PRACTICAL DIGITAL PROTECTION

defense beyond technology

INTRODUCTION:
BEHAVIOUR-BASED CYBERSECURITY

practicaldigitalprotection.com

BEHAVIOUR-BASED CYBERSECURITY

A summary of and introduction to the full and complete manual on
PRACTICAL DIGITAL PROTECTION

practicaldigitalprotection.com

a project by

safeguard
DEFENDERS

TABLE OF CONTENTS

INTRODUCTION

Welcome to the simplified version of **Practical Digital Protection** - the practical, self-study manual on cybersecurity for those operating in hostile environments. This briefer, simplified document outlines the basic *behavioral* aspects of cybersecurity, and helps you analyze your situation, needs, and priorities. For full review of these concepts, and technical solutions to the issues presented, see the full manual.

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 HRDs in places like China, Vietnam, Myanmar and beyond. Each language version of the full manual is tailored to that country and language, developed together with a group of beneficiaries in said country, to provide information and solutions related to their self-assessed needs and wants.

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

Everyone has heard of Edward Snowden and his revelations about the spying, and probably seen American movies about advanced electronic surveillance. Unfortunately, none of this is really relevant for human rights defenders in places like China, Vietnam, or India, or most of the world for that matter. The key problems you will face is not advanced encryption breaking or hacking. The real problem lies in what happens when you are detained or your phone or computer is confiscated.

This simplified version presents basic security concepts and behaviors. For any particular issue that is of interest to you, please refer to the full manual for more details, and instructions on technical solutions for the issue.

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

KNOW YOUR THREATS

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 or Vietnam 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 potential 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 wifi 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.

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 ONE. 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 you 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 you ignoring basic security thinking would affect you as well as others.

STEP TWO. 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 THREE. 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 FOUR. 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 BEHAVIOURS

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 DAMAGE CAUSE BY THIRD PARTIES & 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 mean 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.

For a webmail service, free of charge, that uses both high-level encryption, as well as offer automatic destruction of emails, see ProtonMail.com.

For chat programs with ability to set autodestruct on chat logs, see Signal Private Messenger and Telegram.

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.

For a browser for sensitive work, with many extensions available for additional security, see Firefox. Upon install, go over the settings in detail, and install extensions such as KeyScrambler, TrackMeNot, RefControl, Better Privacy (or Privacy+), and NoScript.

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.

To deal with this issue, install CCleaner, and go over the options for appropriate settings. This will also help remove further traces from your browsers.

"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.

Luckily, the same program that can clear traces of your computer, CCleaner, mentioned above, can also properly delete (over-write) the files you have "deleted." Doing this is key, without it, you will never, and can never, be safe. Ever. Even better, it's a rather simple process, but depending on size of hard drive, can take time.

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. A program called Truecrypt (or Veracrypt) can be used to create such "hidden" encryptions, on your hard drive, or on a USB etc.

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.

For the most part, you likely access the internet through the connection at home. This connection is managed by your router. If you use wireless, you need make sure the signal is encrypted (password protected), or else anyone else can read and monitor what you do on your internet connection. Secondly, the router comes with a standard password, to access the actual router and make changes. This is dangerous, and many people never think about this, and do not access their router to change this. This makes your router an easy target. You need to change that password.

CORE RULES

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 many countries, 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. 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.

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 many local applications. For example, the data Chinese or Vietnamese 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.

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.

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.

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.

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 computers, 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.

THE PROBLEM WITH PHONES

First off, even though phones today are like small computers, they are limited in power, and therefor 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.

"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 bring us to problem one, **location tracking**. Location tracking 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, Vietnam, Thailand and other countries 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."

Due to such threats, your phone, as far as possible, should not be used as a small work computer. Never download or store sensitive files, documents or photos onto your phone. Do not use your phone to store, even temporarily, any work documents.

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

Despite all that has been said above 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*. 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 way to go dark, in a very easy manner, is the use of aluminum tinfoil. Many people who works with sensitive issues and am 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 suspicions.

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

WANT TO KNOW MORE?

The **Practical Digital Protection** manual includes several real life stories on how police or security agents have used these tools, and how they have succeeded, or failed, depending on how the person targeted had prepared.

Practical Digital Protection

practicaldigitalprotection.com