcam privacy settings](#)). If you rarely use the webcam, turn off this service. If you use it often, leave it turned on, but scroll down and go over each and every program, and turn off access for everything except the program you use it for (for example Skype) (WIN10 • 08). The same way as with Webcam settings, where you can either turn off the service completely, or allow it, but then select which programs are allowed to use it, is also provided for many other aspects of the settings area, like for Microphone, Contacts, etc.

Microphone ([Microphone privacy settings](#)). If you rarely use the microphone, turn off this service. If you use it often, leave it turned on, but scroll down and go over each and every program, and turn off access for everything except the program you use it for (for example Skype).

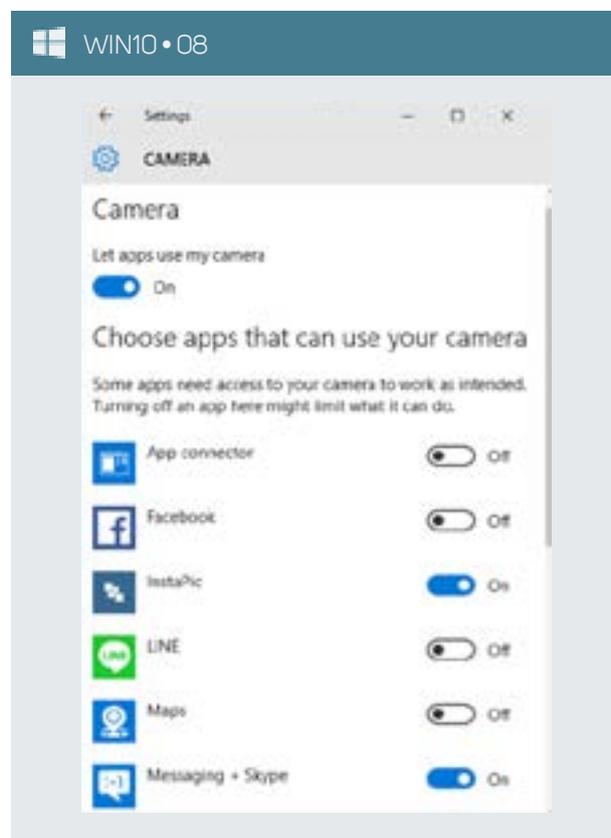
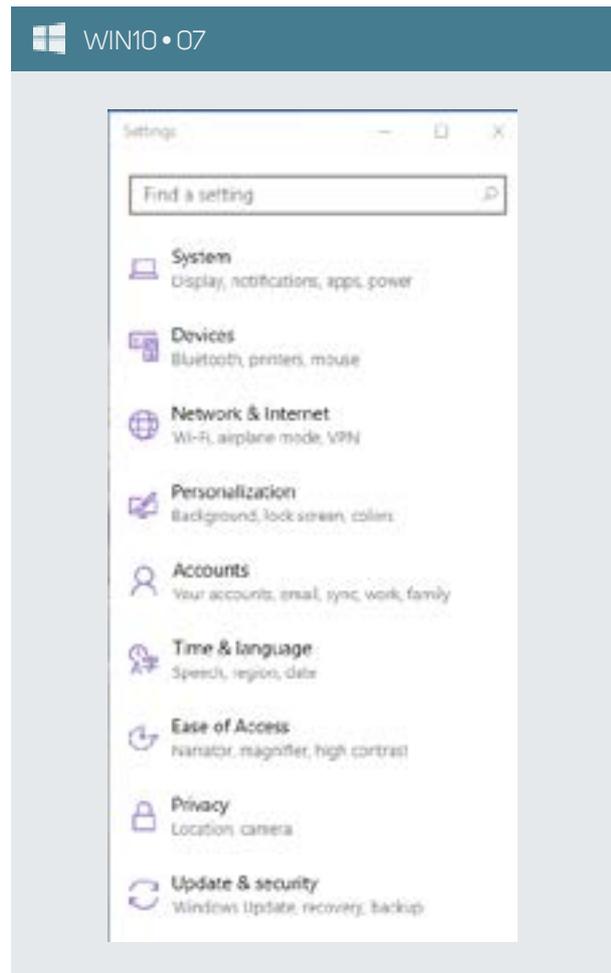
Cortana ([Cortana & Search settings](#)). Turn off all options. This is a Win10 search function, and it likes to collect a lot of information on what you do. Because of that, it's best to turn off this function.

Account ([Account info privacy settings](#)). Turn off Account Info.

Contacts ([Contacts privacy settings](#)). Review all the programs that have access to your Contacts, and turn off everything that is not needed or used.

Under the same area ([Privacy settings](#)), click on General, Calendar, Call History, Email, Messaging, Radios and Other Devices. Turn them all off, unless you know for sure you need to use them, which is unlikely.

Under Feedback & diagnostics ([feedback settings](#)) set Windows should ask for my feedback to Never and



Send your device data to Microsoft to Basic.

Review your sign-in options ([sign-in options](#)) and make sure password is needed to wake computer from sleep.

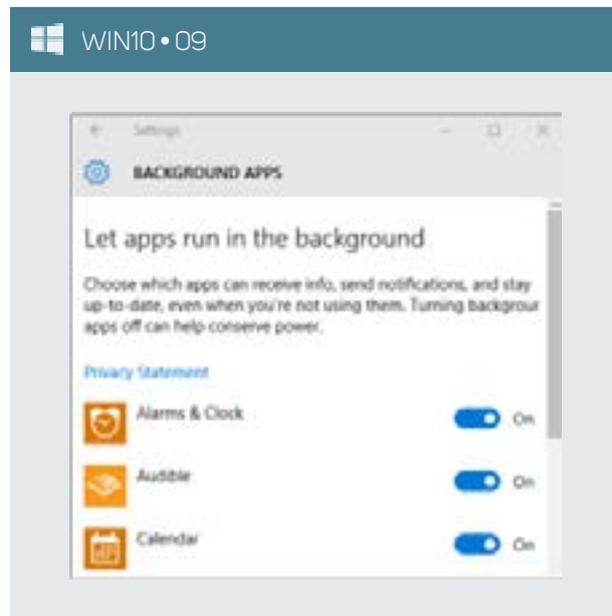
Check your start settings ([start settings](#)) and turn off Show most used apps, show recently added apps and show recently opened items in Jump Lists on Start or the taskbar.

Open your Bluetooth settings ([Bluetooth settings](#)) and turn off Bluetooth unless you use it. If you decide you need to use Bluetooth, click the link More Bluetooth options. In the new popup window, turn off Allow Bluetooth devices to find this PC. Then select/enable Alert me when a new Bluetooth device wants to connect.

Search [Allow remote access to your computer](#) and make sure it's not allowed (Remote Assistance and Remote Desktop).

Finally, at the bottom tab Background apps (WIN10 • 09), review which apps have permission to run in the background, and remove all of those that you do not want to run in background or those you do not use. Chat programs will need to run in the background if you use them on your computer (but you should avoid using chat programs on the computer).

Congratulations, the most boring part of this manual is now complete, and we can move on to the more interesting parts.



A NOTE ON PASSWORDS

We will begin this section by not talking about passwords. The greatest protection you have from police or criminals getting access to your accounts is for them not to know what to ask for. This is why your work browser must be set to delete all traces when you close it (Chapter 4: Getting Information). It's why you must use hidden encryption to store your work files (Chapter 5: Storing Information). And it's why CCleaner must be used to clear all traces of your work when you shut down your computer (Chapter 7: Deleting Information).

Simply put, if they don't know what services you use, they can't ask for the passwords for them. This is how you protect yourself. It's a core part of any secure behavior. Make sure people do not know what to ask for.

Passwords are sometimes called passphrases. Both names are equally bad, because they should be neither words nor phrases at all. To understand why, see below the three main ways to break them.

The first form is social engineering, to figure out what your password could be based on your person or background, like checking number combinations of your mother's birthday, the name of your pets or favorite sports, etc.

To protect against social engineering, never use names, number combinations based on birthdays or anniversaries from yourself, parents, friends etc.

The second form is a dictionary attack, where a computer can run through an entire dictionary in a matter of minutes, as well as combination of words. If you use words, even in a long sentence, it will be broken very quickly, and can be accomplished within hours.

To protect from a dictionary attack, your password should never contain words, even if strung together like a long sentence. This includes slang. This is especially important to avoid for Chinese and English words.

The third form is called a bruteforce attack, with a computer running millions of trials of combining various characters per minute. A bruteforce attack can break a short password very quickly, even if that password is random, especially if it is a PIN code using only 4 or 6 numbers.

To protect against a bruteforce attack, the password should not be too short, and should include all four different types of characters, as this will make it significantly harder to break any password with bruteforce.

Keyboards are designed by having 4 different classes of keys. These are capital letters (ABC), small letters (abc), numbers (123) and special characters (?!@).

A good password must contain at least one key from each group, and be at least 10 keys long. For sensitive accounts, you need to use an advanced password that follows all of these rules.

You can test the relative strength of different passphrases with online services such as How Secure is My Password. You should not type in your exact password but play around with examples. The website will tell you how secure your password is in terms of length it would take to crack it, from a matter of seconds to millions of years.

(<https://howsecureismypassword.net/> )

Also ensure that the passwords you use for work related security is not related to your passwords for personal services. There should be no similarity between passwords for work and those you use for



your online shopping accounts, for example. If you use Innoj-A7? for one personal account, do not use InnojH*ASH-B7? for a work account. It is too similar. Make sure that there is no similarity in style or structure between your different passwords.

We do not recommend you to use password manager software, like KeePass, unless you store the program and the database on a secret, encrypted USB. If you install a password manager program on your computer, a quick look at your computer will reveal that you use it, and police, criminals or others can easily force you to reveal the password to the password manager program, and with that they would then have access to every single password you have stored. We also do not recommend using and storing such a program inside your hidden encrypted space (which will be set up in Chapter 5: Storing Information). The reason for this is that if that hidden space is found and they can break into it, they would find it, and again, be able to access every password you have stored, and this would also show all services, emails, etc., that you use – exactly the kind of information you need to keep hidden.

RETINA OR FINGERPRINT RECOGNITION

Never use retina recognition, fingerprint, or other biometric information. It may seem like advanced technology but it is far less secure than a strong password, following the steps above.

Such biometric data once it is revealed, unlike passwords, it is impossible to change. If your password is compromised you can easily make a new one. You can't just get new eyes or fingerprints.

More importantly, if you have set retina display or a fingerprint to open your phone or decrypt a file, and you are detained, the police don't even need to press you to reveal your password. All they need to do is hold your phone up to your face or force your finger onto the sensor. You don't even need to be conscious. Do not use.

PART II

COMPUTER SECURITY

PART II CONCERNS YOUR COMPUTER, AND CONSISTS OF 5 CHAPTERS, ALONGSIDE SOME BRIEF INSERTS.

CHAPTER 3

Core Rules is perhaps the most important chapter as it shows how basic behavior and rules can protect you far better than technical solutions.

CHAPTER 4

Getting Information discusses internet connections, how to hide your IP address when surfing, use of browsers and how to get information.

CHAPTER 5

Storing Information is on how to store your data and files in a secure manner.

CHAPTER 6

Sharing Information concerns secure emailing, use of cloud storage and other issues related to how to share data and communicate securely with others.

CHAPTER 7

Deleting Information concerns a much misunderstood aspect of IT security, namely how to delete information in a proper fashion.

CHAPTER 3

CORE RULES



These basic rules on behavior will go a long way to protect your phone and computer against attacks. Security starts with behaviour, not technical solutions.

Much of Cybersecurity is not actually technical; it is about behavior. Because of this, a number of core rules will be presented below. Don't worry if you do not understand how to incorporate these into your behavior right away. We will discuss these issues in detail in the following relevant chapters. However, these rules can go a long way in terms of security for your computer and phone, and it would be good to pay extra attention when reading this brief chapter, so you can keep these things in mind as you study along with this manual.

After reading each brief core rule description, pause and ask yourself how it applies to your behavior or routine. They are not complicated but taking a moment to think about each core rule in detail will make sure you grasp how they interact with each other and your routines. Are you already following this advice in your online and offline behavior and if not think about what changes you need to make in order to follow these core rules to be more secure. If you have questions or doubts, circle them or write them down. They will likely be addressed by later chapters in this manual but if not we will also include resources for additional information.

KNOW YOUR THREATS

It is impossible to protect yourself against all the threats out there. Even if you tried it would be your new full time job, and still you wouldn't be 100 percent secure. Instead, you have to focus on the key threats. Be realistic. Because of the principle threats faced by journalists, lawyers, NGO workers and rights defenders in China, we have narrowed down the key threats, which serve as the basis for this manual. However, it goes a long way for you to know about the various ways technology can be used against you, which is why it's important to read and understand Chapter 1: Know Your Threats. It's also important for you to sit down and analyze your own situation, to decide what should be your focus. Understand the causes and consequences of the threats you face, where they come from and how to make them go away or at least make them less

severe. In Chapter 12: Preventive Security you should have followed the template to outline your threats and capabilities.

SIMPLIFY, SIMPLIFY, SIMPLIFY

Even for an expert knowing how to securely use many programs is harder than knowing how to securely use just a few. Every program you have comes with added security risks. The first thing you want to do is to look at all the programs you have on your computer and phone. Do you use them? If not, get rid of them. Are they needed? If not, get rid of them. These days a phone will quickly fill up with many different chat programs for example, but do you really use or need all of them. Probably not. Get rid of them. This has the added bonus of freeing up space and making your computer or phone work faster.

AVOID LOCAL COMPANIES AND PROGRAMS

Unlike foreign or at least western companies, services and programs, strong encryption is not standard in Chinese applications. The data Chinese, Vietnamese or many other countries' programs collect on you is not protected by the courts and is accessible by the state and police whenever they want. The data is also more easily accessible to criminals due to lack of encryption. Local programs have been proven to also collect a lot more information on their users than foreign equivalents (QQ being perhaps the worst of them all). They may very likely come with built in 'backdoors', giving the state direct access to your phone or computer, without you even knowing. Even one program, like WeChat, can threaten the security of your whole phone or computer. Be aware!

ZERO INBOX POLICY

Admittedly, the key threat against your email is not advanced hacking but police detaining you and forcing you to give them your password. If taken, chances are that the police will gain access to your email. Either you will eventually give them your password or, even if you don't, a coworker or friend may give the police access to their email, and with this the police can see any communication you have had with them. This is where a Zero Inbox Policy comes in handy, and is one of the most important tools for your safety that exists.

Assume that your email will be accessed if and when you are taken. The Zero Inbox Policy ensures that there is nothing for them to read. In short, keep your inbox (and other folders) empty. In 99 percent of times, this should not be a problem, as most emails do not need long-term storage. It cannot be stressed enough how important this is. Likewise, ensure that your coworkers or friends do the same. This is further discussed in Chapter 6: Sharing Information.

We will also introduce you to a secure, highly encrypted webmail service that has an autodestruct function, much like the Telegram chat program and Signal SMS program, also addressed later.

NO REPLY AGREEMENT

A No Reply Agreement simply extends beyond the Zero Inbox Policy. If indeed your email is accessed, by simply waiting they can learn a great deal about your communications, because of the way we often handle email. When we communicate, we will often click 'reply' to an existing email, instead of writing a new one. With this, the earlier communication is included in the same email. Often times this back and forth use of reply can go on for a long time, and because of that, one short new email can include a long list of prior emails. This means if your email is compromised, the person responsible can simply wait for someone to email you using

the reply function, and see your prior communication.

As such, when you respond in email to your coworker or friends, avoid using the Reply function, or if you do, make sure to delete the original text. This ensures that after your detention, as police are accessing your emails, any new emails that arrive will contain as little back information as possible, and they will not be able to counter your Zero Inbox Policy by simply reading the text in any emails to you using the reply function. More information on separating work and personal emails and additional secure email habits will be covered in Chapter 6: Sharing Information. Talk to your coworkers or friends you communicate with most and agree to avoid the reply function.

SECURING THE BASICS

You wouldn't spend 10,000 RMB on an advanced security door and lock and then leave the windows to your house wide open would you? The same goes for your computer and phone. Unfortunately, your phone and computer comes with a number of settings, and most of the time these settings are not secure. As such, before you start securing your devices with additional technical solutions and improved behavior, you need to secure these basics. This can be tedious and involve following step-by-step instructions on a variety of small issues. However, it will go a long way to helping you secure your devices and thus your own safety. These different issues are addressed in the Chapter 3: Securing Your Computer and Chapter 10: Setting Up Your Phone and we recommend you do these things after finishing this chapter.

UPDATE, UPDATE, UPDATE

The importance of regular updates cannot be overemphasized and yet it is one of the most frequently overlooked causes of security breach. Do not make this mistake. Make sure your operating system (OS) is set to automatically update. Make sure your browser is set to automatically update. The same goes for any programs you use related to your work. You might find it annoying to pause and wait for occasional updates, but it is key to protecting your computer and phone. Would you rather wait a few minutes for an update or a few months in detention? Programs, OS and services become safer every day as new 'security holes' are plugged, and new threats are discovered and countered, and only by allowing automatic updates will you benefit from this. Out of date programs and applications are incredibly vulnerable to malware and other attacks. Updating regularly allows you to avoid these unnecessary risks.

EMERGENCY PLANS

By the time the police have your friends or coworkers in custody, or confiscated their computer, it's already too late. In fact, if you waited until then to start talking with coworkers about how to deal with removing sensitive or incriminating material, it could be considered attempting to destroy evidence and used against you. You must be prepared in advance for these situations, and you must know what you are supposed to do before, when, and after it happens. Also, you must know what your coworkers and friends will do. **YOU NEED A PLAN.** The only way to achieve this is to talk about it beforehand, and make an agreement on how you and others are supposed to act should someone be taken, or someone's computer or phone be confiscated. Do you all do a factory reset on your phone? Do you double-check to make sure your inbox is empty? Do you all change passwords, or maybe you all re-format your computers? Whatever you decide, what is important is that you and your friends do the same thing and that you all know what the others will do.

This is called having and following a 'security protocol.' If you personally do a bunch of things to stay secure,

but one coworker does not, it could render your attempts meaningless and put many people at risk. Sit down with your coworkers and talk about this. Remember, if your network includes multiple groups of coworkers or fellow rights defenders that work on different issues and they don't all know each other, or some are involved in more sensitive activities than others, you can always create different emergency plans with your different groups, in fact this is advised. Making emergency plans and having a 'security protocol' that everyone knows and is going to follow is likely to be needed, and is not some far reaching unlikely thing. This and related issues are discussed in Chapter 12: Preventive Security.

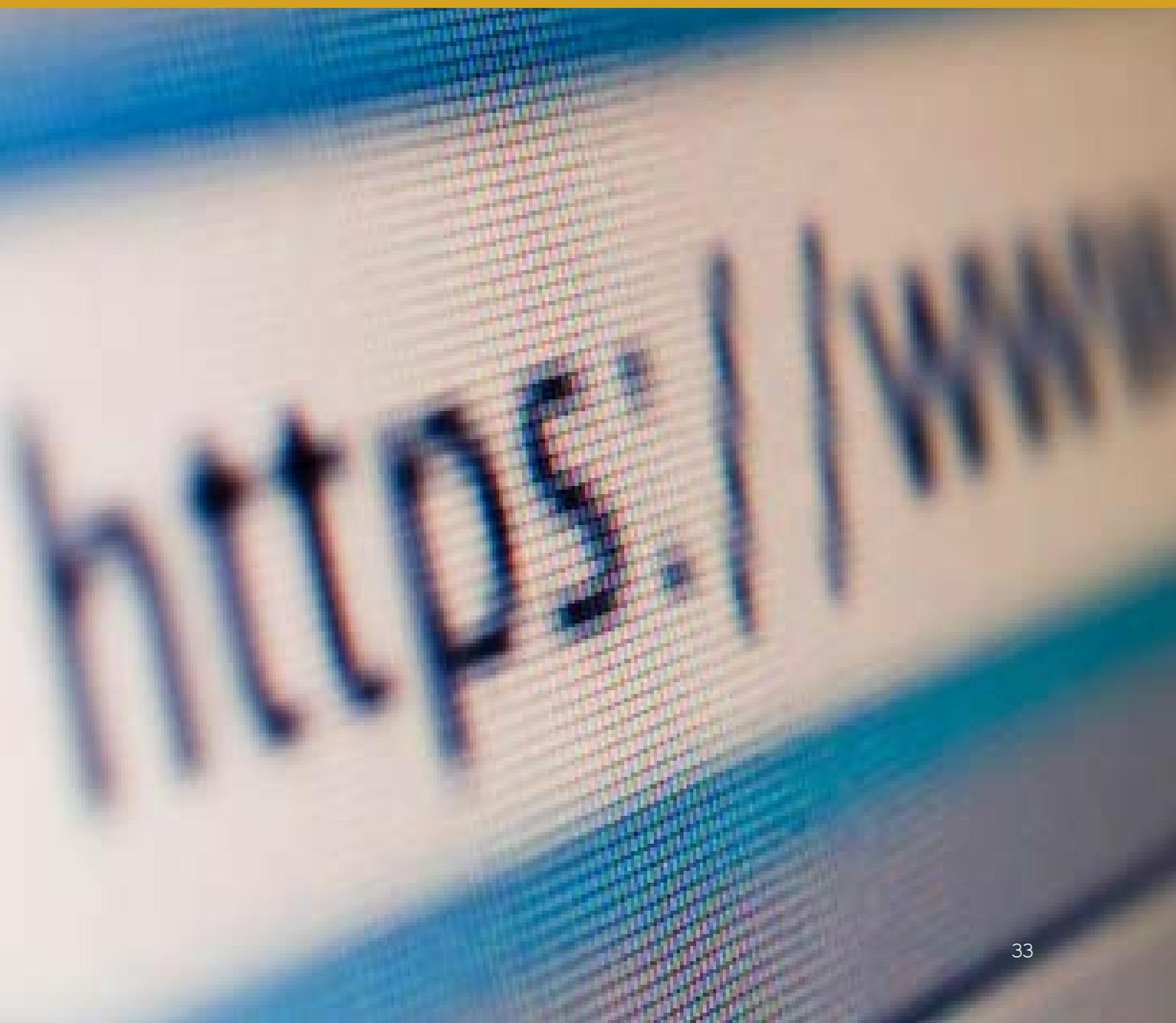
Before continuing to the next chapter, make sure you have implemented the instructions in Chapter 2: Preparing Your Computer. Securing the basics before continuing is necessary to get the most out of the more advanced technical and behavioral security steps that will follow.

END OF CHAPTER QUESTIONS

- What is a zero inbox policy and why does it matter?
- Why is it important to maintain a no reply agreement?
- What are the risks of failing to regularly update security software?
- What is an emergency plan?
- What steps will you take to design an emergency plan?
- Why do you need to simplify and limit the amount of programs you use?

PRACTICAL DIGITAL PROTECTION

CHAPTER 4 GETTING INFORMATION



This chapter will teach you how to safely get information. It will discuss both the method with which you seek and get information, your browser, but also the internet connection that you use when using your browser. For security, you need to consider both the browser itself, as well as the connection it uses to get the information. Knowing how to secure your connection will also allow you to overcome censorship limitations.

OVERVIEW AND BEHAVIOR

This chapter will go over the use of internet connections and browsers. The later chapters on mobile devices will discuss apps. The first part of the chapter is the practical part about setting up your browser as well as how to behave when using a browser. The second part concerns internet connections in general, and is more about understanding how connections work, and how to connect to the Internet in a safer manner.

The later chapters in Part III on mobile devices will discuss use of Apps and mobile devices in general.

Your eyes and ears to the internet is likely to be your browser. Most of you will also use your browser for the purposes of emailing. With so much of your work related to your browser, it becomes important to secure it.

When you use a browser, there are two things that happen. The websites you visit will collect information about you, but at the same time your computer will also collect information on what you do with your browser. It does this by collecting cookies, LSOs, passwords you enter, your browsing history, and more. To function well, most websites use scripts (JavaScript programming), and through this, your browser and computer is vulnerable to get web bugs, viruses that spread to your computer through your browser. Both these issue need be dealt with. Luckily, there are ways to do this. The first step however is as often behavioral:

DUAL BROWSER STRATEGY

Ideally we would advise you to use one browser set to automatically delete everything each time you close it. However, considering how much we use browsers for personal use, we also realize that if you have to log in to each and every service every time, it will be too inefficient, and you will not use it. As such, we recommend

a dual browser strategy. Select one browser for personal internet browsing and another for all work use. For work you should always use Firefox. It's not the fastest browser but allows significant tweaking, with important security extensions/add-ons. If you do not have Firefox, download and install it now from [Firefox.com](https://www.firefox.com) .

For personal use, we recommend a fast browser such as Chrome or Opera. Dual browsers will mean that your personal use can continue as before without being slowed down by add-ons or extensions but your work-related internet behavior will be significantly safer.

Once decided, stick with it. Use Firefox for all work related browsing, from research, emailing and anything else, and your other browser for all personal browsing. Do not install more than two browsers, select your two browsers and stick with them. The Technical Solution on Firefox and extensions further below will show you the details on how to use Firefox in a safe manner.

SAVING FILES IN THE RIGHT PLACE

The insert on Firefox later will show you how to do this. You need to understand why. The default download/save folder of your browser is a major security risk that few people take into account.

If no change is done, any attachment or document you download through your browser will be stored on the Operating System (OS) hard drive. Why is this a problem? As Chapter 5: Storing Information, and Chapter 7: Deleting Information, will show, actually deleting information is really difficult. The details on this will come later. For now, its important that you use your browser and downloading in such a way that you are in control where the new files are stored.

The best way to manage this is to create a folder in your encrypted hard drive (which we will set up in Chapter 5: Storing Information). However, if you set your download path to your encrypted hard drive, and you then try to download something without having decrypted your encrypted hard drive, it will instead be saved to the default area without telling you. As such, in the insert below, we will show you how to select Always ask me where to save files. This means that each time you download anything, it will ask you where to save it. Make sure to always save in both a) the same place, and b) your encrypted hard drive.

Do not casually save new documents to your desktop!

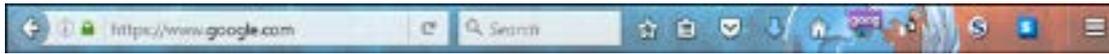
INTERNET CONNECTIONS, VPNS AND TOR

HTTP VS HTTPS

These days, most services that require login use encryption on the internet connection between you and that service, like Facebook, Gmail, banks etc. This is not common for Chinese services, and even if they do, it's of little help, as these companies will record your information and provide it to the state if asked. There is a very easy way to know if your connection to a site is encrypted. All you have to do is look at the address field in your browser (below).

Unencrypted connections say HTTP (<http://www...>) at the start of the URL. Encrypted connections say HTTPS (<https://www...>). Go to Gmail, Twitter or Facebook and test and see. By using the HTTPS Everywhere add-on in

Firefox, the browser will automatically use https if possible with a service.



YOUR INTERNET: YOUR ROUTER

It's safe to say that your access to internet is through wireless connections, whether at home, in your office, or working in a café. Because of this, you need to have some basic understanding of how a wireless router works.

To access your router, you will need a username and password. These are usually written on a note on the back or bottom of the router. These are the same for almost all routers, usually "admin" and "password". Even if different, every single router of that brand or model will have the same username and password, so it's very easy to find out. With this information, any outsider, like a criminal or police or others, can enter your router. If they can enter the router, which controls your internet, they can easily install programs to log all you do, or even block your internet. The vast majority of people never enter their router to change their username and password. Most router access is by opening a browser and writing in the IP address of the router, usually 192.168.0.1. The address will also be printed on the router itself. Using this, you can enter your router and change the username and password.

Another key issue to consider is, when using wireless internet, that the wireless signal needs to be encrypted, or else everything transmitted can be read by anyone nearby. If not encrypted, anyone can connect and use your wireless signal, and also log everything that is done on that connection. Your wireless signal will have a name, which is the name you usually connect to (called SSID). You know encryption is used on a wireless connection if it requires a password to connect. No password means no encryption.

Once you entered your router, you can change the name of your network (SSID), and also select to encrypt the signal. The standard encryption used on Wi-Fi routers these days is called WPA2. Older ones are called WEP. Do not use these. To enable encrypted, you then have to decide on a password.

Hence, there is a username and password to enter the router. Then, there is a name and password for the actual wireless signal you use. These are not the same. If you need guidance on figuring out how to make these changes in your router, simply google your router name and model number, and there will be plenty of help. Even though the interface for your router might look complicated, you only need change a few things, and it's a lot easier than it first looks.

YOUR INTERNET: YOUR ISP, IP ADDRESS AND MAC

In many places, chances are you use an internet connection provided by one of the few, state-controlled, Internet Service Providers (ISP), or if on your phone, one of the Phone companies. This poses a great risk, because many steps you take for security can be undone by this, because the ones providing the internet use for you, will also automatically log everything that is done with that connection. Different providers keep such information for different amount of times, but they all have at least temporary access to your internet use.

When you connect to the internet, your router (the box in your home or office that handles the internet traffic)

communicates and uses the internet service provider (ISP) to connect you to the wider internet. Basically, your router at home connects to the internet first through the servers of the ISP, and from there out onto the wider internet. It is through your ISP that censorship is applied, as they will block websites and web content.

The tracking of you, whether by the ISP that handles your connection, or the websites you visit or services that your computer or phone connects to, is done through your IP address and your MAC address.

Your IP address is your internet connection's address, and can be easily identified, and thus tracked back to you. If you connect through Wireless connections your IP will change (dynamic) but your ISP will always know which IP address have been assigned to whose internet connection at what time.

Your device or computer will also have a MAC address. Every device with a connection will have a MAC address, and this unique MAC address is set for the physical hardware itself. The MAC address is set when the hardware is manufactured, and the MAC looks like this: 00:0a:95:9d:68:16. When you are connected to the Internet however the MAC address is not shared, so you need not spend too much time thinking about it, but your IP address however could lead to problems for you.

In Win10 there is a settings option to enable Random hardware addresses (MAC), and if you have the option, do turn it on (WIN - 10). If you notice any problems with your connection after having it turned on, restart your computer. If the problem persist, turn it off.

Luckily, there are some rather simple ways to avoid having your ISP monitoring your activities, or having websites track your real IP address. Those solutions are called VPN and TOR, and an insert on VPNs and TOR is provided further below. In short, a VPN or TOR will bypass the ISP, connecting you directly to servers outside of Vietnam, and will in many cases also encrypt you traffic, meaning your ISP cannot track your Internet usage. Using a VPN or TOR is essential for your security and privacy.



VPN'S AND TOR

Using a VPN (Virtual Private Network) not only secures your information from being easily accessed by the ISP because it encrypts the traffic/connection, but also circumvents the ISP's censorship. It also makes it harder for websites you visit to record your true IP address. All in all, it's recommended to always use a VPN on

your computer, and have it set to start automatically when you start your computer. There is no reason to use internet without a VPN turned on.

Some VPNs come with a kill switch, meaning it automatically cuts off internet if the VPN stops working (to prevent your real IP from being shown to the website or service you were using when the VPN connection dropped). It is recommended to use this. These days, many VPNs are powerful, and you will not notice any difference in speed. It might cost a little bit of money to get a good one, but it's one of the most important investments you can make.

A VPN connects your computer/router directly to a server outside of Vietnam (and you can choose which ones), bypassing the ISP by creating what is called a 'tunnel'. The websites you visit will see the IP address of the server you are connected to (the VPNs server), and not your own computer's IP address. Likewise, your ISP will not be directing your internet traffic, and therefore cannot record what you do, or block websites you want to access. A VPN basically skips the ISP. This means that although you are physically in Vietnam it can make it look like your computer is in the United States or Australia or another third country where censorship and web restrictions won't apply to your online activities.

[Astrill.com](https://www.astrill.com)  is a strong VPN provider with extra security features, and servers all over the world. VyprVPN and ExpressVPN are other popular choices. Searching online will also show you comparisons of the best VPNs available. For an up to date list of well-functioning VPNs, simply Google and you will find lots of relevant information and comparisons.

Using VPN is strong protection of your IP address, but it is not entirely safe, and with resources applied outsiders could potentially track it back to you. For truly sensitive activities online, you need to use TOR.

TOR is called The Onion Router. Unlike a VPN, when using TOR, a free service, it connects you through a long line of different servers all over the world before coming to the website you are looking for. It's the safest means of communication available. It's very reliable, but also very slow. Forget about trying to watch streaming videos on TOR. If you ever need to do something sensitive, that you think could be used against you if noticed, use TOR. It's easy to setup on both computer and phones.

It's called onion router because instead of using one server, like a VPN, it jumps through many different servers, up to 20, like peeling back the layers of an onion, before connecting you to the content you're visiting. Because it uses many servers, it becomes nearly impossible to track the internet use back to your IP.

DUCKGOGO.COM AND SAFE SURFING

DuckGoGo is a search engine, much like Google. Unlike other search engines, DuckGoGo does not customize search results based on your location, prior history, and keeps no data on those using it. It's a safer way to surf, where no data is collected over time. That means no ads, and no customized ads based on prior searches, location and more. DuckGoGo uses an English-only but very basic interface, so language will not be an issue.

If you use TOR/TOR browser and DuckGoGo together it means little to no traces of your surfing exist, neither with you ISP nor at the website you are visiting. If needed to search for information that could, if monitored and stored, pose a problem for you, consider using DuckGoGo while accessing with the TOR browser. For maximum security, use the TOR browser from a USB stick, to limit traces stores on your computer.

When it comes to surfing, the security levels can be summarized as:

TOR offer best security, higher than while using a VPN, but being on a VPN is still much safer than connecting 'normally'. In terms of choosing browser, using the TOR browser on a USB is your safest choice. Using Firefox properly configured is still much safer and better than using a 'normal' browser setup.

KEY TAKEAWAYS

- Have you setup a dual browser system and made the necessary changes to Firefox (or other designated work browser)?
- Do you understand how VPNs and TOR work, and why it can help you, beyond just overcoming censorship?
- Make sure to use your VPN as much as possible, preferably keep it always on, and learn how to use TOR and the TOR browser for your most sensitive activities online.

ZERO-INBOX, AUTODESTRUCT SAVING THE DAY

A lawyer based in Shanghai made a name for himself as a rights defense lawyer in the late 2000s, having not only defended politically sensitive people but also managed to work in such a way as to get real results. In return for his growing prominence, harassment and threats increased, and he decided that for the sake of his family, he would have to change tactics. Being firmly committed to the rule of law and justice, he started taking on less and less cases, and instead started an informal NGO to offer training, assistance, and other forms of help for other rights defense lawyers around the country, especially younger fledgling lawyers. At the same time, he also slowly started learning more about cybersecurity, to make sure that his information remained secure and out of the wrong hands.

As the widened attack on lawyers and all those related to them started heating up, he was naturally concerned that he might be targeted, but as he had since long stopped taking on active cases, he assumed any such targeting would be limited to trying to force information from him about the “China Human Rights Lawyers” group. This group, in reality, is simply an online group of mostly lawyers sharing information, but in the eyes of the government it is an organized opposition, and a key target in their crackdown. He was right, and in 2015 he became a target. But the government didn’t just go after him. They went after his assistant and two other lawyers he worked with to provide training. He was mistaken in thinking that the police were solely interested in this online group. They were equally concerned about his work with the small NGO he had started to provide training and legal assistance.

He quickly figured that not having served as a lawyer in sensitive cases for a long time, he could deflect much knowledge about the loose online group, and wouldn’t be at risk of incriminating anyone. However, he feared, and still does, that material that could provide proof of his having organized trainings for other lawyers could be used against him. It didn’t matter that training lawyers is perfectly legal. In the end, he spent 17 days in detention, but was threatened with being moved into ‘residential surveillance at a designated location’ where he could be kept for 6 months, regardless of any actual suspicion of crime. Even after he was released, he continues to live under fear, and has since stopped all his earlier work with small NGO.

He claims that two things largely saved him during his detention and interrogation. He had ensured that all his work email accounts were kept empty and that his work communications were either only carried out through secure chat services with autodestruct or that he himself regularly deleted chat logs.

Police initially justified his detention with the material they had found on his assistant’s phone, who had quickly given up his password upon being threatened. The chat logs, which the assistant had failed to completely delete, made it clear that they had indeed organized training and supported rights defenders, which they police claimed constituted a crime.

The lawyer made the mistake of using the Tutanota email app on his phone. Even though he refused to give out his password to the police, they now knew he used this encrypted email provider. The police pressured his assistant to give out his password. They hoped to get to the lawyer through his assistant but, although he had forgotten to delete the chat records on his phone the assistant had followed a zero inbox policy. This way, there wasn't anything to use against them when the police opened his account.

It seems his two occasional partners had not been so strict in keeping their chat programs or emails empty. He still doesn't know exactly how much or what the police got from going through his partner's accounts, but it was enough for them to know the extent of his work, even though they never managed to get the full details. This was enough for the police to threaten him with far greater punishment, even if there were no actual grounds for prosecution, and the reason he is too fearful to continue his work.

TECHNICAL SOLUTION: FIREFOX AND EXTENSIONS

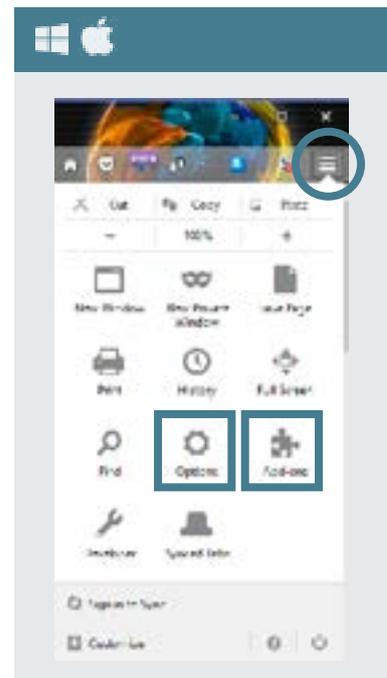
If you do not have Firefox, download and install it now from Firefox.com. After installing it, either on your Hard drive, or if you prefer, straight to a USB, your next step is to download and install a number of add-ons or extensions.

ADD-ONS/EXTENSIONS

You will find the add-ons area by clicking the Settings button on Firefox (WIN + OSX 11) and selecting Add-ons. From here you can search for add-ons to add and find a tab that lists all your installed add-ons (this tab is called Extensions). From there you can also find Options for each add-on.

Find and install the following add-ons,

- RefControl,
- NoScript,
- BetterPrivacy,
- HTTPS Everywhere, and
- Keyscrambler.



 **Refcontrol.** When you visit a webpage, the website will see where you are coming from. That is, if you are on google, and then go to Facebook, Facebook will be told that you arrived at their page from Google. This is a referrer, and is used to analyze how people end up on websites. Installing RefControl allows you to stop this by a few simple clicks. After install, click on Options and select Forge or Block at bottom of window that says Default for sites not listed.

 **NoScript.** This program automatically blocks Javascript from running in your browser. This is very important because many viruses are unknowingly transmitted through infected scripts. This disables movable graphics, automatic video playback, and more. It places an icon in your browser, and if you want to allow a website you trust to run scripts, and often you need to allow it for full functionality, you simply click the icon and tell it to allow. If you are on a website that doesn't load or work properly, it's because some scripts are blocked, and in that case you need to allow it. No further changes are needed for NoScript.

 **BetterPrivacy.** By installing this add-on you are given more options of automatic data deletion from your browser when you close it. Only by installing this add-on will you have the option to properly delete LSOs, a new type of hard to get rid of cookie. After install click on Options, then select the tab Options & Help. Select

Delete Flash cookies on Firefox exit. Also select Also delete Flashplayer default cookie and On cookie deletion also delete empty cookie folders.



HTTPS Everywhere. Some websites encrypt communication between your computer and the website, such as banks, some email providers, some social media and others. It adds a layer of security. Although more websites are providing HTTPS it is not universal and some that allow it do not do it automatically. This add-on automatically enables HTTPS encryption on those websites you visit that support it. Once downloaded you will see the icon in your Firefox toolbar. Click Enable HTTPS Everywhere and it will work automatically.

Unlike the add-ons above, this one below cannot be installed through the add-on area. Instead, go to download.com and search for KeyScrambler. Select to download it and install it like a normal program. The computer will need to be restarted before the program starts working.



KeyScrambler is a small program that encrypts your keystrokes when entering usernames and passwords in your browser. Advanced hacking can place a keylogger program on your computer. This keylogger then records all your keystrokes, and with that the attacker can get access to everything you type, including usernames and passwords. By encrypting the login and password keystrokes automatically, this tiny program will secure you from this line of attack.

After installing these, please spend some time in the Firefox extension/add-on shop and look around to familiarize yourself with what is out there, and what add-ons exist. You might find other useful add-ons suitable for security or efficiency and productivity. You can also Google Best Security Add-ons for Firefox or similar, to see if there are other good add-ons for you.

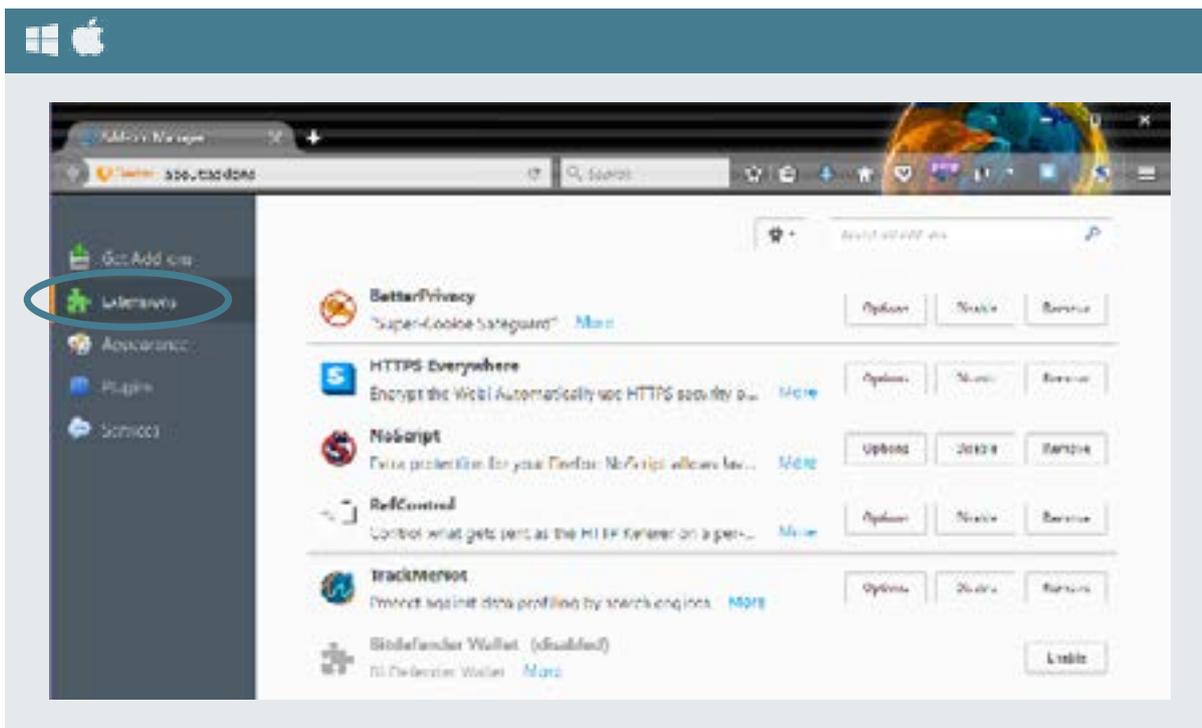
You are now half-way to secure your work browser. Next up we need to make some quick changes to the settings.

SETTINGS AND OPTIONS

After installing Firefox and the add-ons, it's time to take a look at the settings for the browser, to make sure it's configured to be safe. Click on the settings button and then Options (S-W/O1 above). For OSX, you will need to open Preferences (under the Firefox icon at the top of the window). Inside the Options area, there are several tabs. Under each tab mentioned here, some changes should be made.

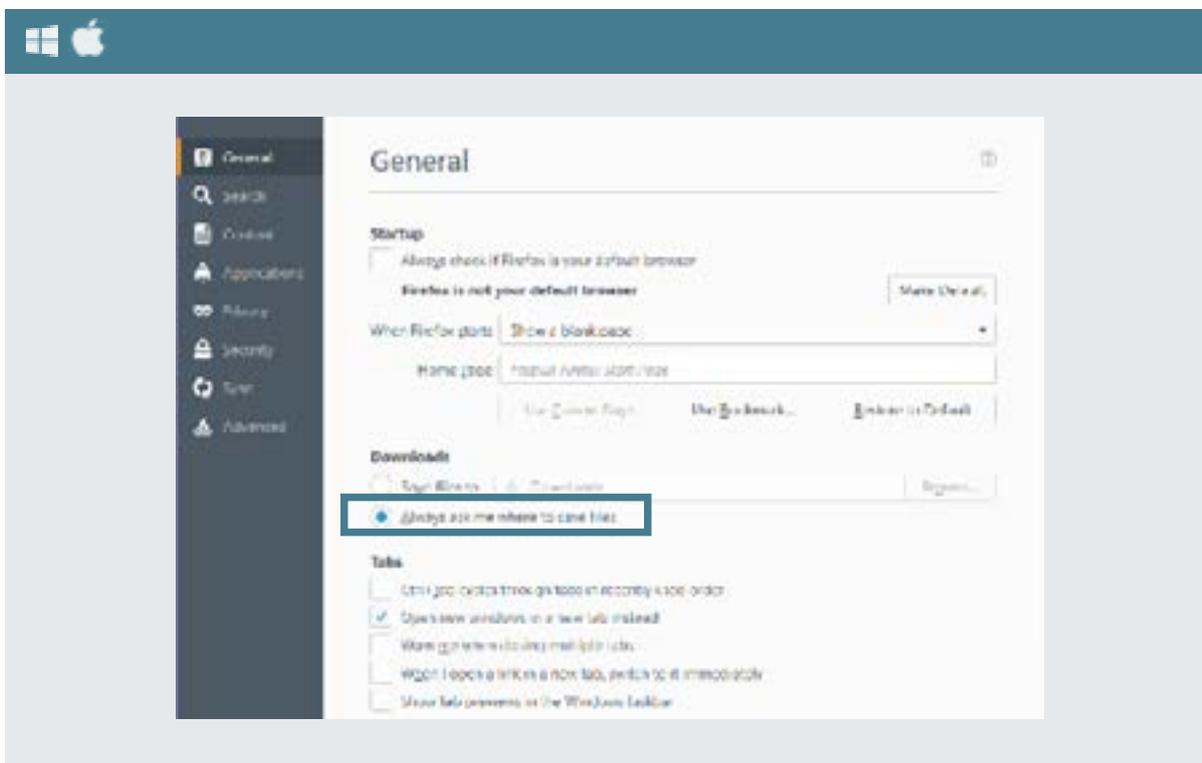
EXTENSIONS

Start first with checking out the options for the different extensions you have installed (WIN + OSX - 12). Most come pre-configured, and require no changes, but as always, its important for you to look around anyway to have a general idea of the options available.



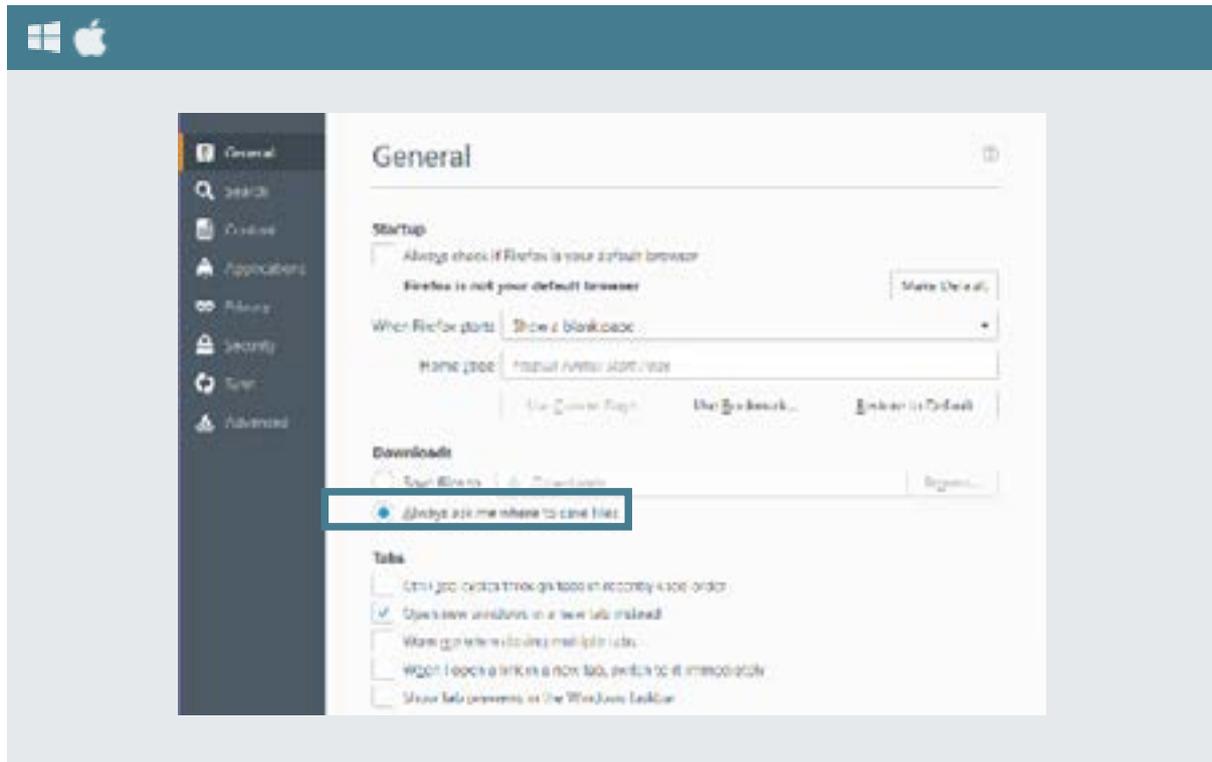
GENERAL

Select Always ask me where to save files (WIN + OSX 13).



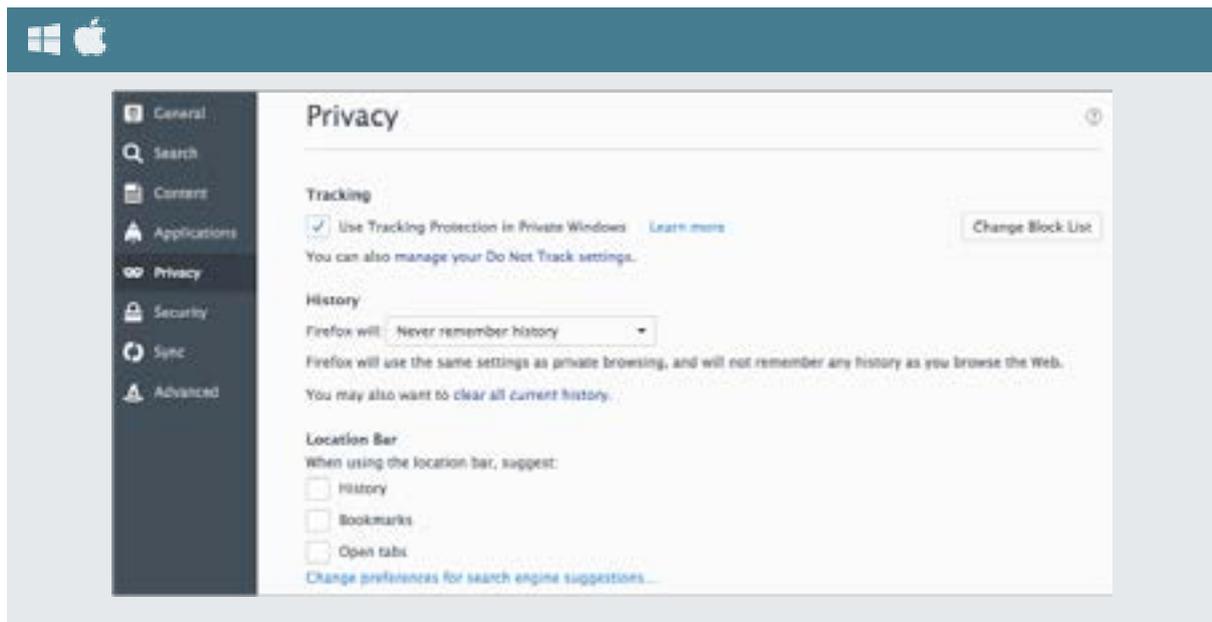
SEARCH

Make sure Provide search suggestions is de-selected (WIN + OSX 14).



PRIVACY

Enable Use Tracking Protection in Private Window. Under History, select Never Remember History. Under Location Bar, make sure nothing is selected (WIN + OSX 15).



SECURITY

Under the Security tab (WIN + OSX 16), select all three boxes under General, and make sure to uncheck the two boxes under Logins (Remember logins for sites and Use a master password. While you are here, click the Saved Logins button and see if anything is stored. If it is, delete it.

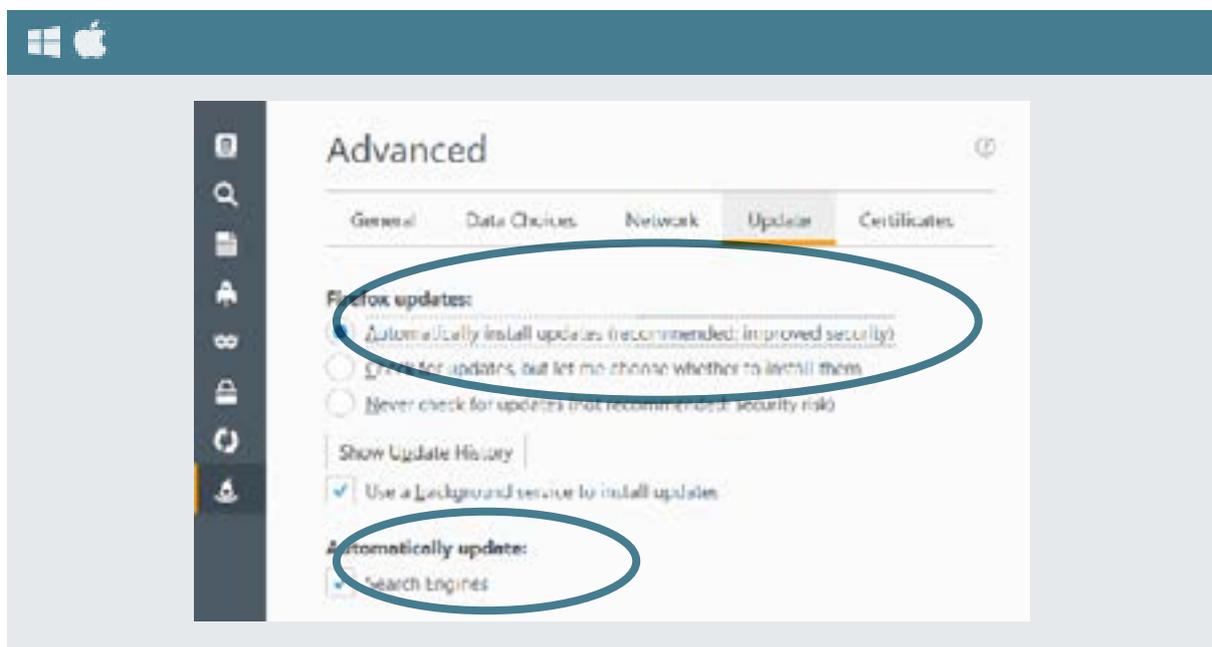


SYNC

Do not use sync, and do not tie Firefox to any email account or similar. Do not sign into Firefox with your email account.

ADVANCED

Under Data choices, make sure all three boxes are unchecked. Under Network, select Override automatic cache management, and write in 50. Finally, under the Update tab select Automatically install updates. Make sure you also selected automatically update Search Engines (WIN + OSX 17).



TECHNICAL SOLUTION: TOR

You can install the TOR browser (a program/application) either on your computer, or straight to a USB. It's simple and works automatically when you start the TOR browser. With this, only that specific browser uses TOR, nothing else on your computer. If you want your entire computer to use TOR, you have to download and install the program instead. If you do this, all connections will be covered by TOR, such as other browsers, background connection data, Skype, etc.

Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is convenient, e.g. the Desktop or a USB flash drive.

Stable Tor Browser			
Language	Microsoft Windows (6.0.5)	Mac OS X (6.0.5)	Linux (6.0.5)
English (en-US)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
العربية (ar)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Deutsch (de)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Español (es-ES)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
فارسی (fa)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Français (fr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Italiano (it)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
日本語 (ja)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Korean (ko)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Nederlands (nl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Polski (pl)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Português (pt-PT)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Русский (ru)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Türkçe (tr)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Vietnamese (vi)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
简体字 (zh-CN)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)

For the TOR browser, go to: <https://www.torproject.org/projects/torbrowser.html.en> and select the browser you will use, depending on your OS and language. TOR also produces mobile Apps.

Download the file to the location you want to install it, either a USB or your hidden encrypted hard drive. If you have no hidden encrypted hard drive or storage yet, return to this chapter after having set up one up according to Chapter 5: Storing Information.

Because the importance, it's worth reminding you. If you use TOR Browser, only that browser's traffic goes through TOR, not other data transmissions on your computer!

TOR ON USB

TOR can also be installed as a USB program with the same built-in browser. With this, you just connect the USB to any computer and start the special browser, which connects through TOR. Because it runs on a USB, it leaves little traces of your internet use on the computer you use. Consider buying a small USB, and install TOR on this USB. Make sure you never use this card for anything else, like storing files etc. The install process is the same as above, but instead save the downloaded file to your USB and then install it on the USB. The browser is the same even if installed on USB, and you should make the same changes to the browser settings as mentioned above. As before, make sure to enter the Settings area of the browser before you start using it and make the relevant selections as mentioned about the Firefox browser.

THE DARK NET

The internet as you know it most resembles an iceberg, which is, only 10% or so of it is visible. Google and other search engines uses indexing to present information from the web for you, and only the indexed part of the internet, which is a very small part, can be found using Google or other search engines.

The rest is usually called the Deep Web. There is nothing ominous about (most of) this, but constitutes all the data held by universities, research institutes, corporations, governments etc., which is usually inside an intranet, and this data you cannot be found unless you get into that intranet. Similarly, using privacy settings, most of the information on your social media, for example your Facebook account, is also part of the Deep Web because this data cannot be found and viewed by using a search engine.

Inside the Deep Web is an area often called the Dark Net. Even if given an address to a Dark Net website your browser will not be able to open it. All Dark Net websites use .onion and there is no .com, .org, etc. on the Dark Web. All addresses are randomized, and looks like "572abeh6g9gfd8gfd438gfd975.onion". The Dark Web operates under the original vision of the internet, complete anonymity. This also means that some people use it for illegal activities, like auction sites for weapons, online shopping sites for drugs, chat rooms for exchanging child pornography and more. However, it can also be used for legitimate reasons, like online shopping using bitcoin or other virtual currency, chat rooms where you can remain truly anonymous, and more.

The only way to access the Dark Web is to connect TOR and open the TOR browser. This is the only way to read and access .onion addresses. If you want to learn more, launch TOR and its browser, and head to this address:

<http://zqkltwi4fecvo6ri.onion/> 

This is a Wikipedia type page with information and links to other pages on the Dark Net, and also contains material so you can learn what the Dark Net is, how it works, and whether it can be useful to you. It is perfectly legal to access the Dark Net, and we recommend you to test it and learn more. However, the solutions for communication already presented in this manual should be enough to secure you, so we will not present the Dark Web in any more detail. To launch TOR and use the TOR browser, see the earlier chapter where it was presented.

PRACTICAL DIGITAL PROTECTION

CHAPTER 5

STORING

INFORMATION



This chapter will show you two different kinds of encryption. The first one, Basic Encryption, uses built-in automatic encryption of your computer, and any USBs etc. you want, in a manner similar to how smartphones these days comes with encryption. The second, and more important, form of encryption is about creating a hidden, highly encrypted (Advanced Encryption) area of your hard drive or a USB, where you will keep all your work files.

Encryption is a word used a lot these days, and covers everything from email and chat communication, accessing websites, to storing information. Encryption means that the data is protected so that outsiders cannot read it. Only those with the key used to encrypt the data can read it (called decrypt). This chapter deals exclusively with data encryption, for your storage use, such as hard drives, USBs etc., and not emailing, internet connections etc.

WEEDING OUT EXCESS INFORMATION

The more data you store, and on the more different hard drives and devices, the more difficult it is to protect. The first step should always be to select one place where you will store your work data, and then only that place. Second is to get rid of everything that you do not need anymore. Unless you really need to keep the data, you should get rid of it. The less you have to protect, the easier it is.

You will need to constantly analyze how to limit the threat against you. You also need to analyze how you will be affected if any layer of your security precaution is broken. For example, if your encrypted storage for work files is compromised, what information will the outsider have access to?

The less information you keep, the less information you have to worry about. This means you should strive to only keep the documents you actually need. When you write a long report, a significant amount of research is needed. If you write a grant request/proposal, you likely need to produce a lot of information for that. If you produce a grant use report, you likewise end up with a lot of information. Often as part of our work process, by the time we have our finished product, we have probably also created a lot of documents, whether drawings,

tables and charts, individual word documents for different aspects, before in the end putting together the relevant information into one final document. By the time the final document is done, do you really need to keep all those other documents created? Probably not. If so, get rid of them and save and store only the final document. Chapter 7: Deleting Information will present details on how to securely delete information.

WHAT TO USE FOR STORAGE?

HDD, SSD, SD, USB. These are only some of the terms out there. These things are about different forms of storage. What type of storage you use will directly affect how easily you can properly delete the information when you no longer need it. At this point, it will be a good idea to read the HDD vs SSD section in Chapter 7: Deleting Information, before deciding on what you want to use for your work document storage. This will matter when you set up your Advanced Encryption. First however, you can read and go over section on Basic Encryption below.

BASIC ENCRYPTION

If you use an iPhone or an Android phone, you will notice that the phones are sold with encryption already enabled. Even if not, the phone allows you to encrypt them easily, and all you need to do is select a PIN code or password (and no existing data is deleted in this process).

These days both Win10 and OSX have the same function, allowing you to encrypt your computer's hard drive(s) very easily and selecting a PIN code or password. Unlike phones, it does not come enabled when you buy your computer, so you have to do it yourself. Enabling this encryption does not format/delete your hard drive or delete anything from your computer. After enabling encryption everything that was there before will still be there, and you will not notice any changes.

This Basic Encryption should be used by everyone, regardless, as it protects your data in a very easy manner. The difference for you as a user is very small. If encryption is enabled, you need to enter your PIN code or password before your computer or phone starts. If you don't it can't start, because it cannot access the hard drive, and thus cannot start the Operating System (OS). You can also enable this form of encryption on external hard drives, USBs etc. (in which case you will be asked for the password or PIN after you plug it into the computer.

Since most phones and computers require a password or PIN to open you might wonder what the difference is. The difference is that the old type of entering a password or PIN you are used to is to unlock the computer or phone's interface (going from the lock screen to the OS interface). These passwords are only required after the OS has loaded and is running, and only prevents people from accessing the interface. This means that nothing is encrypted, and if someone wants your information, they can simply take the hard drive or other storage used, and plug it into another computer and read every single thing on it. Encrypting the device and hard drive will prevent this.

Having a password to disable the lock screen and enter the interface is like having doors on your home. Encryption is like having locks on those doors. A door without a lock is not exactly helpful if someone wants to break in.

Technical Solution: Basic Encryption will show you how to enable this on your computer, the feature is called BitLocker. However, only Win10 PROFESSIONAL, not HOME, offers this. If you have HOME version, you cannot use and can skip to Technical Solution: Advanced Encryption.

ADVANCED ENCRYPTION

Using Basic Encryption gives your computer basic security. If used, in the future, you will enter your password or PIN when starting your computer, and that's it. Next we discuss slightly more sophisticated steps, which is where your work files will be stored and kept. Even if you cannot use Basic Encryption, this hidden encryption will keep your work files safe and hidden to any outsider. The program we will use is Veracrypt or Truecrypt, which functions the same way whether you have Win10 or OSX.

We will create a secure, hidden encryption space for your work files. As shown before, such as when discussing Zero Inbox Policy, the key threat is not that someone uses advanced hacking to break your encryption, but what happens when police or criminals force you to give them your password. If you do, and you most likely will, all your protection is lost. Like with browsing and emails you use, the key for protection is for them to not know that you have it, because they cannot ask for what they do not know exists.

There is an easy and very clever way around this problem, and it's called hidden encryption. The point is that no one will even know that it exists, and therefore no one can force you give out any password. This part, along with Zero Inbox Policy and Chapter 7: Deleting Information are the most important parts of this whole manual. It is the combination of these things that will protect you. We will also take the time to tell you that it's not advanced or difficult to use at all. Some time might be spent to set it up, but once done, you use it with a click of a button.

What creates this safety?

When a hard drive, or part of a hard drive or USB etc. is encrypted, the computer cannot read that part. You need to decrypt it before you can read it (by entering a password). By using technical analysis, police, criminals or others can therefore conclude that you are using encryption (or that your hard drive is damaged). What will follow is that they will try to force you to give out your password. There is no way around this.

The way to overcome this problem is that you don't create one encryption, but two encrypted spaces, in the same space. This space will have what is called an Outer volume and an Inner volume. Volume is just another name for the encrypted space. One password opens the Outer space, while another, much more secure password, opens the Inner one. You are using hidden encryption.

Because the Inner volume is inside the Outer volume, there is no technical analysis that can show that you have an Inner one.

For practical purposes, when you select to mount your encrypted area, if you enter one password it will open

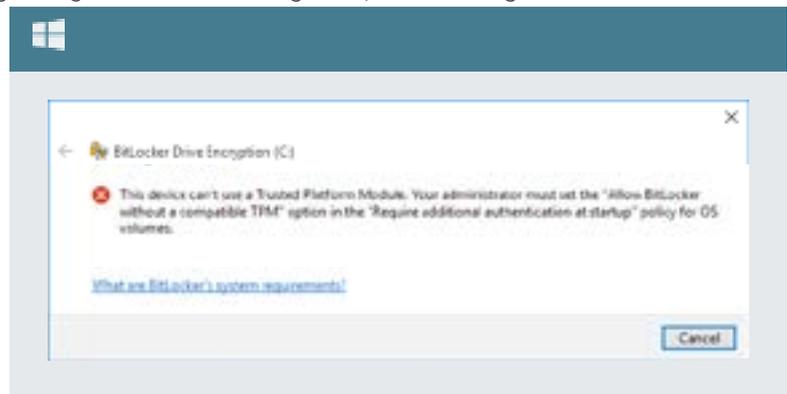
the Outer volume. The Outer volume will function as a decoy, meaning if the police or criminals force you to give up the password and show its contents it won't present anything too sensitive but should satisfy them that they have uncovered all your encrypted information. You will place some work documents and other personal data in this Outer volume, so if ever forced to open it, they will believe they have found what they wanted. But, you will keep the real, or more sensitive material, on the hidden, inner, volume.

- **Have you turned on Basic encryption for your computer?**
- **Have you completed setting up a Hidden encryption and tested it?**
- **Do you understand why the use of Hidden encryption (inner vs outer volume) and the idea of plausible deniability can help you, other than just protect your data from hacking?**
- **Do remember, the less data you have to protect, the easier it will be. Get rid of unnecessary work files that you do not need to keep.**

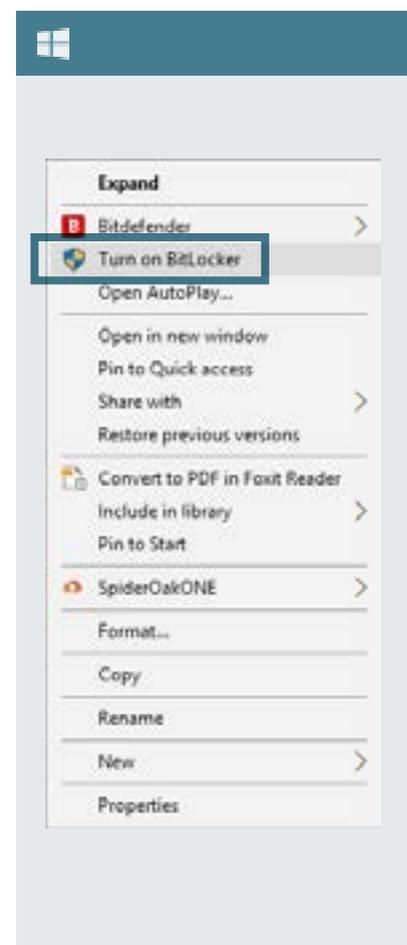
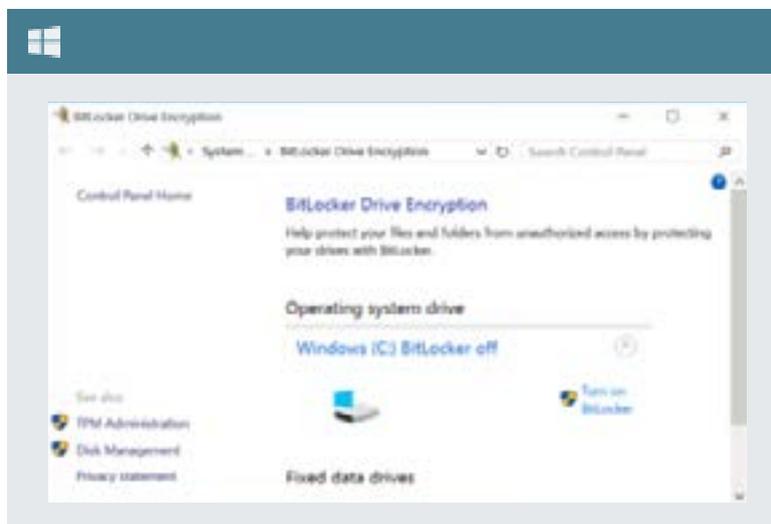
TECHNICAL SOLUTION: BASIC ENCRYPTION

For Win10 the built-in program that handles encryption is called BitLocker (Search Term). You start the program by searching for them in the search area. They can encrypt your OS hard drive, other hard drives, USBs etc.

When you open BitLocker, it is unlikely, but you might see WIN - 20. If you do, this means you need to turn on something called TPM. You do this by following the steps on the screen. This process will require you to restart your computer. If you need further help on how to turn on TPM, googling it will show plenty of easy to use help on how to turn on.

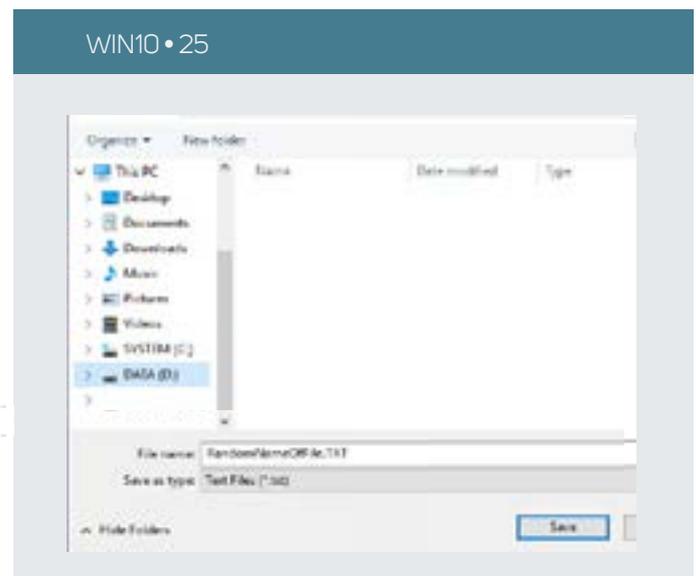
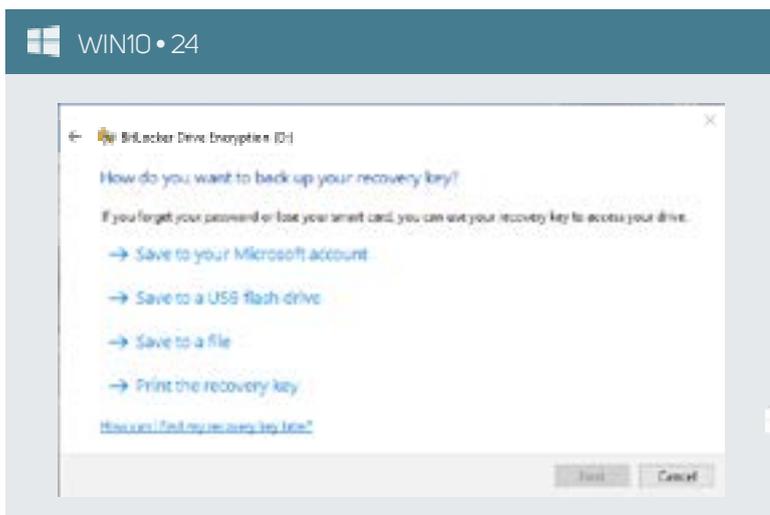
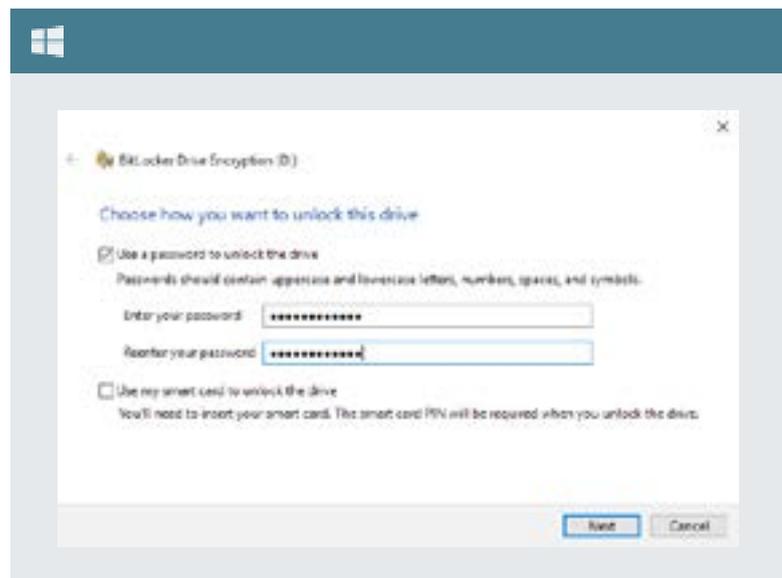


Once you started BitLocker, you can choose what hard drives or removable media (USDs, SD cards, etc.) you want to encrypt from the main BitLocker menu (WIN - 21), or you can right-click on the drive in the Explorer window and select Turn on BitLocker (WIN - 22). Before you start, make sure you have a USB or printer nearby that you will have to use briefly.



Start the process for any hard drive or USB by clicking Turn on BitLocker. The first step is that you will be asked how to unlock this new encrypted drive, and you should choose Use a password (WIN - 23) and then click next. Because this is basic encryption, you can use a PIN code or a shorter password.

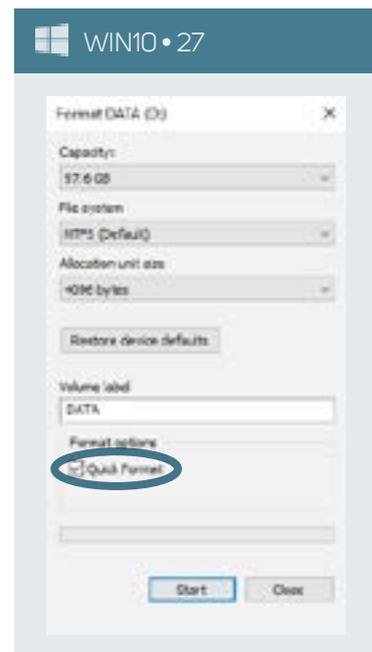
Next it will ask you where to save your Recovery key. This key, which is a string of characters, can be used to unlock your encrypted drive if you lose or forget your password. This is a major security threat. To counter this, choose Print the recovery key if you have a printer available. If you do not, then select Save to a file and save it to a USB for now (WIN - 24, 25). You can also choose to let a copy be stored by Microsoft in your Windows account, but if your windows account is accessed online, it would mean anyone with access could decrypt the drive easily without having your password, so only use if you feel you can protect your Windows account.



After having saved the Recovery file and clicked next you will be asked how much of the hard drive or USB to encrypt, and here you always select Encrypt entire drive. On the next page again you select the encryption mode most suitable to you, usually New encryption mode is best, but the second option, Compatible mode, might be needed if it's a USB or an external hard drive that you want to be able to use on other computers which might not have the latest Windows system.

You are now ready to encrypt the drive, click Start encrypting and let it run in the background (WIN - 26). The larger the hard drive, the longer it will take. This is a background process, so let it just sit there and do its work.

Finally, we need to get rid of the Recovery file. If you printed it, destroy the paper so the string of characters cannot be read. If you saved to a USB, go to that device and Delete the key. After deleting the file, Right click on the USB (in the Explorer window) and select Format, and format the USB. This process will remove all traces of the key. Do not use Quick Format. Quick Format will not securely remove the data (WIN -27).

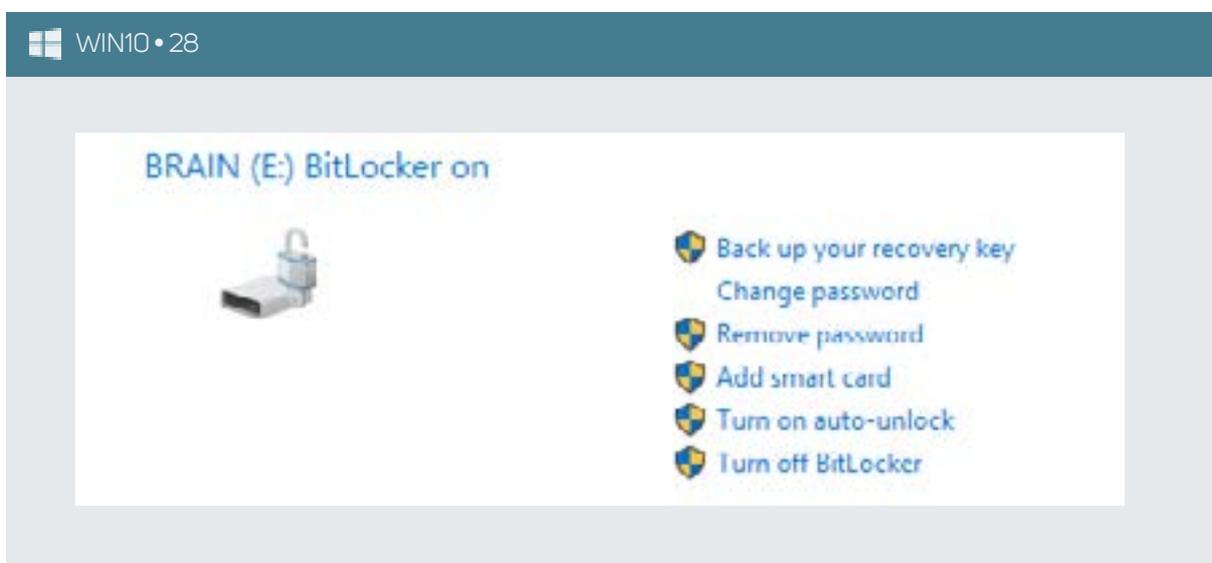


TWEAKING AND USING BASIC ENCRYPTION

From the BitLocker menu you can see that after encryption is enabled you have several options. You can of course Turn off Bitlocker for a drive. You can also decide if a device should Auto-unlock or not. Auto-unlock means that you will be asked for the password or PIN to unlock any non-OS hard drives, USBs etc. once the computer starts (or if using USB or external hard drive, when it's first plugged in). If this is not turned on, it will not unlock those drives until you click on them in the Explorer window, at which point it will ask you for the password or PIN.

This auto-unlock or not feature does not apply to hard drive with the OS. For such drives you always have to enter the password or PIN when you start the computer, or else it cannot load the operating system. WIN - 28 shows some of the different options.

Once you have unlocked a drive, it will remain unlocked until you shut down your computer. You have now finished enabling basic encryption of your computer.



TECHNICAL SOLUTION: ADVANCED ENCRYPTION

To create this hidden encryption, you need to download and install a program called VeraCrypt or TrueCrypt. They do the same thing, and look the same way.

VeraCrypt: <https://veracrypt.codeplex.com/wikipage?title=Downloads>

Truecrypt (7.1a): <https://www.truecrypt71a.com/downloads/>

You can install VeraCrypt on your computer, or on a USB stick. The latter is safer, but requires you to plug in a USB stick (and keep it plugged in) while you use it. Regardless, as always, download the file straight to the location where you will install it, not to your desktop.

Unlike the Basic Encryption, when you want to use the hidden encryption, like when you need to download a new file, or are working on your documents, you simply start VeraCrypt and load the hidden encryption, which will pop up in your Explorer or Finder window just like any other hard drive or USB. Once finished with your work, you simply unload it. The terms used for loading the encrypted storage is mount. For unloading/locking, it's called dismount. The encrypted space created is often called a volume. We will use these terms for the rest of the chapter so you get familiar with them. Once you mount your encrypted space it will appear like a hard drive, for example E: Name, and once you dismount, it will disappear.

SETTING IT UP

Step one is to decide where this encryption will be. Do you want to use a USB? Do you want to use a full hard drive, a partition of a hard drive, or maybe just a small part of a hard drive? We will show how to create such a system for both a USB and whole hard-drive or partitions, and for a small part of a hard drive. (Note: We will not use the option to encrypt the OS drive).

On a step-by-step basis, here is what you do. After installing the program either on your computer or a USB, start the program. In the first window you see, which is also the main window (WIN + OSX - 29) for normal use (mount and dismount), click Create Volume.



After clicking Create Volume, you will have two options (WIN + OSX 30) (a third option for system partition is shown in Win10, but is not relevant to us). One option, and the easiest one to use, is Encrypt a non-system partition/ drive. This encrypts a whole partition or hard drive (not for hard drives with an OS on it). It also applies to external hard drives and USBs.

The other option is Create an encrypted file container, where you yourself decide how much of a hard drive, USB etc. should be encrypted. If you want to use this option, you need create a file somewhere, on a USB or on your hard drive. Create a file of any type, but not a word document or text file, for example a database file or powerpoint presentation or something. This file will then hold the encrypted space. If you delete this file, you delete everything! Remember what file you create, and where, and make sure you do not accidentally delete it.

After selecting either of the options and clicking next you will be asked if you want to create a Standard Veracrypt volume or a Hidden Veracrypt volume (WIN + OSX 31). You select Hidden and click next. After this you are asked to choose between Normal mode and Direct mode. You choose Normal mode (Direct mode is for if you already have an encrypted space since before) (WIN + OSX 32).



After this, it will depend on if you selected Create an encrypted file container or Encrypt a non-system partition/ drive.

Go back to Veracrypt and click Select File from the window (WIN + OSX 33), and navigate to the file you created and select it. It will warn you that any data in this file will be deleted. Say Yes. If you choose Encrypt a non-system partition/disk you also click Select File and from the pop up window select which USB, hard drive or external hard drive you want to encrypt. Encrypting it will delete all data on it, so make sure you have moved away any files you want to keep.

After making this selection, the rest of the process is the same for both methods.



The program will first create the Outer volume. You do not have to make any changes on the next step (Encryption options) (WIN + OSX - 34). After clicking next it will ask about size. If you choose Encrypt a non-system partition/drive you cannot alter this, and the whole space will be encrypted. If you choose create a file container you will be asked how big it should be. Unless you work with a lot of media file, such as video editing, 10 GB should be enough (WIN + OSX - 35). Make your selection and click next.



The next window is to create the password for the Outer volume (WIN + OSX - 36). This is the decoy encryption volume, and the password does not need to be very advanced. Choose something you can easily remember.

After clicking next the encryption preparation process will start. This won't take very long, but depends on the size. While it is being done, please move the mouse around as much as possible (WIN + OSX - 37). This interference will strengthen the encryption. Once it stops and is ready, click the Format button.



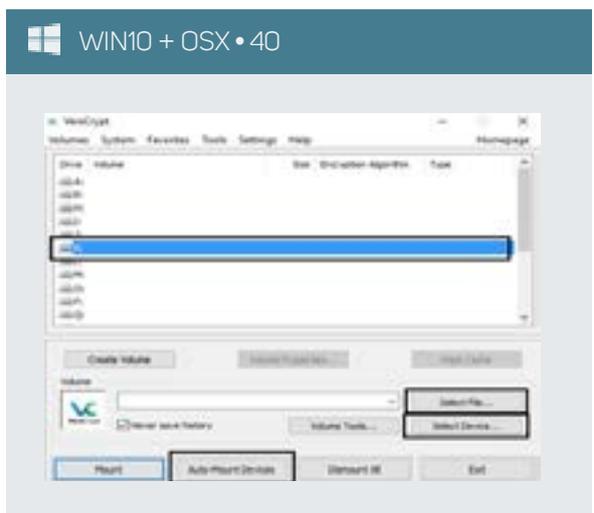
After completion, it will show you the window above, and you click Next (WIN + OSX - 38). This will start the process to create the Inner (hidden) volume begins. Click Next. The only thing to change is the size, which need to be set to be smaller than the Outer volume (we recommend about half), and also to use here a very strong password, a password you will not forget, or you will lose access forever. All other steps are the same, and once complete, the window below will be shown and you click Exit (WIN + OSX - 39). You are now finished, with both an Outer and an Inner volume.



USING VERACRYPT

Everything is now set up and you will not need to bother with this again. To use Veracrypt simply start the program (WIN + OSX - 40). To mount your device, there are two ways. First click on any of the drive letters. Once mounted, your encrypted volume will show up in the Explorer or Finder window as a hard drive with this letter. Select E: or F: or whatever you prefer.

If you created a whole hard drive or USB, simply click Select Device, and from the pop up window select the hard drive or USB. In the password box shown, enter the password. The simpler password will automatically open the Outer volume. The more advanced password will open the Inner volume. If ever pressed or forced to provide your encrypted space, you write in the password for your Outer volume.



If you instead choose to create a file container, click Select File and navigate and choose to the file you created to hold the encryption. Again, if you enter the simpler password it will automatically open (mount) the Outer volume. The more advanced password will open the Inner volume.

There is also an Auto-mount Devices button. Clicking this automatically identifies anything that can be mounted, and asks you for your password. The rest works the same, simple password for Outer volume, advanced password for Inner volume. Unfortunately the Auto-mount function does not always work and can take a bit of time to load, but if it does, it's the easiest way to mount your encrypted volume.

After mounting your volume, you can close the program and work as you are used to.

Once you finish your work, or no longer need to access your work files, or you are about to leave the computer, start the program and select Dismount all. This will close the mounted encrypted drive (and it will no longer be visible in the Explorer or Finder window).

In the future to mount and dismount is the only thing you need do.

FINAL STEPS

The ability to deny access to the real hidden encryption (Inner volume) is in English called plausible deniability, and is key for protecting yourself. However, to work, it must be believable. Believable here means that the information in the Outer volume (decoy) must be something that you obviously don't want to share. Once you are forced to open the Outer volume, when police, criminals or whoever it is, sees the material in it, they must believe that this is what you were protecting. If it's empty, or contains just music etc., they will obviously figure out that this is not what they are looking for, and continue to pressure you.

Thus, after setting this up, take some time to make sure to place in the Outer volume a lot of files that are sensitive, but not very sensitive. You must place information here that looks sensitive. For example, you could store some bank documents, pirated media files, or the pdf of a blacklisted book. You also need to put some work files here, for example reports, documents you have written, or work-related files that you have downloaded. You will place copies of these files here, but will not need to use them. Every once in a while you should add some new documents to the Outer volume so it appears like it is still in use.

If a situation arises with heightened security concerns, copy a few more work files to the Outer volume. However, the really sensitive documents should not be placed here. This is again only a decoy. The reason or the decoy is to throw the police or criminals off the trail of your real sensitive information.

The reason you need to update the Outer volume sometimes is that all files and folders have a time stamp when the file was last moved, changed, edited etc. If they access your Outer volume and see that no documents have been changed for two years, they can realize you do not use it, and that it is either old or a decoy, and thus press you for more information.

The easiest way to create this system is to move all your work files to the Inner volume. After that, you may want to go over those files and copy some of them for the Outer volume. Again, select files that are about your work, but which are not sensitive, and do not contain names, details or damaging information on others, etc.

Because this Outer volume must be believable, we also advise you to put there anything that would normally be considered sensitive or personal. Additional examples include:

- **Many people store a list of passwords for non-sensitive things, like login information to online shopping sites, social media only for personal use etc. If so, place it here.**
- **Perhaps from your past you have written very personal letters or documents, about deeply emotional and private issues. If so, place it here.**
- **Perhaps you have shared personal information, photos and letters with a lover. If so, place it here.**

In short, this Outer volume will be (very) safe in a normal sense, and under threat only if police or criminals force you to open it. If things are so serious that they are forcing you to give out passwords like this, be prepared to have such personal matters viewed and read, and realize allowing this will go a long way to help you, by making them believe that you truly don't want the information here to be found or read.

To be believable, don't give up the password to the Outer volume easily or immediately. You should still resist if asked, otherwise the adversary may become suspicious. If they believe you, your real sensitive information will be safe. And yes, no one would like police, a criminal or a kidnapper to see revealing photos you might have taken of yourself and sent to a lover, but compared to imprisonment, the choice should be simple. In fact, if you have none of the personal type of information mention above, its recommend to create it now and put there, fake it if necessary. This setup could mean the difference between freedom and imprisonment.

HIDDEN ENCRYPTION AND FILE RECOVERY

A seasoned rights defense lawyer received a message on Telegram from a trusted colleague that the police had been asking questions about her and that she should expect to be detained or at least questioned.

She had at this point already taken on many rights defense cases and worked with many other similar lawyers for several years. She was quite skilled in cybersecurity, having always been afraid police might detain her or take her computer and try to use her information against her. She rarely used WeChat, and never for work, and had since long stopped using QQ altogether. She even knew how to use hidden encryption, and had been using it for over a year, to not only protect the data itself, but also hide its very existence.

This person wasn't a journalist with a duty to protect confidential sources, but she did have much information on both her own clients and sensitive information related to the work of others. If this information fell into the wrong hands she was very worried she could be imprisoned and that it could make it possible for the police to attack others. Making sure documents did not find their way into police hands was a key issue for her, and for her colleagues and clients' safety.

She had already been smart enough to realize that normal encryption would be of little help. If police knew what to ask for, she doubted that she would be able to resist for long, as she as a lawyer was well aware that the legal protections against torture and mistreatment in China is barely worth the paper it's written on. It was knowing this that had led to her start using hidden encryption, despite it taking some time to understand it at first.

When the police eventually detained her and placed her alone in a cell, to undergo more than a month of interrogations, they also seized her computer, phone, and USBs.

After a few days in detention, she was very surprised when the police began to start each new day by showing her documents from her computer. She knew these documents had been stored in encrypted spaces on her hard drive that the police absolutely did not have access too. She had at this point not even been asked for any passwords to encrypted spaces. It was obvious to her that the police not only did not have access to her encrypted space, but didn't even know that it existed.

She was frantic each time the police produced one of these documents. These documents threatened to expose some of her sensitive rights defense work and provide evidence that would make it easy for the police to go after her clients.

Before being detained she had agreed to a cover story with her colleagues who might also be detained. Some of the documents the police produced challenged their cover story, and severely increased their risks. It increased her anxiety and she spent several nights wide-awake fearfully trying to predict how to counter the next set of documents or accusations from the police, and constantly wondering how they could possibly be able to access these documents, many of which only she had,

no other colleague has these after all.

The documents the police had were very random, and luckily very few of them were among the more sensitive documents she had. Many of them were also just partial, a few pages of a larger word document, or one or two excel sheets in a larger excel file. How they hell did they get these documents, she continued to wonder.

In the end, the police did not find the 'smoking gun' they were looking for, and even though she remains to this day under threat, having been released on 'bail', with police able to pick her up again any day they wish, the fact that most documents remained protected saved her.

Only after her release, with time and access to information online did she figure out what had gone wrong. File Recovery program it read. With this, she would learn of something that even many of those skilled in Cybersecurity fails to understand, or if they do understand it, fails to realize how big of a threat it is.

Data she realized are like memories. They linger for a long time, and even when they begin to fade, it happens slowly, and only parts of it disappears. Data, once 'deleted' she realized, is not actually deleted at all, it continues to lie on the hard drive, only not visible to the normal user. It's all still there, until the space hold the data is filled up with something new. The fact that most of data was in an encrypted space didn't always matter, as many of the documents she had produced over the years had been created on the desktop, before being moved to the encrypted space. An act of laziness. Many other documents from coworkers and research material downloaded from online would regularly be saved to the desktop, only to be moved to the encrypted space.

So what had happened? All those documents that had been on her normal hard drive, once moved to the encrypted storage, was readily available to the police using File recovery, easy to use programs available for free online. All they had to do was scan her hard drive in detail, and step by step pieces of old data deleted could be put together.

PRACTICAL DIGITAL PROTECTION

CHAPTER 6

SHARING

INFORMATION



Securely communicating over email is a key issue for many people and this chapter will show how to easily use secure emails, and how to use it in a way that protects you, should a serious threat arise.

This chapter will deal primarily with emailing, as it is likely to be your principal means of communication for work. Chatting, SMS and mobile communication will be dealt with in Chapter 11: Secure Apps For Use, except some notes on using chat programs on computers. This chapter will discuss email encryption, present some options for easy to use automatically encrypted web-mails, and explain what PGP encryption is. It will also discuss Cloud storage.

Encryption is helpful but it can become overly complex for most situations. For this reason this chapter does not include information on PGP encryption. No encryption can save you once you have been detained and your passwords forced from you.

If you want safety, the most important part is to properly use the work browser so they cannot know what email services you use, and to use the Zero Inbox Policy, so if they find your email and get your password, there is nothing to find.

ENCRYPTION VERSUS “END-TO-END ENCRYPTION”

These two expressions need be understood.

‘Normal’ encryption means that the service you are using, for example Gmail, encrypts your data, in this case, email. This means that you need to send the email to Google’s servers, which then encrypts it, and sends forward to the recipient. There are two problems here. One, that your ISP might be able to read the data when you send it off to Google (unless you use a VPN or TOR). Two, this means that the service provider (Google),

encrypts it for you. This also means that they can decrypt. You might be able to trust Google, but can you trust a local Vietnamese company, which can easily be forced to decrypt your data if police asks?

If a service provides end-to-end encryption, it instead means that the data is encrypted on your device, for example your phone or computer. This data is then sent all the way to the recipient, who decrypts it on his or her phone. This means that your ISP cannot spy on you, and the service provider cannot know what the data contains (like chat messages, emails, etc.). Using end-to-end encryption is a key issue, and should always be used if available as an option. In this situation, even if a company wanted to spy on you, or a government were to force them to give out the information, they cannot, because they did not encrypt, and therefore cannot decrypt it.

SECURE EMAILING

For practical, and security, purposes, your best bet for a secure and easy to use email, is to use a webmail. Secondly, it is to use a webmail that offers end-to-end encryption, and finally, one without servers in your home country.

You should avoid using Apps on your computer (or phone) to access these emails, only access through your work browser. You should also avoid using a mail client on your computer.

When you are setting up a secure webmail of your choosing, make sure to not use your name or nickname in the name of the email address. This only makes it easier for outsiders to pinpoint which email account belongs to you.”

Besides using one of the secure email services we present below, we advise you to setup a Gmail email. It offers relatively strong security, especially if you enable 2-step verification, and keep a Zero Inbox Policy, and can be used very easily and efficiently for much of your work that is not very sensitive. However, you will need a more secure email for your more sensitive work emailing, and preferably one with additional security features.

There are several secure webmails with end-to-end encryption. Perhaps the best one, with additional security features, is ProtonMail.com. Alternatively there are Tutanota.com and Hushmail.com. Neither of these currently have Vietnamese language interface. They are however easy to use, with clean and easy interface, and you can quickly learn how to use them even if you don't read English.

Most email providers and encryption systems do not encrypt the Subject line. Remember this, as most encrypted emails will still show the title/subject you have written. It is best to choose a cryptic subject line that will not attract attention. Note: ProtonMail does encrypt subject line too.

The downside of these secure webmails mentioned above is that they work with maximum security only when communicating between internal accounts. That means if you use a ProtonMail email, the person you email should also use ProtonMail. As such, before setting up a new secure email, it is worthwhile to talk with those you email with most often, friends, coworkers, partners etc. This way, more of you can decide to use the same service.

There are also ways to send secure emails from these secure webmail to normal emails, where all you need to do is write in a password the recipient need to know to read them. On top of that, the recommended one, ProtonMail, even includes self-destruct emails, set to a timer, so that you can email others, or people you are not sure if they are safe, and the email will auto-destruct both from your email and their emails – and this works even if it is not a ProtonMail.

In short, setting up and learning how to use one of these secure emails is very important.

We advise you not to install any Phone App for these emails, especially not for any App without password protection. Having an App installed on your phone means anyone that accesses your phone knows what email provider you use. If the App itself is not PIN or password protected, they could also access you inbox. We all like to be brave, but once in custody of police, security agents or criminals, it is unlikely you can refuse them this password. The dangerous of Apps is discussed further in PART III (Phone Security) of this manual.

After you set one of these email up, enter the settings area and familiarize yourself with the options, but no changes are needed, as they are set for high level security at start. The section Technical Solution: Using ProtonMail and sending to “normal” emails will show you the interface of ProtonMail, and how to send auto-destruct messages and secure emails to other “normal” emails.

Furthermore, the insert “Sending Information Securely” on pages 77-78 will be of great use to many of you, and is also based on ProtonMail as a solution.

IMAP AND EMAIL CLIENTS

We advise you not to use any mail clients, such as Outlook, Mail or Thunderbird for your secure email. There are no reliable options to lock access to these programs with a PIN code or password (those that exists have bugs and are not safe), those secure emails listed above do not support using email clients anyway. It adds an unnecessary security risk, and is not useful if you use the Zero Inbox Policy. Having the email installed in a program on your phone or computer also means that whoever has taken you already knows what email you use, and can coerce you into providing the password. Having a mail client on your computer or phone counters all the key points so far discussed, namely to hide your tracks and make sure others cannot figure out what you use.

4 KEY BEHAVIORS

ZERO INBOX POLICY

As expressed several times already, the key threat against your email, will not come from advanced hacking but from someone forcing you to give them your password. If taken, chances are that the police will gain access to your email. This is where a Zero Inbox Policy comes in handy, and is one of the most important tools for your safety that exists.

“A zero inbox policy is one of the most important tools for keeping you secure.”

Assume that your email will be accessed if and when you are taken. The Zero Inbox Policy ensures that there is nothing for them to read. In short, keep your inbox (and other folders) empty. In 99 percent of the time, this should not pose any problem, as most emails do not need long-term storage. It cannot be stressed enough how important this is. Likewise, ensure that your coworkers or friends do the same.

NO REPLY AGREEMENT

A No Reply Agreement simply extends beyond the Zero Inbox Policy. If indeed your email is accessed, your captors can wait until you receive new emails and read all previous communications revealing potentially incriminating information. This is because of the way we often handle email. When we communicate, we usually click 'reply' to an existing email, instead of writing a new one. With this, the earlier communication is included in the same email. Often times this back and forth use of reply can go on for a long time, and because of that, one short new email can include a long list of previous emails. This means if your email is compromised, the person responsible can simply wait for someone to email you using the reply function, and see your prior communication.

As such, when you respond in email to your coworker or friends, avoid using the Reply function, or if you do, make sure to delete the original text. This ensures that after your detention, as police are accessing your emails, any new emails that arrive will contain as little back information as possible, and they will not be able to counter your Zero Inbox Policy by simply reading the text in any emails to you using the reply function. Talk to your coworkers or friends you communicate most with and agree to avoid the reply function.

NO AUTO-LOGIN AND DANGER OF CROSS-SERVICE LOGIN

Automatic login can be a real threat, especially since accessing one account could give others access to other accounts by the same provider. For example, if you log into your Gmail in your browser, you can automatically use other Google services without having to log in, like Google Drive (cloud storage), YouTube, etc. The same applies to the family of services provided by Apple, Windows and more. Be aware of this and act accordingly.

The best way to avoid this is to only use one service from any company. If you use Gmail, don't use Google Drive for cloud storage, etc. This will block the danger of auto-login and account syncing.

“Never allow automatic login or syncing of any work email or storage services.”

Services also like to auto-sync these days. If you use google Chrome on your Phone, and you sign in to your Google Chrome browser on your PC or MAC, auto-sync will, if allowed, sync these two different browsers from two different devices. Any bookmarks saved in Chrome on your PC or MAC will show up on Chrome in your phone, alongside browsing history, saved passwords and more. This is a major issue. Do not sign in to your work browser.

APP ACCESS

Even though Win10 now allows for installing of Apps, just like on a phone, we strongly advise against using such Apps. To start with, most do not have native (built-in) password or PIN code protection, meaning anyone who gets access to your computer could open the limited App interface and read message, chats, calendars, emails, etc., or send such, pretending to be you. Having an App installed also clearly shows what services you use, and with that you lose your ability to protect yourself should you be detained.

CLOUD STORAGE

Cloud storage usually refers to the online storage of information. Some cloud services are strictly for backup of work files, while some store and update computer settings and programs. Others operate as a collaboration platform, allowing you to share your documents with others and to simultaneously edit those documents. In general, anything stored online is less secure. For this reason, never use services such as OneDrive for Windows, iCloud for Mac, or Google Drive for any sensitive work purposes. That said, cloud services are not all bad and can be used securely if you know what you are doing.

	Free Space	End-to-End Encryption	Encrypted Storage	App PIN	2-Step Verification
Google Drive	15GB	No	Yes, but weak	No	Yes
iCloud	5GB	No	Yes, but weak	No	Yes
OneDrive	5GB	No	No	Yes	Yes
Dropbox	2GB	No	Yes	Yes	Yes
SpideroakONE	2GB	Yes	Yes	Yes	No
Tresorit	5GB	Yes	Yes	Yes	Yes

You undoubtedly have cloud storage services already, even if you are not aware of them. For example, if you have Gmail, you also have Google Drive. If you have a Mac computer, you have iCloud, and if on a Windows system or you use a Hotmail, you have OneDrive. Many cloud services come pre-installed with your phone and computer.

Your focus, if you need cloud services, should be to use a service that provides backup of the files you specifically select. These programs will run in the background on your computer and phone, and any time you make changes to your documents, the cloud storage will be updated. It is thus a backup in case you lose your computer or phone, or they are confiscated. But it also means that your cloud storage is another way that someone can access your information, and thus it needs to be protected.

Firstly, you should go over your phone and computer, and see which services are already enabled and what Apps are installed. For those you will not use you should disable. Phones especially come preconfigured to save your personal settings as well as photos, videos and documents automatically. This can be very dangerous, especially since most of these services can be accessed on phones without having to enter a username or password through their respective Apps. Remove/uninstall any cloud service you will not use.

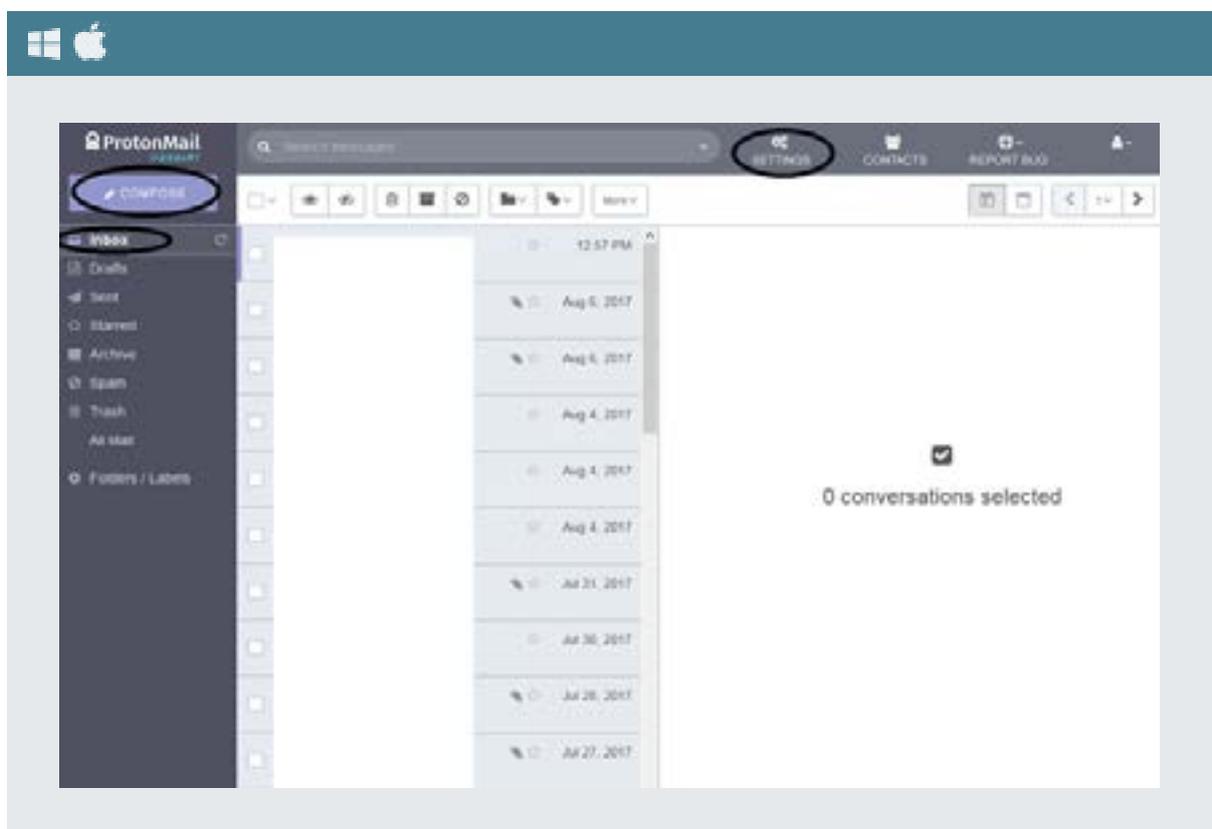
Secondly, in line with what has already been covered about hiding your information, you should not rely on Apps to access your cloud storage. Apps are easy to use, but pose real risks. Anyone who takes your phone or computer will easily see what service you are using, and they can forcibly get the password and/or username. There is little point in using hidden secret encryption to store your data if you don't take steps to protect that same information being backed up online. Only access your cloud services in your work browser, through your VPN.

Some cloud services will run a process in the background to automatically upload new documents and changes made while working. This is discouraged. For others, you have to manually enter the cloud service and upload the documents you want saved online. We recommend this, as it adds protection, and hides your choice of service from anyone getting access to your phone or computer. As should be very clear by now, never use a cloud storage service provided by a local company.

TECHNICAL SOLUTION: PROTONMAIL

Using these secure webmails is straightforward and doesn't need to be explained much. However, due to language limitations, the screenshots below, for the main interface, will be explained. Study this, log into the email and familiarize yourself, and you should easily be able to use ProtonMail without any difficulty. Should you choose to use Tutanota or Hushmail instead, they both work fairly similarly.

If you want to use ProtonMail (WIN + OSX - 41) to send a message to a normal email, for example Gmail, you have to select and write in a password. When you send the email, the recipient will not receive the email, instead they receive a link (in his or her email inbox). When they click on this link, they will be asked to enter the password you set to be able to read it (and respond to it).

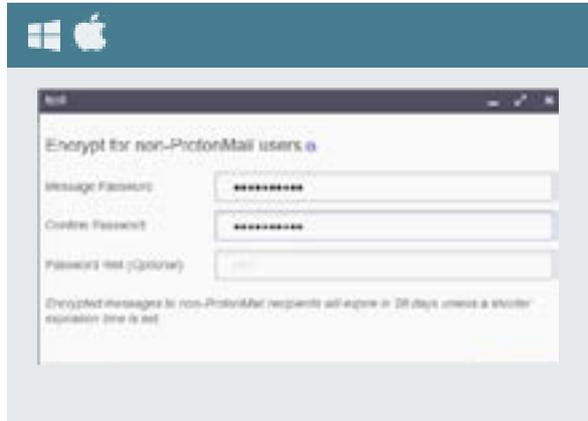
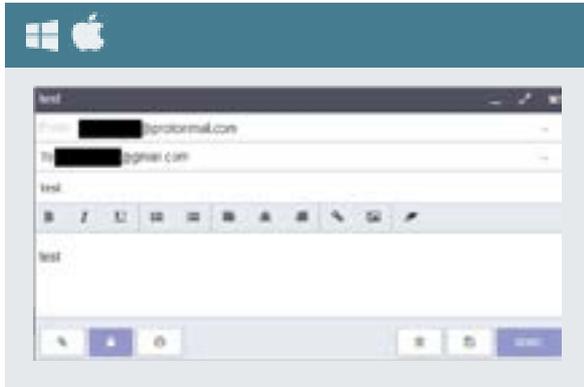


Hence, after you email someone, you need to use a secure chat app to give them the password, or you can have agreed on a standard password in advance. We recommend sending the password over signal or telegram with self-destruct function enabled, more on this Chapter 11: Secure Apps For Use in PART III (Phone Security).

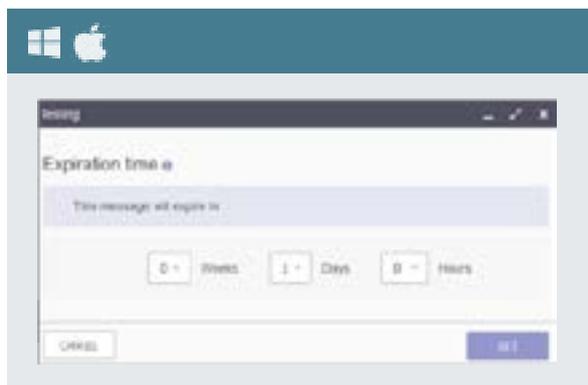
When you do this, or even if you email just another ProtonMail, you can also set a self-destruct timer, so the email will be destroyed automatically, and it will be destroyed both for sender and recipient, a very powerful too. The screenshots and text below will show how to use these functions.

Open Compose (WIN + OSX - 42) to send a new email. In the bottom-left corner there are three buttons, for attachments, for encryption/creating password, and for auto-destruct timer. Click on the middle one for encryption/creating password.

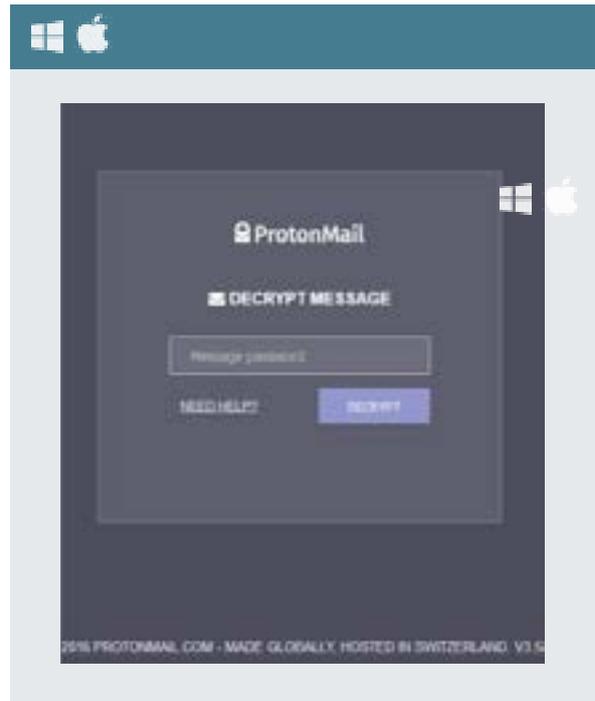
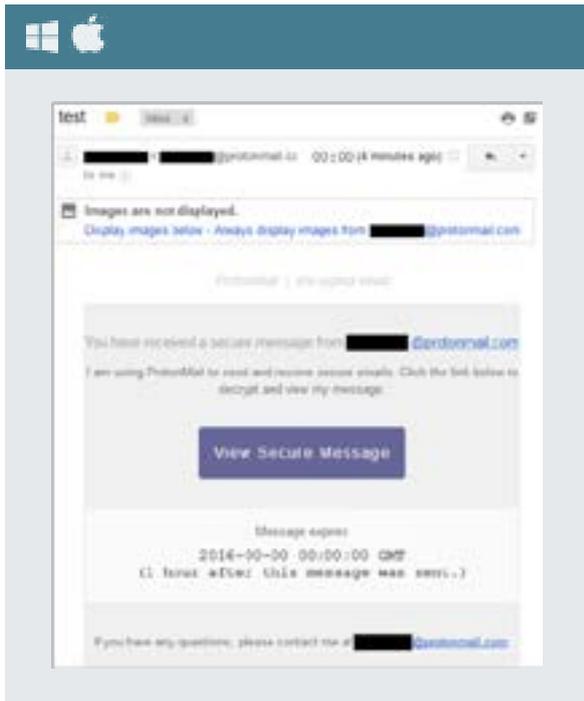
Create the password and click Set (WIN + OSX - 43) and you will return to the first screen again. Then click on the third button to set auto-destruct timer.



Set the auto-destruct timer (Expiration time) and again click Set to return to original window (WIN + OSX - 44). You select Weeks, Days, Hours in that order (from left to right).



After sending the email, the recipient will receive an email containing a link (WIN + OSX - 45). They click on that link and are taken to a webpage to enter the password (WIN + OSX - 46). Note: If instead you sent to another ProtonMail, it will instead appear in their mailbox just like a regular mail (but self-destruct timer will work the same).



At this point they can then click reply, and send a reply to you, using the same password (WIN + OSX - 47).



SENDING INFORMATION TO PEOPLE AT RISK

If you need to send information, whether questions, information or instructions, to a person who may be at risk, there are ways to do so while limiting potential damage. This person may be at risk of detention, kidnapping or being taken against their will. Or this person may be a target of Cyberattacks, or simply not entirely trustworthy to handle the information you need to get them in a secure way. Not all people will follow instructions on how to handle information securely, at which point it's important you do so in a way to limit potential risks, whether to the recipient, yourself, or others.

There are no ways for a normal user to provide files or data to another person's computer without losing control of it, as any program or script to, for example, delete such data after reading, would constitute a virus, and be blocked.

Firstly, you should always send as much information Inline: as text inside an email and not as an attachment. Never use attachments unless strictly necessary. If you really need to send an attachment, make sure to limit the information in the attachment, and delete the metadata before sending it. The way to do this is shown below.

SENDING EMAILS THAT WILL AUTO-DESTRUCT

First, a key advantage of ProtonMail over other emails is its Auto-destruct function for emails. Similar functions exist for two Chat programs (Telegram, Signal) presented in the Phone Security part of this manual. You can thus write an email to someone, and set a timer. This timer starts ticking when you send the email. This is very important. The timer starts when you send the email, not when the recipient clicks read. You can thus set a limited timer, say 1 hour, or 1 day, etc., after which the message will be destroyed. The message is destroyed both in your email (sender) as well as for the recipient. Make sure to send a secure message to the recipient so they know to check email quickly, see below.

Another important advantage of ProtonMail is that you can use it to send highly secure emails to non-Protonmail accounts while still allowing the autodestruct function. The recipient will receive the email with instructions on how to retrieve the Protonmail message, as shown in Chapter 5: Sharing Information, but once the pre-selected autodestruct time has passed the link to retrieve the Protonmail message will no longer work. In effect, the message has been auto-destroyed. Any attachments sent with the email will also be destroyed. However, any attachments that have been downloaded will not be deleted. Again, avoid sending attachments as much as possible.

To use this system effectively you need to also be in contact with the person on Signal, Telegram or in some other way. This is because you will need to tell the recipient that an email has been sent, and that they need to read it. If they don't see it in time it will be destroyed, and they will miss it. As such, ProtonMail should for full effectiveness be used together with a secure Chat program. If you send a ProtonMail to a non-ProtonMail email, you need to select a password, which the recipient needs to know. See Chapter 5: Sharing Information for a reminder of how to do this. Once you have selected the password you will need to share it with the recipient through a secure Chat program, especially Telegram or Signal that also provides for auto-destruct.

Using auto-destruct means you don't need to worry if the recipient is following secure procedures like deleting emails and keeping a zero-inbox policy because you will know that after the pre-selected time the email will be securely auto-deleted regardless of their behavior. If the person you are emailing is suddenly taken, any information you have sent will have be destroyed within the time limit, hopefully well before harmful third parties are able to see it. Nobody will be put at added risk because someone forgot to delete a sensitive message.

SENDING ATTACHMENTS WHEN NEEDED

As the section on Metadata will later show, any document you send contains more information than people think. Obviously the information in your document will be there, but also the metadata. Metadata contains information like when the document was created, what computer or phone was used to create it, the name of the person if their computer or phone is personalized, the GPS location where it was created, even the names of individuals in photos based on automatic facial recognition on your phone, and other similar information. To understand Metadata better, and how to remove it, see special section on Metadata in Part II.

If you do indeed create a document to send as an attachment, you should consider:

- To not include photos, excel charts, tables or other graphical information;
- To use the built-in Office/Word/Excel function to scan and remove all metadata before saving document ('Inspect Document' function);
- To send as a PDF file, not word, excel or similar; and
- To password protect the PDF file.

When you export a word or excel file to a PDF, you will have the option to Password protect the file. We recommend you do that as standard, and then use a secure Chat program, such as Telegram or Signal, to tell the recipient the password to open the file. A password protected file, just like an empty inbox, will secure the recipient from harmful hacking, as any access will have limited consequences. For most documents you receive as an attachment you probably don't need to keep them forever. As soon as you have used the information in the attached file, whether to update a case file, add information to an article, complete a petition or anything else, you should securely delete the document following the process outlined in Chapter 7: Deleting Information.

Finally, as an important reminder, try to always keep and follow the 'Zero Inbox Policy', and discuss this concept with anyone you communicate with extensively, or anyone you communicate with who may be a risk. The 'Zero Inbox Policy' is your greatest tool to ensure safety.

METADATA, PUBLISHING, AND MS OFFICE

Metadata is information about something other than the content. For an email, for example, metadata is the time the email was sent, its size, the address (IP address) used, the subject line message, and who sent it and who received it. For MS Word documents or PDF files, it will be when something was created (or edited), who did so (name of computer user), time of changes, and more. The same applies to publishing and design tools, like MS Publisher, InDesign etc.

These days, photos you take with your phone, or videos, will likewise contain such metadata. If location access is allowed, it will also say where it was taken, with precise GPS location. Even more, photo apps are now so sophisticated that it can recognize the people in photos and tag them by name based on your address book and earlier photos taken. With this in mind, realize just how much data can be included in a PDF file you publish, or a photo you send someone.

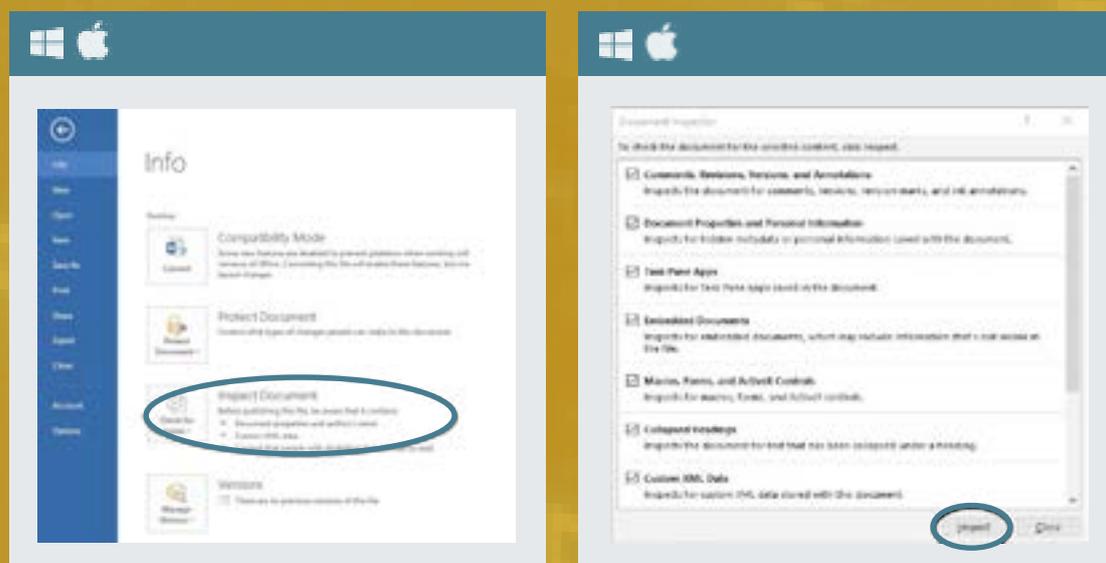
The reason to consider metadata is to make sure you are not communicating or publishing more information than you think, as metadata leaves a trail of evidence.

FOR OFFICE DOCUMENTS AND PDFS

The MS Office suit, covering Word, Publisher, Excel etc., comes with a built-in tool for scrubbing (removing) such metadata from the document. This also means it's removed before being saved as a PDF etc. It functions the same on Win10 as on OSX, and you can locate the function easily, namely click on File, which will take you to the tab for Info shown below.

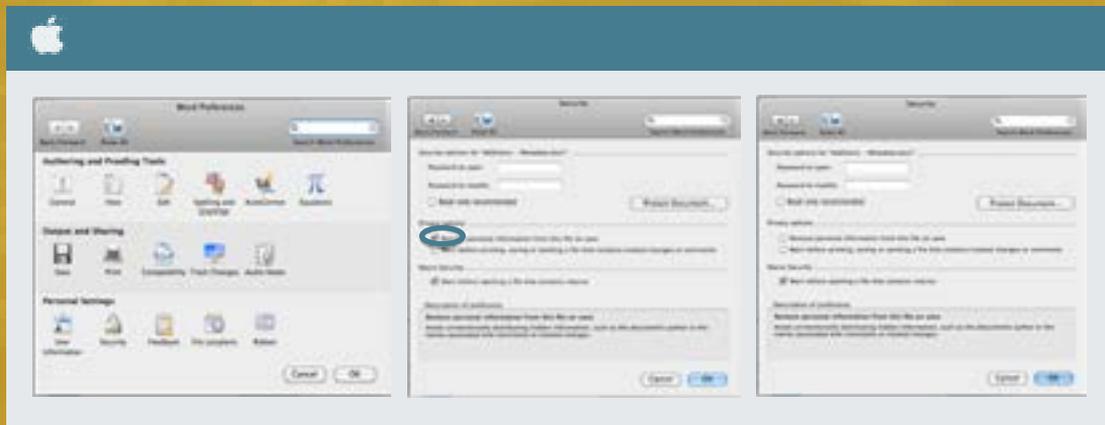
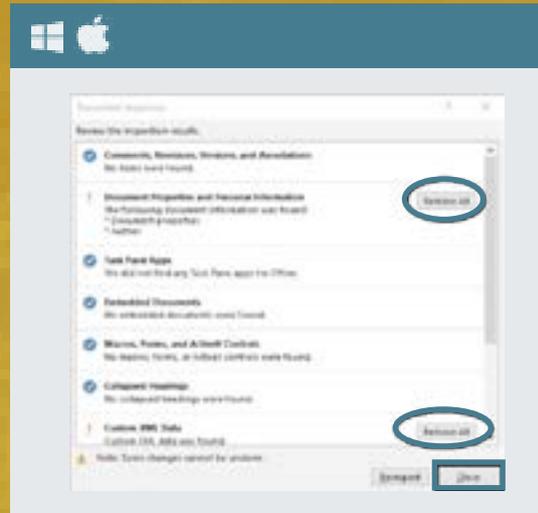
Click on Inspect Document button shown in (WIN10 + OSX • 48) and from the dropdown menu click Inspect Document. A popup window will appear (WIN10 + OSX • 49) showing a list of issues that will be checked, click Inspect button.

After having clicked Inspect, the window will show you what information has been found for each issue (WIN10 + OSX • 50), and if anything found, there will be a Remove All button on the left. Click on all Remove All buttons, and then click Close. All metadata has now been removed, and you can



save the file as you wish, or make it into a PDF.

For older versions of MS Word on OSX you will have to go about this a little differently. Open the document of concern and then click Word > Preferences > Security. In Security uncheck Remove Personal Information from this File on Save (OSX • 51).

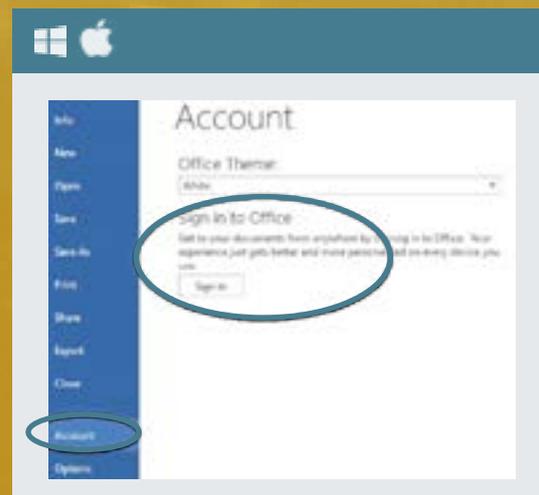


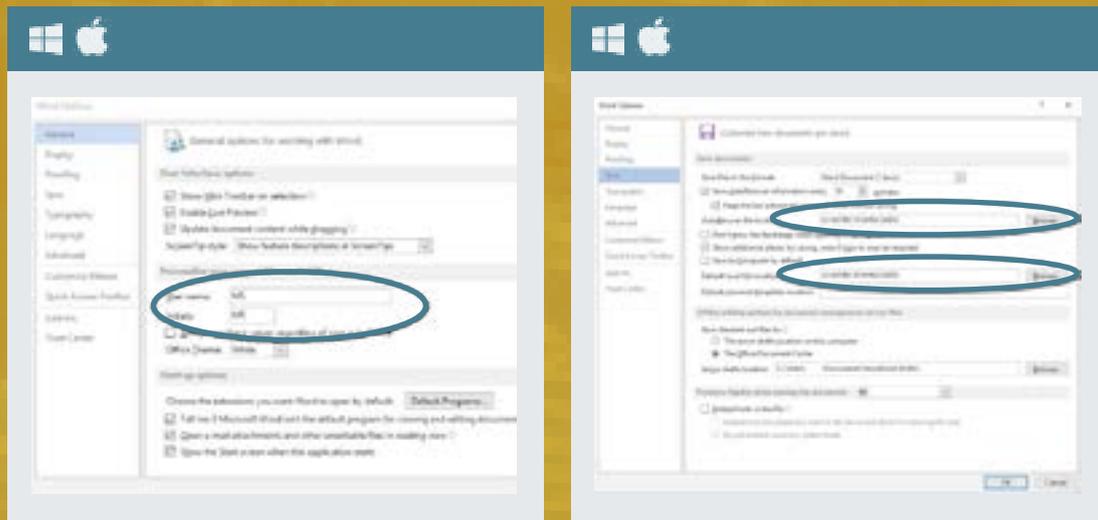
MS OFFICE SETTINGS

At this moment it would make sense to check out some settings about your Office suite. Open a Word or Excel file, and click on the File tab in the top left corner. On the side menu you will find two tabs at the bottom for Account and Options. If you click on the Account tab (WIN10 + OSX • 52) you will see it offers, just like most browsers do today, to sign in.

This will allow to synchronize your use and settings of Word or other Office programs. If you want to keep your metadata out of your work files, do not sign in.

If on the other hand you click on Options, a popup window will appear. There are two tabs of interest. The first one is the top one called General. Look in the middle (OSX • 53) and you see entries for User Name and Initials. These appear in your documents, so make sure your proper name is not written here. You can change it and click ok.





The other tab of interest, and this is important, is the one called Save. There are two entries you need to pay attention too, shown in (WIN10 + OSX • 54). These are Auto Recover file location and Default local file location.

Throughout your use of Word or other Office programs, the documents you work on will be saved automatically every once in a while. This is in case your computer crashes, so you don't lose all your work. However, these auto saves are placed, if you don't change it, in the Office folder of your OS hard drive, and only deleted after you have saved the documents and closed Word or other Office program. As we have learned in the section on deletion, this is not actually deleted properly, and is very unsafe. So, to protect against this small but dangerous threat, make sure to click Browse and navigate to your encrypted hidden hard drive or USB and select a folder there for this auto save to take place.

FOR PHOTOS

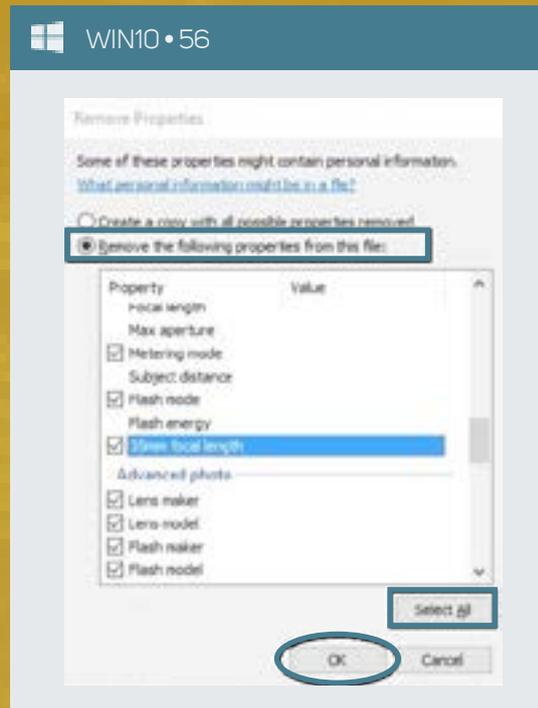
For any photos you have and use on your computer, there are small and effective programs than can remove metadata with a single click. You can also do it manually in Win10 or OSX. If you intend to publish online any photos from your computer, or use inside a report, word document, PDF etc., we strongly recommend that you remove such metadata first.

"For all files, and for both WIN10 and OSX, you can either use the OS's built in function to remove metadata, or use a dedicated program."

For Win10 we recommend MetaNull, which can be downloaded at http://download.cnet.com/Metanull/3000-20432_4-75732772.html. You simply start the program, select which photo (file) you want to scrub (delete metadata from) and select where the new version should be placed (WIN10 • 77). If you afterwards right click on the file and select properties on the new file (Details tab) and compare it by doing the same on the old file, you will see what metadata has been removed.

If you do not want to use a program for it, you can also remove metadata from a file directly in Win10. Just right-click on the file and click Properties. Then click on the tab Details.

At the bottom of the popup window you will see Remove Properties and Personal Information. If you click the button for Select All and then OK, it will remove this data (WIN10 • 55, 56).



For OSX, download ImageOptim from <https://imageoptim.com/mac>, and install the app. Place a desktop icon in an easy to access place (OSX • 56). Once you want to use or publish a photo, start ImageOptim, and drag said photo into the window and select to remove metadata.

You can also go to ImageOptim Preferences to select what kind of data will be scrubbed when you perform this action. On the General tab, select all the choices under Enable (OSX • 57). Making these changes means the selected data will be removed every time you drag a photo into the ImageOptim program/window.

To manually remove metadata from image files on OSX first open the image with Preview. Go to Tools in the menu bar and select Show Inspector. Open the (i) icon in the info panel and select GPS (OSX • 58, 59). After that click Remove Location Info. This will leave some other metadata, but remove any potential location information.



PRACTICAL DIGITAL PROTECTION

CHAPTER 7

DELETING INFORMATION



Delete

This section will teach you how to actually delete files and information, and will show you that everything you think you know about deletion is likely wrong. Together with creating a secure encrypted space for your work files, and using emails and browsing in a safe way, it will go a long way to protect you.

Before you read this section, you will need one important piece of information, is your hard drive HDD (Hard Disk Drive) or SSD (Solid Disk Drive). If using Win10, simply open the search function and find Disk Defragmenter (SearchTerm). Start the program, and it will immediately show what type any hard drive, partitions, USBs, etc. connected to the computer. For OSX, you find out by clicking >About this Mac >System Report >Hardware> Serial-ATA (see "Medium type").

Most of this section is based on your use of traditional HDD, which is still the most common type of hard drive. If on the other hand you have a newer, high-end, laptop or recently purchased external hard drive, it might instead be a SSD. If you have an SSD, much of what is written here does not apply. For SSDs, a special section is included further down, but you should nonetheless read this chapter as normal, especially since it will still apply to other hard drives, USB sticks, etc.

“Safe behavior, strong passwords and encryption won’t protect you from a file recovery program if you don’t consider secure deletion.”

What’s the big deal you might think? When you click delete on a file, or ‘empty recycle bin’, nothing is actually deleted. The document you think you deleted yesterday, or 2 years ago, is still on your computer to be read by whoever wants to. For those in need of protecting information or sources, this constitutes a very big deal. The file might disappear from your Explorer or Finder window, but it is still there, for anyone to read. Accessing such ‘deleted’ files is a favorite of many criminal gangs as well as police and security agents, and it’s very easy to do.your files, videos, etc. The free space consists of the space you have left.

Deletion is a bit of a blind spot for many. That is, even people who are well educated about Cybersecurity often neglect to consider secure deletion. To understand the risks posed by insecure deletion we need to understand how the hard drive works. This applies to all forms of digital storage, such as USBs, SD cards, and computer hard drives.

DATA STORAGE

Different type of storage format works differently. This makes secure deletion more difficult. For this reason, as well as many other reasons already given, you need to limit yourself to what computers, phones, hard drives and USBs you work with. The more you need to deal with, the more difficult it get.

All digital storage (hard drives, USBs, etc.) consist, at the most basic level, of two types of data; free space or available data vs used data. Your used data is of course the space taken up by your files, videos, etc. The free, or available, space consists of the space you have left. However, the free space is not exactly empty space. It is the space on your computer that is not currently occupied with used data and is free to save your new data as you work.

When you delete something, or empty the recycle or trash bin, that data is not actually deleted. It is still there, in the same spot on the hard drive where it was before. What happens when you click delete is just that you have told your computer that you no longer need that data. Once a piece of data has been marked no longer needed, it is considered free (available) space where new files can be saved in the future. As a user, you cannot see the previous data but it hasn't gone away. Think of it as hiding until it is saved over. But with simple software, called File Recovery program, it is easy to find.

The "deleted" data can still be read. Even worse, it requires no technological skills to read it. All you have to do is download a free program, and with the click of a button, all those files will be shown. These programs are common tools by law enforcement and criminals alike.

It is furthermore important to realize that the "deleted" data isn't kept in any chronological. When you save new data it doesn't necessarily save over the older or newer recently free space. It is random. This means you shouldn't have any expectations about what data might have been saved over and what data might remain. This is why it is important to securely delete all data.

For old "deleted" data to be actually deleted, it must be overwritten with new data. Only after that space holding the old data has been overwritten with new data has the old been deleted. To make matters worse, just like with a word document, you can "undo" an action. Maybe you deleted a paragraph by mistake, and you choose undo to recover it. This kind of undo function can also be performed, and an outsider can access at least some of your deleted files even if it's been overwritten. In short, for security, the old data must be overwritten several times, to make sure no one can access it.

Luckily, there are programs that will solve this problem for you. This program is called CCleaner, is easy to use, and it's presented in Technical Solution: CCleaner further below.

SSD DRIVES

Most hard drives are HDD (Hard Disc Drives). Still today, many computers will use HDD. Over time, programs and techniques have been developed to securely delete data of such devices, for example using CCleaner. However, a new type of hard drive is now becoming more common, called SSD (Solid State Drive). They are smaller in size but faster and with higher performance. Because of this, they are still mostly sold for high-end computers, and even if you have a new computer, you are likely to have an HDD.

The Good part. The SSD drives in your laptop will automatically come with a new, special feature enabled. This is called TRIM. It works to delete the material you choose to delete in a far more secure way than a traditional HDD, making "File recovery" by criminals or police a lot more difficult.

The Bad part. The problem, in essence, is that the function of CCleaner (and other similar programs) that overwrites "deleted" data doesn't work, or at the very least, doesn't work very well. In fact, on CCleaner for OSX, this function has been removed completely. Even if you have it, it will not be very useful, and will also hurt the SSD hard drive, wearing it out very quickly. Because the normal CCleaner functions doesn't work, it leaves you without certainty that the information is truly gone, because you don't know when the TRIM command is run to delete it.

TRIM is automatically enabled on OSX computers. In Win10 it is also usually enabled. If you need to make sure, click on the search area, write in "Command Prompt" and right-click on it and select "Run as administrator". In the new window that is shown, copy this code in: `fsutil behavior query DisableDeleteNotify` and click enter. Response should read `NTFS disabledeletenotify = 0`. The 0 indicated it's enabled, a 1 indicates it's not. If it reads "1", then copy in this command: `fsutil behavior set disabledeletenotify NTFS 0` and click enter. It will now be set to enable TRIM.

MOVING FILES

It's important to realize what moving a file actually means. When you move a file, you simply create a copy of that file at the new location, while the file at the old location is "deleted," as in our discussion above. That means that if you, as many people do, create a new word document on your desktop (which is stored on your OS hard drive), and then move it into your encrypted space, the old file will just be marked as free space and easily accessible to any outsider using a simple file recovery program. The same goes with any files you download through your browser to the default download location (almost always on your OS hard drive) and then move to your encrypted space.

One reason it's important to keep files, from beginning to end, at the secure location, is because it ensures there will be no trace that can be found by unwanted parties. Any file that is stored, however briefly, on, for example your C: drive, will be available through file recovery on that hard drive. If on the other hand you store a file directly on a USB and keep it there, once deleted, it will be available only from that USB stick. You can then easily properly delete it from that location using CCleaner.

This is yet another reason your phone should never, ever, for whatever reason, be used to store, even temporarily, a work file. Never download files from your email, for example, onto your phone, even if it's just to read it quickly before 'deleting' it.

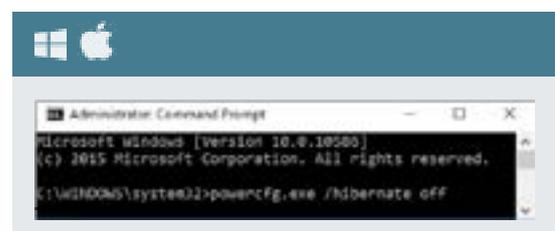
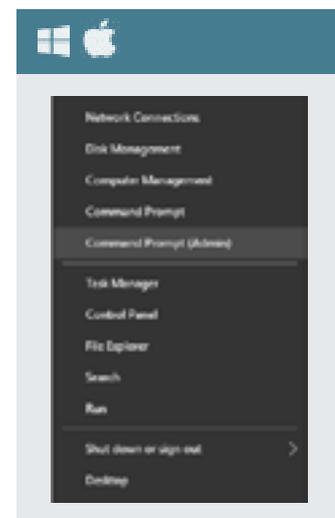
VIRTUAL MEMORY

Finally, on a side note, under Chapter 2: Preparing Your Computer you made a change in the Local Security Policy (Win10), to automatically clear the "page file" when shutting down. In OSX this change was made in Security under Use Secure Virtual Memory. The reason you were instructed to do so is that a computer will work using memory, which keeps information on what you are working on fresh. When you shut down, this memory, called RAM, is cleared. However computers also use part of the hard drive to assist with this, and this area will collect information on what you have been doing. This "fake" memory is called many things, like virtual memory, swap file or page file. Because the change you already made, you have already set your computer to properly delete this every time you shut down your computer. If you don't, the hard drive can contain information on what you worked on earlier, for technically skilled people to read after taking your computer. This problem has here been solved.

HIBERNATION

Hibernation is a function in Win10 that allows your computer to quickly resume operation from where you left off after the computer is turned off. It's tempting to use this function because you can resume your computer work quickly. The reason it works is that the OS will take all your information and save it on the hard drive. When you later start your computer, it will reload all that information. This means that if your computer is taken and started, it will show everything you last worked on, logs on your browsing, and a lot more information. This information is stored without encryption. This is very dangerous.

To disable Hibernation on Win10 click on search area and write in Command Prompt (SearchTerm) and right-click on it, select Run as administrator (WIN - 60). In the new window, write in powercfg.exe /hibernate off and press enter (WIN - 61). Settings about sleep and power use in general can be found by searching Power & Sleep settings.



- When you create a new document or file, do so in that encrypted hidden space or whatever storage you intend to keep the file in.
- Do not create new documents on the desktop.
- Be careful about moving files around, it leaves traces.
- Do not access files or store work files on your phone or pad.
- Do not use hibernation function. When you leave your computer for an extended period or if going to sleep, use proper Shut Down.

TECHNICAL SOLUTION: CCLEANER

CCleaner is a small program that will allow us to solve many problems. This program will both securely delete various kinds of data collected about what you have been doing, like cookies, temporary files, information in Microsoft Word on what documents you have been working on, etc., but also securely clears our computer's free space and "deleted" files.

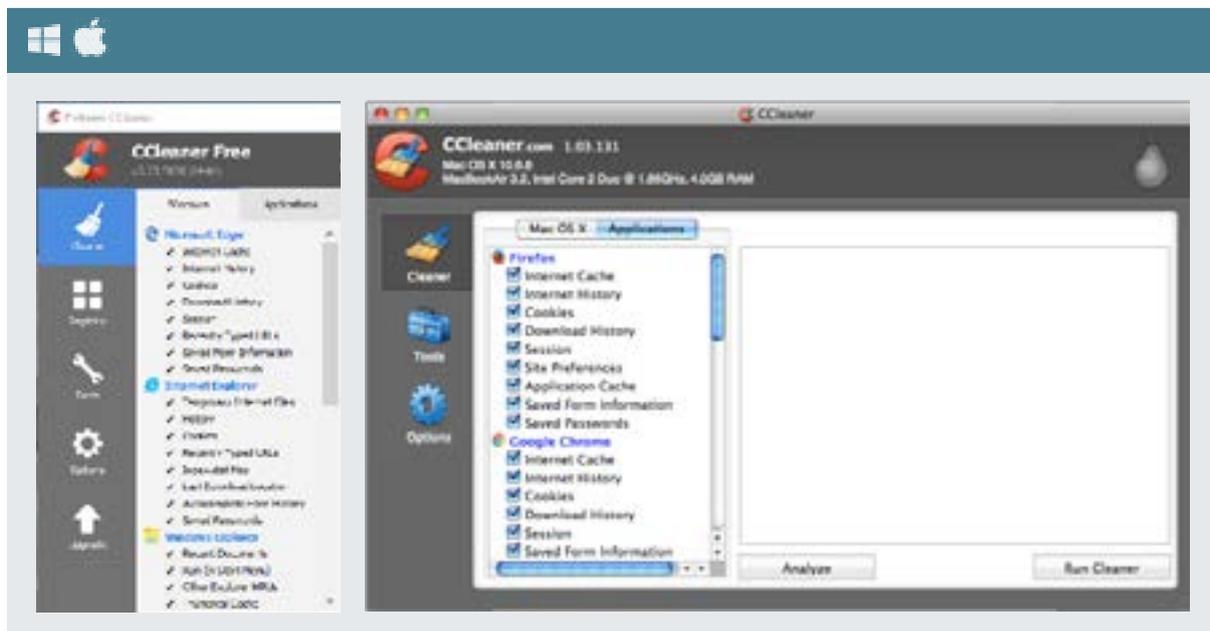
Note: The "Erase Free Space" function will not be useful, or in some cases, even available, if you have an SSD hard drive. However, all the other functions, to remove traces and logs, are, and you should install and use this program nonetheless.

For both Win10 and OSX you can download the program on download.com. After download, install the program. Start the program, either by clicking on the icon placed on your desktop or applications folder. In Win10 you can also right click on the Recycle Bin and select Open CCleaner.

Opening the program you will find several tabs on the left side. The Win10 version has more of them, while the OSX version has only three, but they contain some of the same settings and options.

The program starts on the Cleaner tab. In the window on your right you will also see two tabs, one for the operating system (Windows or Mac OSX), and one for Applications. Under the Windows or Mac OSX tab, select all boxes. These are all the different types of information that will be removed securely when you run the program. In Win10, at the very bottom of the list is the entry for Wipe Free Space (do not select this one for now, any never if you have an SSD hard drive).

Under the Applications tab, you will find more options for what to securely delete. The entries you find depend on what is installed on your computer. Here you should select all boxes with one exception. If you have decided to use a personal use browser, and do not want the information deleted all the time, then do not select the boxes for that browser, or choose which boxes to select (you can remove browsing history, but not saved login information, for example). See WIN + OSX - 62 as example.

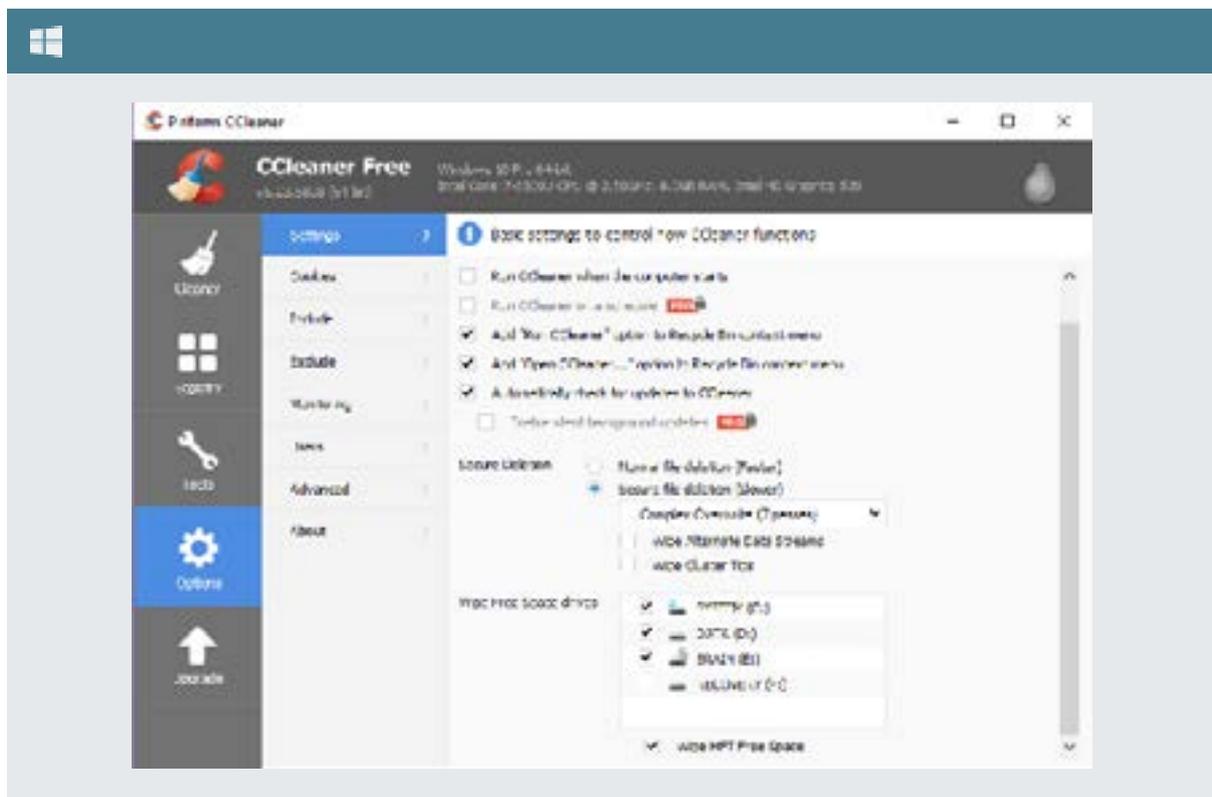


After this, click on the Options tab a little bit below. It will first show the Settings subsection as shown below. On OSX you simply choose Secure file deletion and from the drop down menu select either Advanced Overwrite (3 passes) or Complex Overwrite (7 passes) (WIN + OSX - 63). The higher the number of passes the more secure the deletion but the longer it will take to complete the command.

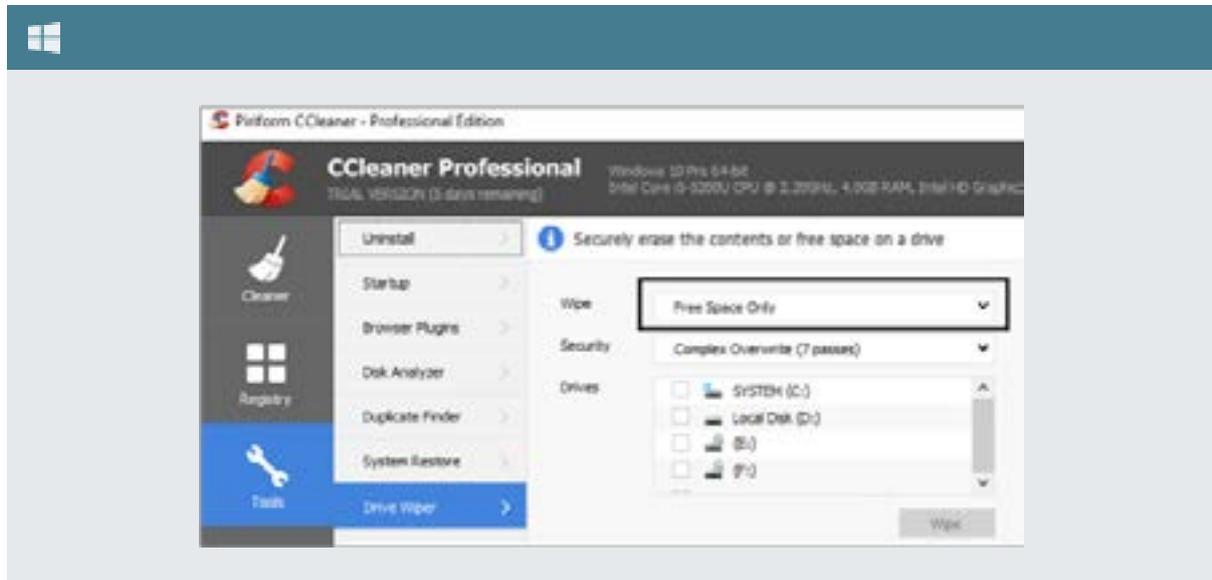
Following WIN + OSX - 63 you select either Advanced Overwrite (3 passes) or Complex Overwrite (7 passes), and can also make other choices. Click the box to Automatically check for updates, and then look at the bottom and select which hard drive(s) (if you have many) to Wipe Free Space. Any USBs in your computer will also show up on this list, if you want to Wipe Free Space from them.

Note: If your encrypted storage is opened/mounted when starting CCleaner, it will also be shown in this list. There is no need to include it. Most of the time, just your regular hard drive (C:) need be selected.

On Win10 you also have another area under Options called Advanced. Click on that, and click on Hide warning messages. You can also select Shutdown after cleaning, if you do, the computer will automatically shut down once the program has finished cleaning.



Finally, you have a tab called Drive Wiper under Tools. This allows you to wipe free space only, without using the full Run Cleaner function—remember earlier how we discussed that free space is really old files you supposedly deleted? Just make sure (WIN + OSX - 64) you select Free Space Only as shown in screenshot, or else it will delete your existing data too.

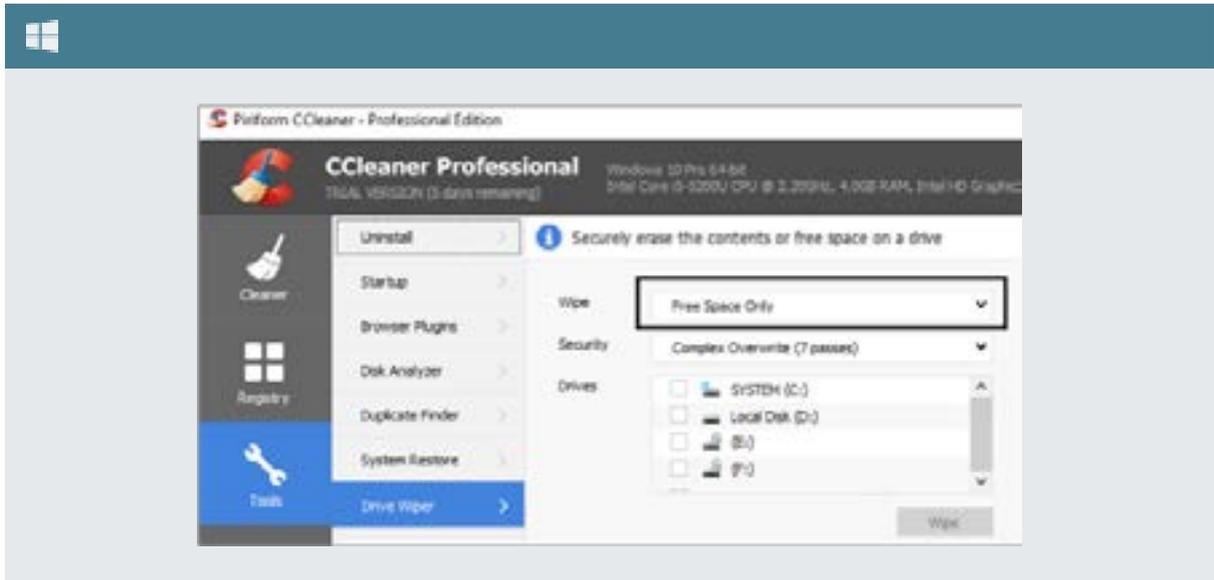
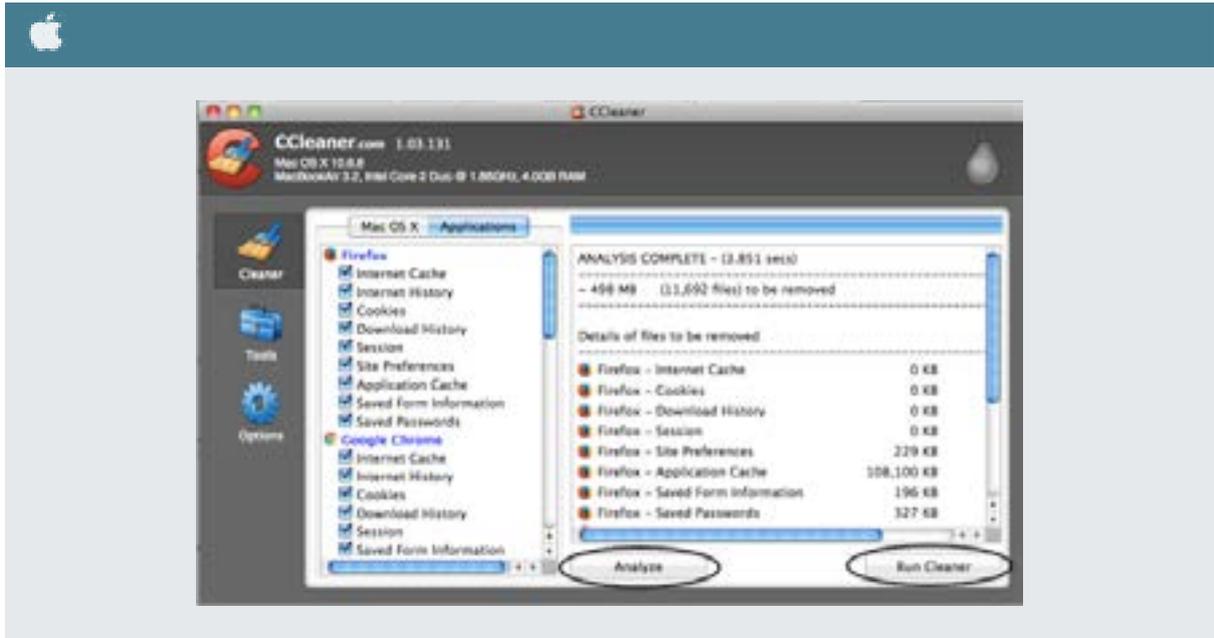


You are now done with setup and can run a test. Go back to Cleaner tab and press Analyze (WIN + OSX - 65). After a quick analysis, it will show what will be deleted. To delete the selected files click Run Cleaner. If you included Wipe Free Space (Win10) and Erase Free Space (OSX), it will take a long time. If you only want to clean traces from your OS, Browser activity etc., then make sure you did not select Wipe Free Space (WIN + OSX - 62), then return and click Analyze again. If you have not closed any word documents, programs affected or browser, it will ask you to close them, otherwise they cannot be cleaned.

USING CCLEANER

You can run CCleaner in two ways, with or without Wipe Free Space—Clear Free Space. Including Wipe Free Space will make the program take much longer (unless you have a very small hard drive). If you simply want to clean up your data traces, then run the program without having selected Wipe Free Space. Do this often. In fact, once you finished your daily work, you should ideally run this before you shut down the computer.

If your security situation is heightened at any given period you should also take the time to run the Wipe Free Space/Erase Free Space on your computer's hard drives. You do this by either including it when running a Run Cleaner, or you can use the special Wipe Free Space tool presented in WIN + OSX - 66.



USE CCLEANER TO SHUT DOWN WIN10

While checking out the Advanced tab of the Options area (WIN10 • 65) you saw a box that said Shutdown after cleaning. If you select this one, your computer will shutdown automatically after having completed CCleaner.

If you are using Win10, it is strongly recommended to check this. After this, you simply shutdown your computer with CCleaner instead of the normal Shutdown button or function. Because you are shutting down, it doesn't matter that it takes longer, as you are leaving your computer anyway.

In the future, you can click Run Cleaner instead of clicking Shutdown, and both clean your traces, wipe your free space, and shutdown with one click. Again, you need to select the option for Shutdown after cleaning for this to work.

To make it even easier, you can create a button (shortcut) on your desktop, and by clicking this button CCleaner will run and then Shut Down automatically. We recommend you make a shortcut of the CCleaner icon to your desktop, and then rename it SHUT DOWN. After this, right-click on the icon, select Properties. Locate the "Target" line, which will include the path to where the program is located. At the end of that line, add /AUTO /SHUTDOWN. After adding it, It will look something like this: "C:\Program Files\CCleaner\CCleaner64.exe" /AUTO /SHUTDOWN

Click Apply or OK, and then you are set. In future, when you are about to leave or shut down, simply click on the icon, lock your computer, and leave.



METADATA AND JOHN McAFEE

It was the story of an internationally renowned computer expert in 2012 that got people thinking about the dangers of metadata. And yet, most people are still unaware of what Metadata is and how it poses a risk. The American John McAfee is one of the creators of the McAfee Antivirus Program, one of the most successful antivirus programs ever created. In 2012 while living in Belize, he was wanted as a person of interest in the murder of a neighbor. He has since returned to the United States and has been exonerated. However, despite being innocent, he was paranoid about the police and went into hiding. His secret location was ultimately revealed following an interview he gave with a VICE journalist. The journalist had taken several photos during the interview, which were later published with the VICE article. The journalist didn't realize what kind of information a photo can reveal.

Once the article was posted, it was easy for people to download the photo and scan it for metadata. Anyone with even just basic computer skills could quickly see when the photo was taken, what phone it had been taken with, and the GPS location of where the photo had been taken. Not long after the article was published, Belizean police detained McAfee. He spent an agonizing period in a run-down detention center, before being released and deported.

The moral of this story is obviously even more important for human rights defenders in a repressive state than for someone who just doesn't want to be found, like McAfee.

PART III PHONE SECURITY

PART III OF THIS MANUAL CONTAINS SEVERAL CHAPTERS, ALL OF WHICH CONCERNS YOUR PHONE.

CHAPTER 8

Understanding Phone Security will provide some general information on how phones work and what the main security issues are.

CHAPTER 9

Using Your Phone will present some guidelines on how you should use your phone in a secure way and some other issues concerning your behavior with your phone.

CHAPTER 10

Settings Up Your Phone is, like Chapter 2 for your computer, a boring chapter which deals with basic settings on your phone, and how you can change those settings to increase security.

CHAPTER 11

Secure Apps For Use will present you with relevant Apps that can allow you to continue using your phone effectively, but with stronger security.

CHAPTER 8

UNDERSTANDING

PHONE SECURITY



In this chapter we will cover how your smartphone can be used to spy on you, what the main threats are, and show how installed Apps increase security risks.

First off, even though phones today are like small computers, they are limited in power, and therefore limited in how much you can do to solve security threats. In short, your phone will never be safe. This is important to remember. If in doubt, or in a situation of heightened security concern, never rely on your phone. Turn it off, when possible remove the battery, and leave it somewhere safe. As long as your battery is in the phone you can be tracked. If you need to bring the phone, look at Going Dark in Chapter 9: Using Your Phone.

“In short, your phone will never be safe.”

You can test for yourself how your phone can pose problems for you. Remove the SIM card from your phone. Take a walk. If you check your location function you will see it remains working even without the SIM card. If you can follow your movements on Google Maps or other programs that means so can the police or anyone else who wishes to track your activities. This is because as long as not in “flight mode”, your phone will continue to use radio waves. This is how the phone connects to the phone network for phone calls, SMS and tracking. This is also the reason that even without a SIM card, all phones can still call emergency services. This means that police can track you whenever they want.

This brings us to problem one, location tracking. Location tracking functions mostly work like this: Every once in a while your phone, even if you don't make a call or send a text, sends out a radio signal, which will be picked up by the nearest cell phone tower. Your phone keeps in constant communication like this so when someone calls you or texts you, your phone is ready to receive it. In large cities there are a lot of these cellphone towers, and by looking at how your phone connects to them, they can pinpoint the location of your phone very narrowly, sometimes down to which room in a house you are in (triangulation using several different cell

towers). These days' phones also have GPS functions, and can also use your wireless internet connection to help with this. This means the only time your phone is safe from tracking is when in "flight mode" or otherwise blocked from accessing these various signals. Finally, these days many apps on your phone also request your location, such as WeChat. This opens up more options for police to locate your phone. Location tracking is not the only problem to think about.

If you are concerned about your conversation with colleagues, clients, or sources being overheard, then the phone again presents a problem. In technical terms, using your smartphone to eavesdrop on your conversations is called using a "roving bug," but in normal terms we can just call it eavesdropping.

To eavesdrop on your conversation first the police have to identify your phone. This is easy since China requires real-name SIM card registration. While unregistered black market SIM cards might slow down this process they aren't a guarantee, since the police can simply identify the phone that is sending signals from your known location, such as your house or office. After your phone has been identified it is possible to access your phone and turn on the microphone to record and transmit anything within microphone range. This is performed as a background service and runs without notification so you won't know. In the same way, the camera on your phone can be turned on without your knowledge and used to record you, your clients, and surroundings. Remember, the risk of remote access microphones and cameras also applies to your computer.

"The camera and microphone on your phone can be turned on without your knowledge."

Today's smartphones pose more problems. The way earlier cell phones were designed made it easier to neutralize these threats by removing the battery completely from the phone. These days, phones can be turned off but often batteries cannot be removed. Or if the battery can be removed, most phones come with a built-in small extra battery. This is done so that, for example, even if you turn off your phone at night the alarm will still sound in the morning or if you've left your phone off for a while your calendar and time zone settings will be correct when you turn it on again. Even when your phone is turned off and you have removed the battery, some country's police have managed to eavesdrop anyway, because this small battery allows intrusion just as above. So, simply turning off your phone will never provide proper security, and removing your battery is becoming less and less the security measure that it once was.

"...simply turning off your phone will never provide proper security."

If you are a serious risk to the police, there are of course more ways they can access your phone, read your documents, take screenshots, and more. These days you do not need to be an expert hacker to achieve these things.

Due to such threats, your phone, as far as possible, should be treated only as a communication device and not a small work computer. Never download or store sensitive files, documents or photos onto your phone. Properly erasing files from a phone can be real difficult, and if you remember from the chapter on deletion, just deleting a file doesn't actually remove it. As such, do not use your phone to store, even temporarily, any work documents.

IMSI catchers is a new favorite tool of many countries police, and is a small, easy to use and cost-effective tool for phone surveillance, often used during demonstration, larger gatherings and other events where many people are congregated. An IMSI catcher pretends to be a cell phone tower (base station), and all nearby phones connect to the IMSI catcher, thinking it's a cell tower. These IMSI catchers are now so small that they can not only fit in a suitcase, but are sold as personal carry equipment. Your phone's encryption standard is always set by the cell tower, not the phone itself, so the IMSI catcher instructs your phone to use no or very basic encryption. Police can then identify all phones in any area, record all signals and data, and directly read it. The IMSI catcher thus places itself between your phone and the cell tower. This is usually called a 'man in the middle' attack, and is also used for computer and internet traffic, although it works differently then.

Finally, again to remind you, besides these risks, which are posed by the way that phones function, the Apps you allow on your phone will allow the same type of access but through the Apps instead, often even easier. Be careful what you install, and realize anything local is automatically dangerous, because police have direct access to these companies and their servers, and these companies do not provide you with legal protection against giving anything to the police once asked.

IS YOUR PHONE BUGGED

In older days it used to be fairly easy to figure out if your phone was bugged. Repeating clicking sounds was common to hear if your landline phone was tapped, or irregular interferences and reverberations is heard on your cellphone. These days, a lot more eavesdropping is carried out through hidden Apps, and is more similar to computer hacking than classic phone tapping. However, regular phone tapping continues to be used widely.

As such, there are a few things to consider.

In general, if your phone line is being monitored, it will produce noises, because the link is shared with another listener. If you grew up in a household with several phones to one landline, you will know that if someone else lists up the phone while you are talking it will change the background noise and you will clearly notice.

To be able to use this, you need to pay attention to the regular noises you hear when you call a specific person. If you notice changes in the type of noises, that is a cause for concern. However, calling different people in different places will have slightly different noises, so you have to compare with this specific person and phone, and see if you notice changes. Typical sounds are:

- repeated clicking sounds
- static noise interference
- high-pitched humming

To test for this, make sure you are not in close proximity to other electronic devices (TVs, routers, computers etc.) which could be responsible for the static.

If your phone is compromised through apps or background processes instead of tapped through the phone line, you are also likely to notice certain things like:

- random SMS messages contained random text, numbers etc. (a bug in the monitoring software that fails to keep these SMS, used to control your phone, secret)
- heavy battery drain
- popup advertising
- slow, bad or uneven performance
- increased data use
- overheating

KEY TAKEAWAYS

- Be aware of the type of threats that exist for phones
- Limit the amount of Apps you install
- Review your phone settings and go over pre-installed Apps, removing all those you don't need
- If in doubt or feel in danger, do not use your phone, do not bring it with you, do not leave it turned on
- Do not use your phone as a work computer, it's only a communication device
- Avoid Chinese companies' Apps and services
- Google (or even better, DuckGoGo) is your friend - anything in your phones' settings area, or any pre-installed App you do not understand or know what it does, just check it online by Googling it

PRACTICAL DIGITAL PROTECTION

CHAPTER 9 USING YOUR PHONE



This chapter will show you how your behavior, i.e. how you use your phone, will be far more important for your safety than the technical solutions that can be offered.

WHAT YOUR PHONE IS NOT

Unlike with a computer, you cannot protect your content in any effective way. Even if you do keep it encrypted (and most phones are encrypted automatically these days), you cannot use any more advanced method for it. There are few layers of security from the PIN code you enter to access your phone to all the different parts of your phone. For keeping what's inside safe in case you lose the phone is not a major issue, but keeping it safe from police or criminals if you have been taken and am forced to provide the PIN to start the phone is. In the latter respect, your phone is un-protectable.

Because the lack of layers in offering protection, and the common use of Apps to access services instead of using a browser (and the lack of properly clearing traces from phone's browsers'), if you are forced to give out your PIN they would not only get access to what is on the phone, but to any services for which there are Apps on the phone for, or those access through the browser recently. Through these, whoever is forcing you can get easy access to services otherwise well protected. They can thus use your phone as a backdoor to what would otherwise be safe. Do not allow them to use your phone to circumvent your security, i.e., do not use your phone as a secondary work computer.

“Unlike with a computer, you cannot protect your content (on your phone) in any effective way.”

All this means that your phone is not a secondary work computer. It should never, ever, store any work documents, be used a transfer device for files, nor should you allow access from your phone to any work services you use on your computer.

WHAT YOUR PHONE CAN BE

Despite all that has been said above, and in the previous chapter, your phone can be a very efficient and safe communications tool. The key is to use it only for this purpose, and not allow it to be used as anything else. Another step to take to achieve this is to use secure Apps for such communication, which allows for automatic destruction of your messages (logs), to prevent outsiders being able to track and map earlier conversation if they get their hands on your phone. End-to-end encrypted chat programs coupled with automatic destruction of your chat logs is a powerful and efficient tool for communication.

GOING DARK

Going dark, meaning to cut your phone off from any type of transmission, is the only way to be sure your phone is not being used against you. If you are in a discussion and want to make sure your talk is not recorded, it's the only solution. Likewise if you don't want the camera to record you, or the exact location of where you are to be known, you have to go dark. You can do this in several ways, and the easiest and most overlooked way is to turn on Flight Mode. By doing so you will stop cellular network transmission (phone traffic to cell phone towers), wireless internet transmissions, as well as Bluetooth. Whether it will turn off receiving GPS signals varies by phone. However, smartphones only receive GPS data, it does not (nor can it) send it. That means that as long as other forms of transmissions are turned off, you are safe.

One weakness with the above is if an App turns on data transmission without your knowledge, which can be done if your phone is targeted. Another is that your GPS location will still be recorded if you have GPS turned on, and that location data could be sent by an App later on when you are no longer in Flight Mode.

Another way to go dark, in a very easy manner, is the use of aluminum tinfoil. Many people who work with sensitive issues and are at risk will often pack a few sheets of aluminum tinfoil in their bag and have it there. By wrapping your phone in two layers of tinfoil (covering all parts of the phone) you will kill all transmissions. It is your best method for going dark. These days' online stores also sell special small phone pouches, lined with tinfoil on the inside, which will achieve the same thing, without looking suspicious. We recommend you to test it. Wrap in your phone in two layers and try to call it. Send it a message or an email and see if it receives it (makes the relevant sound). If it does, then you need another layer, but it's very unlikely. However, if you want to use this method, even just as a backup, test it first so you know the results for your own phone.

“By wrapping your phone in two layers of tinfoil (covering all parts of the phone) you will kill all transmissions”

AUTO-SYNC AND BACKUP

Another major security threat with phones is that it comes with automatic login to many services. These Apps often only have a limited interface compared to the full service available in a browser. However, the access is usually not password or PIN protected. Access to your phone thus means access to all services installed. Do not underestimate how big of a threat this is. Never install Apps for work related services you usually access through your work browser on your computer, despite how tempting it might be. Likewise do not use any cloud storage service, or other online service, on both your work computer and phone. Use separate account and services. If you insist on using cloud storage for example, use Google Drive on your work computer, and use Dropbox or OneDrive or something else for your phone. Keep your work computer and your phone, and the services they use, separate.

The key for safety is thus to limit how you use your phone, and a view your phone solely as a communications device, and not use for work purposes other than communication. Do not do online research with your phone, do not download documents, or have work files on it.

**“Keep your work computer and your phone,
and the services they use, separate.”**

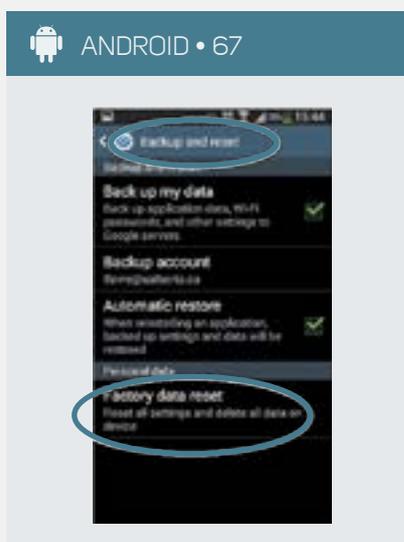
Flight mode will also turn on NFC (on Android sometimes called Beam), which is a short-distance transmission system – basically you can put two phones next to each other and they can communicate and transfer data.

THREE INITIAL STEPS TO SECURING YOUR PHONE

Before moving on two the next two chapter, first on basic settings for your phone, and secondly to recommended secure Apps and how to use them, you will need to take three steps.

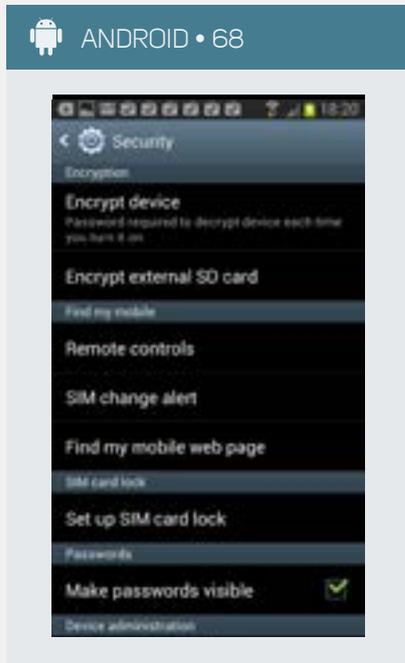
STEP 1: FACTORY RESET

Unless you have a complete understanding on what is on your phone, and feel very secure in the current state of phone security, you need to start securing it by doing a factory reset (ANDROID • 67). This will make you lose anything on your phone, so back up any photos or other files you might have and want to keep.



STEP 2: ENCRYPT

Your phone might come with encryption already enabled. If you have an Android, chances are it is not. The phone, and any SD card in it, can be encrypted very easily. After doing a factory reset, the first things you do is to turn on encryption if not already turned on, and select a suitable PIN code or password. Include the SD card (if any) when you do this. (ANDROID • 68)



For your Android phone, you simply need to go to Security under Settings and click on Encrypt device, and it will ask for a PIN code or password and start the process. No data will be deleted. You can also choose to Encrypt external SD card, and if your phone uses an SD card, you should do this after you have encrypted your device.

STEP 3: REMOVE/UNINSTALL

Go over the Apps and Services installed on your phone after factory reset and encryption has been done, and uninstall or disable any and all such Apps and services you will not be using. Many phones comes packed with Apps even after a factory reset. Remove all of them, which will help with your safety, but also makes your phone faster, and let the battery last longer.

HOW A PHONE ALMOST DESTROYED IT ALL

The person behind this story is neither a lawyer nor a journalist, nor is he based in Beijing, Shanghai or in other rights-defense hubs. Instead, he lives in a secondary town outside one of the provincial capitals in one of China's eastern poorer provinces. Neither is he university educated, having not even finished high school. However, what he lacks in degrees he makes up in practical experience. Over more than 10 years he has worked tirelessly to help victims of illegal government actions in his own community, and slowly as his reputation has increased, in other parts of the region.

Despite being outside the big cities, in today's modern China, he would of course use both emailing, his computer to learn and study China's laws and how it could be used to help whatever client he was working with, and his phone was his principal nerve center, the most efficient way to organize support. Often, when yet another farmer was to have his land taken from him with laughable low compensation, he would organize other farmers and victims to come together to assist. Numerous were the times many of those contacted would never show up, having been visited by police even before leaving their home. Other times they would disappear midway, only to reappear a few days later, after having spent time under 'administrative detention.' It didn't take long for him to realize his messages to others were at least sometimes being read, and used against him.

Being far smarter than his lack of education might otherwise suggest, as with the law he had learned himself step by step, he started learning how to communicate securely, sharing his ideas, knowledge and tips with others as much as he could. Even though he had been blocked by police from leaving his house, taken in for forced 'tea chats' and even twice been placed in short-term administrative detention, as a local activist he had little reason to fear any greater scrutiny of his work or attacks on him.

When, late 2015 he was picked up at home by two local officers he had many interactions with before he wasn't overly concerned. Once at the local station however, being met by a group of provincial police, and later taken to the provincial capital, he quickly realized he might be in a world of trouble. It quickly became clear he had overstepped the line, and his phone was quickly removed from him, and later he would realize, his computer, camera and other equipment from his home taken as well.

The police having his phone didn't make him overly concerned. Most chatting was set to destruct by itself, and the few chat logs they might access could of course show that he had instructed people to partake in various activities, but it was mostly just directions and brief talks. With those chats, it be hard to show him as instigating others. He felt rather certain of this. He, like many activists, had sworn to himself never to incriminate others, which meant he was dead set on never giving out his password to his email. He was already using a blocked email service, Gmail, known for strong protection, which required him to use a VPN to access it from both computer and phone. They stood little chance of getting access to that.

In the end, it was all in vain. The police didn't exactly consider him a top threat, just a nuisance. It was not like they would devote massive resources to try to crack Gmail's encryption. And in the end,

they didn't have to. He had installed a Gmail reading App on his phone, and as soon as they had access to his phone, they had access to his Gmail. Sure, the App doesn't let you check passwords or make changes, but all they need was to read what was in there, and they could present a convincing picture of a professional instigator. That he had enabled location sharing, important for many daily interactions on WeChat, also meant that all his photos, often taken at meetings and public disputes offered police both time of these meetings and the location, as the photos contained that as metadata.

Luckily it had been an intentional policy for him to delete older emails, always worrying that such things could somehow hurt him or others later on. Because of this, with only a limited amount of 'evidence', police let him go after a maximum 15 day administrative detention. Even though he avoided formal arrest, police made it clear he had gone too far, and next time he overstepped his bounds he wouldn't be so lucky.

In the end, that long password to use VPN-accessed email wasn't worth very much since he offered anyone with access to his phone a direct backdoor into it. It's likely not a mistake he will make again.

PRACTICAL DIGITAL PROTECTION

CHAPTER 10 SETTING UP YOUR PHONE



This chapter, must like Chapter 2: Preparing Your Computer, will provide information on settings you can control on your phone. As with computers, getting to know these settings, and making suitable changes, is an important step, and always the first step, to securing your phone. No amount of Apps or programs can secure your phone unless the basic settings have been adjusted first.

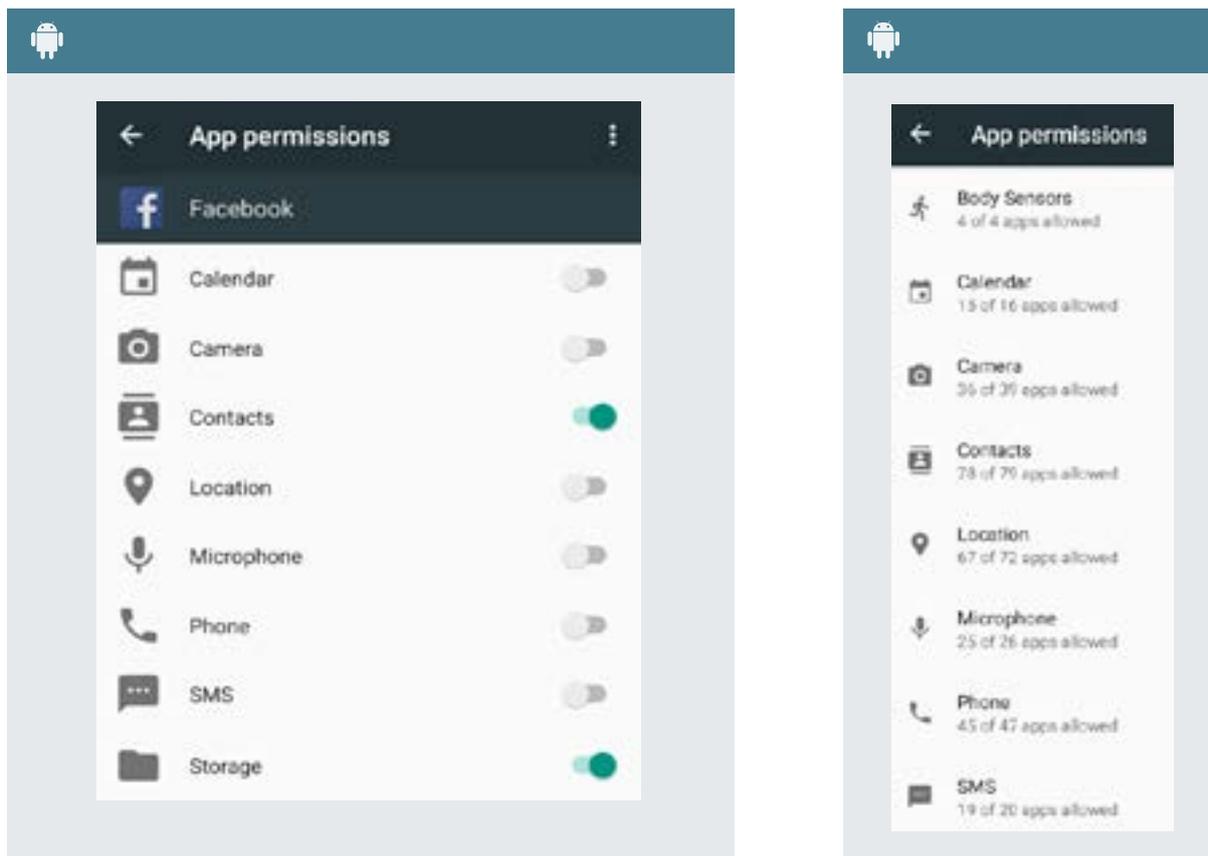
We are now ready to go over the settings area of your phone, and make the changes needed to bring you basic security. Because Android phones vary in appearance and layout of the menus and settings area, but almost always use the same terms and expressions, we will provide the terms or expression and let you find it inside the settings area of your phone, instead of showing step by step screenshots of every step, as it wouldn't apply to many of you anyways. It will also allow you to familiarize yourself with the settings area of your phone if you have not already.

Due to changes between different versions of the OS on phones, and different makers of Android phones, some phones might use different terminology, or change how to find a setting. If the below instructions don't work for your phone, use DuckGoGo or Google to find the way to make this changes on your phone.

SETTINGS AND APP PERMISSIONS

For Android phones, we will go over the Settings area. On Android, if you have a Google Settings area, we also need to go over that.

The easiest way to get control of your phone and limit what Apps can do is to either access the Application Manager, and click on each App, and select what right that App has, for example access to your calendar, your camera, your location, etc (ANDROID • 69).



On many phones (but not all) there will also be another settings area where you instead can check each service (Android – 69 and 70), for example Location, Microphone etc., and see what Apps has permission to that particular service. You find these settings by:

SAMSUNG: Settings > Applications > Application manager

ANDROID: Settings > Apps > Select which APP

SAMSUNG: Settings > Privacy and Safety > App Permissions

ANDROID: Settings > Apps > Permissions > Select Permission category

Unfortunately Apps will often ask for maximum amount of access even when it's not needed, and even when an App cannot even use that permission. Because of this, it's important to set aside some time and go over either of the two areas mentioned above, and check permissions given for everything. This is the best way to properly control what Apps can do on your phone.

This also means you have two choices. You can either turn off a service completely, for example Location, or you can allow it, but micromanage what Apps are allowed to use it. You are always better off turning off a service completely, but that might not always be suitable and effective for you. If you leave a service on, make sure to review (as above) which Apps are allowed to use it, and do it regularly after installing any new Apps.

Location, Camera and Microphone are the three key services to pay attention to. Other types of permissions you can control include read/send SMS, access your storage, calendar, contact list, read/send emails, etc. Make sure you have total control over what Apps can use your location, camera and microphone. It is strongly advised to turn off location entirely.

You should turn off other connectivity that you do not use. Besides Wi-Fi, your phone also offers Bluetooth, NFC and in some cases Android Beam. Turn all these off unless you are actively using them. These are short-ranged wireless connectivity options and there is no need to keep them turned on unless you regularly use them.

SAMSUNG: Settings > Bluetooth + NFC and Payment + More connection settings > set Nearby device scanning off

ANDROID: Settings > Bluetooth + Wireless & Networks > More...

What can be installed? Under the security and privacy sections, you will find settings allowing or not allowing Unknown Sources. You should not allow this. This will block allowing installation of any programs or Apps that is not verified by the official phone store. If you need install something special you simply turn it off while installing said program, then turn on again. For iOS Phones you do not need worry about this, as only Apple Store Apps can be installed as standard.

SAMSUNG: Settings> Lock screen and security

ANDROID: Settings> Security

NOTIFICATIONS, LOCK SCREEN, AUTO-UNLOCK AND AUTO-DESTRUCTION

If you are to protect outsiders from accessing messages and other forms of communications on your phone, protecting your lock screen is key. Most phones comes pre-set to show notifications in full on your lock screen, meaning you can read new messages, emails, etc., on the lock screen without having to open the phone. This need be changed. Again, like above, you can either set to hide all notifications, or you can choose to allow them, and then check the list under that settings and allow/deny for each individual App. Regardless of your choice, no App used for work should be allowed to show notifications on your lock screen.

SAMSUNG: Settings > Lock screen and security > Notifications on Lock Screen

ANDROID: Settings > Sound & Notifications > When Device is Locked (select Hide sensitive notification content

You can also control what Apps can or should give you notifications in the phone (not on Lock screen). There might be Apps you don't want any notifications from at all, and only check manually.

SAMSUNG: Settings> Notifications

ANDROID: Settings> Sound and Notification

ANDROID: Settings > Sound & Notification > App Notifications

ANDROID: Apps > Permissions OR Apps > Click Gear Icon > Select App Permissions

While you are dealing with the lock screen, make sure to enable Lock Automatically and set the time to something short, like 5, 10 or 15 seconds. Also enable Lock instantly with power key if possible (lock screen goes on when you push the power key). Finally, enable Auto factory reset. This last setting means that if someone enters the wrong PIN to your phone 10 or 15 times in a row, your phone will automatically be reset/wiped.

SAMSUNG: Settings> Lock screen and security > Secure Lock settings

ANDROID: Settings> Security

You already selected a PIN or password when you turned on Encryption, but if it's for some reason not enabled for the Lock Screen, make sure to enable this. Also, if your phone or pad allow fingerprint (touch), voice, face-recognition or retina (eye) recognition as a way to unlock your phone or pad, turn it off.

AUTOMATIC UPDATES

As with your computer, your phone is only as safe as the latest update. Make sure to enable automatic updates for your phone.

SAMSUNG: Settings > About Device

ANDROID: Settings > About Phone

SYNC AND CLOUD STORAGE

Identify any built in cloud service, which should show up in your settings area, and make the changes needed. Make sure any such cloud service is either turned off, or that it does not include anything related to your work. If you want to use Cloud based backup or storage, please refer to Chapter 6: Sharing Information and decide how to best use it, and what services to use.

A few last notes on phone settings.

For your Android Opt out of Interest-based ads (Android).

ANDROID: Google Settings > Ads

For safety, you might want to either turn off voice command functions (OK Google, Cortana, Siri etc.), or at least make sure it cannot be used when Lock Screen is on.

Finally, if you use an Android phone with Google Settings on it, browse the area and make sure you are aware of the settings, what Apps and devices are connected to your account, and turn off Smart Lock for Passwords, and make other changes as you see fit.

KEY TAKEAWAYS

- Make sure new messages, emails etc. cannot be read directly on the lock screen.
- Make sure you have complete control and understanding of Apps and functions that can use your location.
- Double-check what permissions your different Apps has, and change accordingly.
- Make sure your camera never has access to your location.

A NOTE ON LOCATION TRACKING

Be aware that if you feel a strong need to avoid tracking, letting your phone 'go dark' will not solve your problem if you have police, state security or mafia after you. Your car will be automatically mapped in how it moves by road security cameras, toll cameras on highways, and toll cameras in cities. Likewise, your use of credit/debit cards, or use of any other cards registered or tied to your name, be it a library card or similar, can also give away your location. Friends posting photos of you can also give away both location and time of when photo was taken, and is easily identified by automatic analysis, should someone decide to dedicate enough resources to track you down.

Going dark for any longer periods is more or less impossible, and even for shorter periods very difficult unless you are prepared with cash, means of transportation, etc. These days even normal security cameras in a shopping mall can scan for identifiable characteristics in your face, and do so quickly. Do not underestimate how sophisticated some of these technologies has become.

Your phone is identified through through unique identifying numbers, one for the hardware itself, and one for the SIM card. These are called IMEI (your phone) and IMSI (your SIM). These numbers are registered by the cell tower and data/phone provider, such as China Telecom. You cannot hide or change these unique identifying numbers. If your phone is known, the state will likely know at least the IMSI number, and if your phone is taken, can find your IMEI numbers and check it against stored data by the phone service provider. With this, they can map all your metadata (location, numbers you have called, data used, etc for a long period backwards). Again, your phone is a great risk and should be limited as a work tool.

In short, never take steps that puts you in such a situation. Your work is important, but your safety must come first. Living to fight another day should be your guide.

In this chapter we will present a string of Apps and programs that can do what you need done, in a safer and better way. We will replace the built in SMS managing program for one that can do the same but with end-to-end encryption, we will show how to easily use TOR automatically to surf the web securely and without limitations, and present chat programs which not only encrypts but automatically destroy your chat logs.

When you first install an app, make sure to go to its settings area, and familiarize yourself with the Apps possible settings. Some secure Apps, like Signal and Telegram, comes with built-in, or native, PIN and password protection. This means that the Apps allows you to set an individual PIN code to access that App. For Telegram and Signal, this is a must. Many Apps however do not allow for this. By using a native PIN for an App you can make sure that even if your smartphone is accessed, access to some specific Apps are still blocked and therefore safe.

SMS AND PHONE CALLING



Install Signal Private Messenger, an App that will replace both your SMS and phone calling program. When sending SMS (Settings > EMS and MMS > select SMS Enabled) or making a call to anyone using Signal, you will automatically use end-to-end encryption, protecting your SMS and phone calls from eavesdropping.

It comes with a built-in (native) PIN or Password protection. Turn it on and use a specific PIN code for accessing Signal (Settings > Privacy). For messages, which when on Wi-Fi will function just like normal chat messages (not sent as SMS, and therefore save on money) (Settings > SMS and MMS > enable Wi-Fi Calling). Finally, enter settings again and Chats and Media and enable Delete old messages and set the length (for example, it

will auto delete anything more than 5 most recent messages).

Once you start a chat, click in the upper right corner and you will see an option for Disappearing messages. Click on this and select a timer. This means any messages sent and received will be deleted after set amount of time (after having been read).

To use the 'end-to-end' encryption, for chat messages, SMS and phone calling, both you and the receiver must have Signal Private Messenger installed. As such, make sure you install it, and let your coworkers, partners and friends do the same. Even if an ISMI catcher is used to remove your normal phone signal's encryption, you will remain safe, as the program uses its own 'end-to-end' encryption.

CHATTING



As a complement to Signal Private Messenger, we recommend you to install Telegram. Telegram can function like a normal chat program (with normal encryption), but also have another function called Secret Chat. If using secret chat, your messages are end-to-end encrypted, and you can set an auto-destruction timer for all messages sent and received.

As has been mentioned before, the automatic destruction of the chat logs is key for your safety, more so than advanced encryption, as it leaves no evidence that traces and information that others can steal or use against you. As with Signal Private Messenger, Telegram has a built-in or native PIN/Password protection. Select a unique PIN code to open Telegram.

SURFING, TOR AND VPNS

The easiest way on Android to securely surf is to use the Guardian Project's Orbot or OrFox app.



Orbot is TOR for Android, and is the app that starts TOR on your device. You can, in the settings area, select which Apps should be routed through TOR (that is, which Apps should be connected through the TOR connection), and you can select all if you want. After this you can start any browser and surf through your TOR connection.



OrFox is another app, a browser specifically built to be used with Orbot/TOR. If you start OrFox, that browser will automatically connect through TOR, and you do not have to do anything else. However, in this case, only the OrFox browser is set to use TOR, all other connections are as normal. If you use OrFox, before you start surfing, go to settings area and select Privacy, and then click Clear private data on exit and select all forms of data. This will wipe traces of your browsing once you close the App.

If you use other browsers for surfing, it's strongly recommended to never use the built-in browsers. Always uninstall those, or if not possible, disable them, and then download a reputable browser such as Opera, Chrome or Firefox. As with your computer, make sure to enter the settings area and turn off automatic saving of passwords, auto-fill of forms, etc. Also turn on Do Not Track and make sure to click Clear browsing data after finishing using your browser.

Again, do not use your phone or phone browser to access your work services, like emails, cloud storage etc. Never, ever access through your phone. Data cannot be properly wiped on a phone.

As of recently, no TOR browser or App for iOS phone has worked in mainland China. However, it changes over time, so enter the App store and look for TOR apps, which will often specify how they are or are not working in mainland China at the moment. VPNs function the same way on phones and pads as on computers. If you have a proper, paid for, VPN it will likely come with a phone app to use for connection to the VPN.

METADATA

As was mentioned in the earlier chapter on Metadata, the collection of such is often even worse on phone, as the photos taken can include location and automatic naming on people that appear in the photo from your contact list. As such, you will need to consider this when taken photos from your camera to use on any publishing (social media), transfer to computer to use in documents, publishing etc., or for any other use. In phone apps metadata programs often use the term Exif or Exif data (Exchangeable image file format).

If you take the photos to your computer you can wipe the metadata using your computer and the methods we have shown. If you want to direct publish something from your phone however, you will need to install a metadata wiper program.

For Android we recommend Exif Eraser or Metadata Remover. Both of these are easy to use but there are also many other options. Install a program and test it, to make sure you understand how it works. If uncertain, test another program until you have one you feel comfortable with. Almost all the programs have instructions on how to use them online.

OTHER APPS

The Guardian Project mentioned above also produces several other types of security Apps.



Amongst them is ChatSecure, a client program for managing/using chatting on both your Android and iOS. Using ChatSecure allows you to use for example GoogleTalk/Chat with strong encryption, and can be set to start automatically with TOR. That would mean any communication on that account would only be through TOR connection. You can also PIN or password protect the program, as well as set automatic deletion of messages.



Another popular App from the Guardian Project is ObscuraCam. It's a camera App that identifies faces in the photos you take, and blurs the faces, so the people are not identifiable. It can also be used on existing photos to blur faces from those. They also have other Apps, so go to their website and have a look.



If you want to have a better idea of what cell phone tower (base station, or BTS) that your phone is using, and be warned if its suspected you are being redirected to an IMSI catcher, you can for Android use AIMSICD. This program is only available in English. You can download the program from: <https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector/releases> 

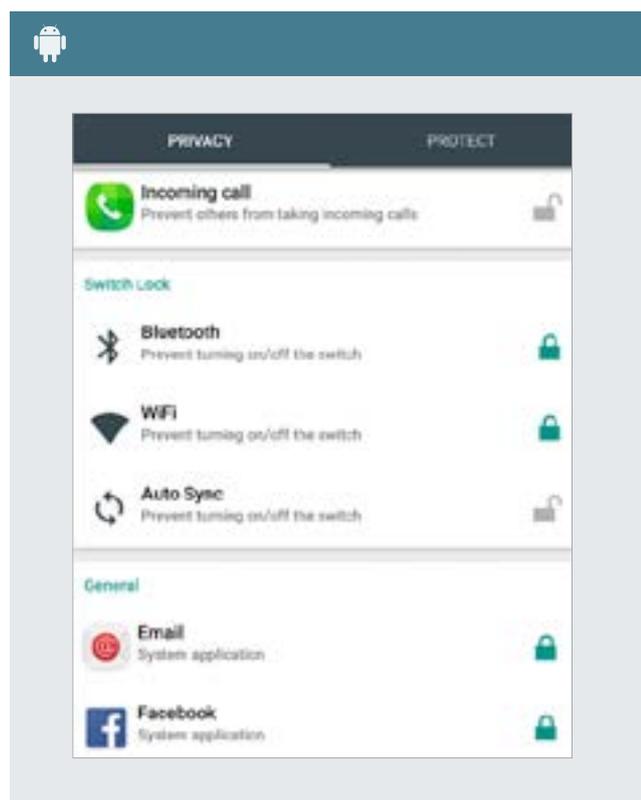
The download will be manual, and you then have to select to install it yourself. You will need to go to Settings and change to Allow Unknown Sources. After install is finished, go back to Settings and change it back to not allow Unknown Sources. The program offers information on what BTS your phone is connected from, and will warn you if it suspects your phone to connect to an IMSI catcher. There is also a map function that will show what cell towers are around you.



AppLock is an English-only App for the time being. If language allows, do however use AppLock because its been tested and verified as safe. AppLock is an App that allows you to create a PIN code, and select any App that you want to use it with. With this, you can PIN code protect any App or function you want, even if that App does not have a native PIN code support. The program itself is hidden, so others cannot easily know that you are using it. It only allows for one PIN code (or pattern), so all Apps you choose will use that PIN code for access.

After you have installed AppLock, it will ask you to install a support program (which offers more options to AppLock) called Advanced System Protection. Install this. With this installed, you will create a password for AppLock, and it will also hide the program, and make it impossible for those without the password to uninstall it.

After install, navigate around to see what you can use the App for. The App has two tabs, Privacy, where you can select what functions and Apps you want to protect, and Protect, where you can change settings, like if you want PIN or Pattern, if you want to hide AppLock so it cannot be easily found (which you want). If you choose to hide the App, in the future to start the App, you need open the dialpad (like when making a phone call), and write in #1234 and click call. This will launch the App. If Advanced Protection has not been installed automatically, click to enable Advanced Protection under the Protect tab.



COMBINING WITH COMPUTER USE

As has been mentioned over and over, it's important to separate the use of your computer and your phone. We generally advice you to not use any phone-based Apps on your computer. For example, Telegram has an App for Windows computer, where you can use the chat program straight from your computer. However, the computer based version does not allow for Secret chats, and cannot be password protected. Similarly,

other Apps might have programs for your computer too, but we recommend you to not use it. There are also computer programs to read, send and manage your SMS traffic these days, but again, please avoid.

The one exception is Signal Private Messenger, which can run on both Win10 and OSX and still maintain Disappearing messages (auto-destruct), and which can also do so for group chats. However, you need to use your phone to start a chat or group chat with Disappearing messages, and cannot start it from the computer program itself, but once started can use and control from the computer.

WHAT IF?

If you, despite knowing how hard it is to protect a phone, need to use it for research on a browser, browser access to an email or account, or use your phone to store a file or data, do take the following precautions. Any use of the browser means you have to enter the settings area for the browser, and make sure no passwords are saved, no auto-fill function is used, and that after the use of the browser is finished, that you select to 'clear all private data' from the browser.

If you ever stored any files or data on your phone, install a free space eraser program, and run the program after having removed/deleted the file or data. This will not work as well as on a computer, but will help make sure no easy file recovery can be used to find the file. For Android phone's we recommend Secure Eraser, and if iOS iShredder (only available in English). Many other similar Apps exist too. If your phone has an SD card, also make sure to run 'erase free space' on the SD card as well as on the phone's internal hard drive.

TO CONSIDER

- Before publishing photos or anything else from your phone, make sure you know what Metadata is included in the file.
- Make sure your secure chat programs are set to automatically delete your chats, and if you use functions without auto-delete, make sure to delete the chat log after finishing the conversation.
- Make sure to set Signal as your default SMS program, and use Signal for both SMS and making phone calls.

A DAY IN THE LIFE

For a normal days work, in a safe manner that protects you against future attacks, consider the work flow presented below.

Upon arriving at work, you start your computer, having been properly shut down last night and not just left to sleep. You start your day by turning on your VPN and accessing your normal work resources, checking and responding to emails, etc. This, and any other research undertaken is done using your dedicated work browser, with security settings applied.

As far as possible, while doing research you use [DuckDuckGo.com](https://duckduckgo.com)  as your search engine, or Google search engine without being signed into your Gmail or any other Google account in the same browser.

Once you need to start working on a document, or download files from email or through your browser, you mount your encrypted drive (hidden inner volume). Preferably you keep this on a USB stick, but can also be a partition on your hard drive or a file container. Only after having mounted your encrypted drive do you start downloading any files, or creating new ones. Anything downloaded or created is placed directly on this drive, not on the desktop or some temporary download folder.

As soon as you leave your computer you first dismount the encrypted hard drive and lock the computer. If you leave the computer for any longer period you shut down.

If you need to undertake particularly sensitive work requiring for example a one-time use email other communication or research that requires you to mask your IP and location as much as possible, you launch TOR, instead of using your VPN. After accessing the TOR browser you use this to access your anonymous email or service. Once you have performed the work requiring added security and anonymity, you turn off TOR and re-launch your VPN, since TOR is terribly slow and only for email access or browsing when security matters more than speed.

Throughout the day, any PDFs or any other presentation material created, or any word document you need to share, or photo to use in a document or share online, you make sure to remove any metadata, or at least check what metadata is included in the file, to make sure what information you are actually sharing. In most cases you simply remove the metadata.

You use your phone, not your computer, to handle any basic chat communicated, using Signal for messages or SMS, or Telegram, and on both you use secret chat/disappearing messages, so no track record is kept of what you have been communicating.

If you have created a lot of documents while working during the day, especially small side documents, you decide whether they are still important or have been incorporated into larger documents and not needed anymore. If you decide they are important to keep, you either consolidate them into fewer documents or save them however you want them organized within your encrypted partition. You never leave work documents on the desktop or accessible folders at the end of the workday.

At the end of the day you take a few basic steps. You access your work email, and unless you have

received or sent any email with very important information you need to keep, you make sure to empty your Inbox, Sent folder and Trash/Bin, so that unauthorized access to your email cannot access anything left behind. Also, having already made sure to securely save any documents in progress, you will securely delete any remaining documents when you run CCleaner. You make sure any chats on your phone not automatically deleted are deleted manually. Finally, after closing your browser and dismounting your encrypted hard drive, you run CCleaner, to wipe traces of your day's activities.

If you have not cleaned the Free Space for a while, or you have done something extra sensitive, or if you are in a situation of heightened security concern, you let your computer Wipe Free Space overnight, locking the computer as you leave. Again, if you do this, make sure computer is locked, and that the encrypted drive is dismounted and if on a USB removed.

KEY TAKEAWAYS

- Do not use your personal browser for work
- Do not conduct work without being on your VPN (or TOR)
- Do not download or store files on your phone
- Do not save or create documents outside of your encrypted hard drive
- Do not leave your computer for the day without first running CCleaner

PART IV **PREVENTATIVE SECURITY**



CHAPTER 12

PREVENTATIVE PROTECTION



If you are reading this, it likely means you now or may in the future face certain risks to your safety or freedom, which no matter how small should not be overlooked. Go over the points below, which should not take more than 15 minutes and follow the suggested actions. They may play a key role in keeping you safe in the future.

Based on the Checklist provided, create a document that includes all such information, and anything else you want.

Before you start writing, you will need to analyze your own situation, and what kind of assistance you would like, should you get into trouble. For that, please review the three points below.

STEP 1: WHAT ARE THE LIKELY THREATS AND SCENARIOS AGAINST/FOR YOU?

Outline what type of potential threats you may face, and for what purpose. If you are a journalist, for example, is it short-term detention to prevent reporting on a story, or confiscation of materials to track down your sources, or more serious arrest and charges to stop your work completely?

Different threat scenarios may require different preparation. What actions have you taken, or people do you work with that could increase your risk? Have you reported on local corruption or represented a victim of torture before a hostile court? Once you have outlined your actions that may result in reprisal you should identify the likely source of reprisal. Do you already know who the most likely perpetrator would be (an antagonistic local government, national security police, state security etc.)? Do you know what the likely method and charge would be if actions were taken against you? Outline answers to these questions, as fully as you can, as it will greatly increase the speed in which help can be provided.

STEP 2: WHAT ASSISTANCE DO YOU WANT?

Based on the different types of actions, you have outlined above, what kind of assistance do you think you would want? Do you, for example, think that international media attention would be useful in a specific scenario, if yes, then this must be stated, and in what way (for example, if detained, would you like to receive media attention only after the first week has passed, or maybe you only want local/domestic social media attention, or prefer more quiet diplomatic or UN support and no media attention. It is important to realize that different approaches have different benefits depending on the circumstances and you may want to speak about your options with trusted colleagues, as they may well be the ones speaking on your behalf). What other forms of support might you want?

Do you have family members who rely on you for financial or otherwise support that would need some form of assistance if you are detained or disappeared for prolonged periods of time? What kind of support, financial, medical, tuition costs, residence etc.?

Likewise, if detained, or worse, do you want legal assistance, and do you have any specific legal requirements? Are there any circumstances under which you would deny your right to choose your own legal representation? Do you already have a lawyer that has promised to assist you if needed? If yes, who is he/she, and how to contact him/her? Does he or she have access to a power of attorney?

If this applies to your decision, you should make a note of your chosen legal representative, clearly stating under no circumstances would you change for a State-appointed lawyer, and leave copies of this note with more than one trusted friend or colleague.

STEP 3: DESIGNATE A TRUSTED, SECURE (NOT-AT-RISK) SAFETY PERSON

Your safety person will sit on the information provided here and will be responsible for sharing this with relevant people should something happen. All the information provided here must be given to this person, and this person must be instructed in what to do if anything happens.

Also designate a family member that is legally allowed to provide power of attorney should it be needed. Think twice before selecting, and realize many family members are often hesitant to provide it in the beginning, not knowing how to deal with these kinds of situations. Also keep in mind that the police have many times harassed or detained family members as punishment so make sure to discuss the risks and requirements with the family member you select and make sure they understand and agree. Select a family member that is understanding of your work, and tell them that you have selected them, and that if ever needed, they should provide such power of attorney without hesitation. Share information on your safety person to this family member, so they know who they are, should they ever have to contact this family member, and of course connect your safety person to this family member, or at least write down contact information etc. about this family member in the document you give to your safety person.

The below list of issues and points (Checklist) can serve as a guide to what information should be included.

CHECKLIST

- A CV/Resume
- A narrative description of yourself and your work, try to include specific dates for key activities that may cause reprisal. (This is especially important in proving that any State or police measures taken against you

are being done as reprisal for your rights defense or civil society work. It is crucial for any advocacy efforts on your behalf and should not be overlooked.)

- Contact information (and preferably an introduction) to any designated lawyer who has agreed to provide legal counsel for you.
- Contact information (and preferably an introduction) to your emergency contact (safety person)
- Contact information (and preferably an introduction) to your selected family member for power of attorney
- Contact information (and preferably an introduction) to any relevant friends and family
- Contact information (and preferably an introduction) to any journalists or diplomats you know or would like to be included in any assistance work
- A written overview of relevant coworkers and/or work affiliates, with contact information (This may be important for additional preventive protection or threat identification.)
- Do include some photos of yourself that can be used, should public/media advocacy be needed. This will give you some control over how you will be represented.

PRE-ARRANGED MATERIAL

Pre-arranged material (by yourself) to be released in the case of your detention, arrest or other (and outline specifically when/if/how you want this information released). See example below. Making some small videos can be very helpful.

Explaining pre-arranged material. What pre-arranged material you should use is entirely up to you, and based on both your work and the type of threats you imagine, for example:

- These days forced confessions are becoming more common. Gui Minhai, a Swedish citizen, was abducted from Thailand to China. In his forced confession, he has asked to not receive diplomatic assistance from Sweden, and said he wants to renounce his Swedish citizenship. Imagine if he had made a pre-recorded video saying that if he ever appears in China it will be because he has been kidnapped (because he did not have a valid visa in his passport to China), or if in the pre-recorded video he explained that if he would never renounce his Swedish citizenship or deny diplomatic assistance, then this would have been a very powerful counteractive force against the State broadcast of his false-confession. It would have raised attention to his case and extended assistance.
- Many rights defenders are taken and denied the ability to meet or communicate with family members or lawyers, with the police claiming the rights defender said they don't want their lawyer and instead prefer to use a state-appointed lawyer. Imagine if this person has pre-recorded a video saying clearly that they will never renounce their right to select their own lawyer, and that they will never ask for a state-appointed lawyer.
- If you think police will try to use any specific aspect of your work against you, imagine how helpful it could be to have a pre-recorded video explaining this work and why and how it is perfectly legal? Or if you have been previously threatened, warned, intimidated or otherwise for your work, make note of the past persecution.
- If you think Police might accuse you of illegal conduct doing NGO work, or accuse you of financial misconduct or fraud? Then send copies of financial reports, audits etc. to your safety person, that can

counter such accusations.

IMPORTANT: If anything changes, such as your address, the contact information to your emergency contact, your family situation, or your work, and especially if you anticipate any changes in threat level, this document must be updated to reflect these changes, and you should send your designated emergency contact person a new version.

