# 1/ Assessing Digital Security Needs

*Step by step*

These cards detail different threats and means of protecting sensitive information, to ensure secure and successful engagement with civil society. This card will help you decide which cards are most relevant in your situation.

Firstly, what is **sensitive information**? Think of sensitive information as any information which, if it fell into the wrong hands, could have negative consequences. Many types of sensitive information, such as personal data, are protected by legislation. Still, it is highly recommended to protect all of your data.

*Are you certain you are covering the basic essentials of information security?*

- If not, see cards 2 and 3.
- If you are, then see cards 2 and 3 in any case, to make sure.

*Are you concerned that the authorities may be monitoring your online activities?*

- If so, see cards 4, 5 and 6.

*Do you often work from outside the office, and travel with your devices?*

- If so, see cards 2, 4, 7 and 11.

*Do you offer financial support or engage in projects with civil society organisations?*

- If so, see cards 5, 8, 9, 11 and 12.

*Are you connected to civil society via social media, or are you considering this?*

- If so, see cards 5 and 6.

*Do you use Dropbox or similar services to share data with HRDs?*

- If so, see card 8.

*Do you use WhatsApp, Facebook, or commercial email to communicate with HRDs?*

- If so, see cards 5 and 6.

*Are you operating in an environment where targeted malware is used to attack or spy on journalists or human rights defenders?*

- If so, or if you are not sure, see card 10.
- If not, try to keep up to date on this issue as it may become relevant in your context.

See the website *https://digitalsafetymanual.org* for more information.

# 2/ Basic Device Security

*Easy steps for big improvements in digital security*

Every attempt to gain access to information starts with the simplest possible means. So, you have to have “the basics” consistently covered.

## DO THE FUNDAMENTALS

- Use a **strong passcode or password** for mobile phones.
- Switch on **disk encryption** on phones, tablets, and computers where possible.
- Strengthen the security and privacy settings of apps, in particular messaging apps, and switch on **PIN or password protection** for apps where possible.
- Protect your computer and user accounts with **strong passphrases.**
- Switch off **Bluetooth and Near-Field-Communication** when not using them.
- Turn off **location services** when not needed.
- Ensure that important and sensitive data is **backed up**.
- Use a **USB-Charge-Only dongle** to prevent unwanted data-transfers while charging.

## PROTECT YOUR DEVICES

- Know **where** your devices are at all times.
- Leave them **protected** in the office or in a hotel room if it is safe to do so.
- Place **tamper-evident tape** over the USB ports and hard drive cover.
- Use a **security cable** (Kensington lock) to protect your computer when you work outside the office.

## AVOID MALWARE

- Install **anti-malware** applications and keep them updated.
- Exercise caution when opening unexpected attachments, and use **secure file transfer methods** where possible.
- **Update** your apps and operating systems and respond to notifications about updates.
- Download software updates from **original download sources** regularly.
- Download apps from **trusted repositories** like the Google Play Store, F-Droid, or Apple’s App Store only.

## MANAGE YOUR APPS

- Use a **privacy-respecting browser** to access social media sites on any device containing sensitive information. Avoid installing social media apps as they often collect sensitive information from your device.
- Customise the **permissions** of apps regularly in the device’s settings.
- **Switch off** apps that you are not using, and **delete** those you do not need. They might run in the background and collect user data.

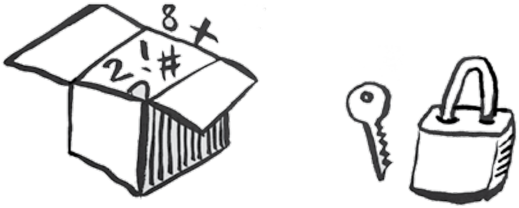
# 3/ Passwords and Account Protection

## *Things to consider*

- The techniques and software used to break passwords have evolved significantly over the past few years. It takes more effort to make strong passwords now.
- Brute-force dictionary attacks are used to guess passwords, which can now also decipher patterns with numbers and symbols.
- A number of servers of online service providers have been compromised in recent years. This has led to the leaking of a huge number of passwords onto the open internet. Brute force attacks may also include these stolen passwords.

## *Protection tactics*

- Passwords should not be easy to guess, and should be **long** (12-15 characters minimum), including numbers, letters, and symbols. They should also be **changed regularly**.
- Avoid using the **same password** for more than one account.
- **Use passphrases** rather than passwords: phrases consisting of several words, ideally unrelated, and also including symbols and numbers. This is much more difficult for dictionary-based password-cracking software to guess.
- **Don't trust your browser** to save passwords. The underpinning security of these services is often undocumented.
- **Use a password management software** to generate stronger passwords and passphrases. These tools can also save your passwords using a "master password", so that you do not need to remember them. Choose one with the following characteristics:
  - ○ **Open-source:** given that the software is managing the keys to your sensitive data, it should be open source and/or subjected to independent audits to verify its security bona fides.
  - ○ **Strong encryption:** the software should use strong encryption to store your passwords securely.
- **Use two-factor authentication (2FA):** After entering your password to log in, you will be asked for a further code which is often generated in an app or sent to your phone via a messaging service.
- **Be smarter with "secret questions":** These are questions relating to your personal life and can easily be guessed. Generate random or long passphrases as "answers" to these questions, and save them in your password manager.
- Frequently check if your email addresses have been included in recent **data breaches**, through services such as the "Have I been Pwned" website or the database provided by the Hasso Plattner Institute.



# 4/ Connecting to the Internet Securely

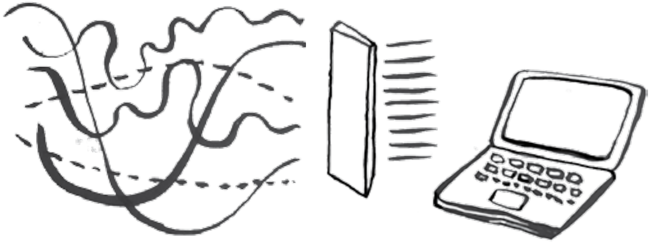
*Things to consider*

In certain areas and contexts, the very act of connecting to the internet – as an embassy staff member working on human rights, or as a human rights defender – can be a threat to your information security:

- Network administrators, opportunistic criminals, Internet Service Providers (ISPs) and even State agencies may be **monitoring** internet users, and looking for vulnerabilities to exploit.
- Wi-Fi networks in **public places or hotels** can be closely monitored by the network administrators, as well as by the parties mentioned above.
- On public Wi-Fi, **unencrypted content** sent over the internet, such as the content of webpages that do not have an SSL (or "https") connection, as well as metadata (such as visited websites) is vulnerable to being accessed in these cases.
- Wi-Fi networks might also be used to install **malicious software** on devices. Examples are known of journalists, NGOs, or political opposition being targeted in this manner.
- At workplaces or at home, routers used to connect to the internet may have insecure **firmware**, allowing for access by adversaries. They can enable routers to store data about your internet use or facilitate its handover to third parties.

*Protection tactics*

- Install and use a **Virtual Private Network** (VPN) on your mobile devices and computers to hide the relationship between your device and your online activities. Some VPNs have been made with HRDs in mind and can be recommended to them in these cases.
- Connect to your mobile network by creating a **hotspot or tethering** from your phone, and avoid connecting to the provided network when in public places where you suspect there might be a likelihood of network monitoring by authorities or even a risk of malware infection.
- Consider using **Tor Browser**, also available as an app, which routes your data through a combination of at least three nodes in the Tor Network, facilitating access to blocked content and anonymity on the internet. Be aware that using Tor might trigger attention from authorities in some contexts.



# 5/ Secure Calls, Chat, and Email

*Things to consider*

- When communicating with someone via an online platform, both the **content** of the communication (the messages) and the **meta-data** (information about the devices, the app, and the communication) travel through a number of different points, often all over the globe.
- This includes routers, the infrastructure controlled or rented by Internet Service Providers (ISPs), national gateways often controlled by the State, Internet Exchange Points, etc.
- When data is sent **unencrypted** across these channels, it can be read by people with access to any of these many points.
- Many email providers and messaging apps encrypt content now using a protocol known as Secure Socket Layer (**SSL**). This can be seen as **"https"**, such as when browsing websites. This provides some protection, but can not be trusted on its own for secure communications.
    - SSL encryption does not protect data from being read by the owner of the website or app, such as many free email providers, and social networks. They can access content and data either for their own interests, or when requested by authorities.
    - SSL is a common target for those trying to **eavesdrop** on communications or access other sensitive data.

*Protection tactics*

- Always discuss the potential risks posed by communication between embassy staff and HRDs at the start of any cooperation. Decide about apps and channels to use based on this assessment.
- Sensitive communications require services, tools, or applications with **end-to-end encryption**, that ensure only the sender and recipient(s) of an email, message, or call are able to decrypt it. Some messaging, call, and video services provide this by default. However, in some contexts they are illegal or attract further attention.
- Look for apps that implement "**Perfect Forward Secrecy**" and 'disappearing' or 'self-destructing' messages. Perfect Forward Secrecy is a security feature which ensures that intruders can only decrypt one message at a time. **Self-destructing messages** 'disappear' after a certain amount of time, or can be deleted by users from their own and their interlocutors' devices. However, it is not clear to what extent these messages can be recovered.
- Some HRDs use **PGP** encryption on their emails. If this is not possible, move all sensitive discussions to an encrypted messaging application. Email attachments can be encrypted and the password should be shared over a secure third channel.

# 6/ Security and Social Media Use

*Things to consider*

Social media can be a useful tool in supporting and giving visibility to the work of civil society organisations. As contexts vary widely, it is important to use it carefully and strategically.

- Being **visibly connected to HRDs** and promoting their work via social media can reduce the risks they face, or have the opposite effect and increase risks.
- Social media sites are **not appropriate** for any type of sensitive communication. There are a number of potential risks to communicating sensitive data over such platforms, including:
  - The provider of the website may be obliged or requested by authorities to **hand over user details**, including private messages and ‘deleted’ content.
  - The regular **changes in Terms of Service** by many social media platforms often lead to changes in the privacy settings available or the defaults, making information previously thought to be ‘private’ more freely accessible to others.
- **Facial recognition** software is also ever more common on social media platforms, regardless of whether users opt into being openly ‘tagged’ in pictures or not.
- Private messaging on sites and apps may only be protected with weak encryption.

*Protection tactics*

- Protect your accounts using **strong passwords and two-factor authentication**, and encourage HRDs to do the same.
- Avoid having or using social media apps on devices which contain sensitive information because they collect information from your device. Ideally, access social media sites via a **privacy-protecting browser**.
- Check the **privacy settings** of the social media sites that you use and make them as private as possible.
- If an HRD wishes to connect with you over social media, **double-check** with them if they are sure they would like to do this.
- Always **ask explicit permission** before uploading any pictures, including of HRDs, to social media platforms, and before tagging them.
- Avoid discussion of any sensitive issues over social media messages and encourage HRDs to use alternative, **more secure methods of communication**. Exceptions could be made to this in cases where secure messaging applications themselves are the subject of stigmatisation or criminalisation by authorities.
- Exercise extreme caution regarding any **links which are shared on pages** or in groups related to political or social movements, especially during times of civil unrest, as these may be malicious.

# 7/ Secure Data Storage and Deletion

*Things to consider*

Although you may have a user password, data on devices may be accessible to third parties who obtain physical access to the device.

- Better resourced adversaries are not deterred by a strong user password: in most cases, **data is stored in a readable format** on hard drives, mobile devices, and USB keys, unless additional measures have been taken to protect it.
- Files deleted via the normal 'Recycle Bin' option **do not disappear** after the Recycle Bin is emptied. Instead, they are assigned by the Operating System as **'free space'**. This means that the space on the drive can be overwritten by new data. However, until that point, the data remains recoverable.
- Deletion of data on modern flash storages like USB drives, mobile phones, or solid-state hard-drives (SSDs) is technically **nearly impossible** without overwriting all free space after the deletion of the respective data.

*Protection tactics*

- Remember the basics: ensure that your user accounts on your computer have **strong passphrases**, and that your mobile devices have **PIN or passwords** activated.
- Regularly **wipe your 'free space'**: There are programs that overwrite 'free space' on hard drives, and which can delete old and temporary files. However, there is no guarantee that data on devices with SSD hard drives can be effectively overwritten.
- There are some options to protect your data through **encryption**. Be aware that in some contexts, this may be legally restricted or may draw attention to you.
- Consider **full disk encryption**, which means encrypting all of the data on a particular device or drive partition, or creating encrypted folders on your device. Many smartphones and some computers come with this option; see the website for more up-to-date information regarding this.
- In addition, or as an alternative, you can use **encryption software** to create encrypted volumes. This involves creating a space, like a folder on your device, where sensitive data can be stored.
- Accept only **encrypted external drives** such as USB keys. This implies that they are only readable on devices with the right encryption software installed and with a password created upon encrypting the device.

# 8/ Secure File Transfer

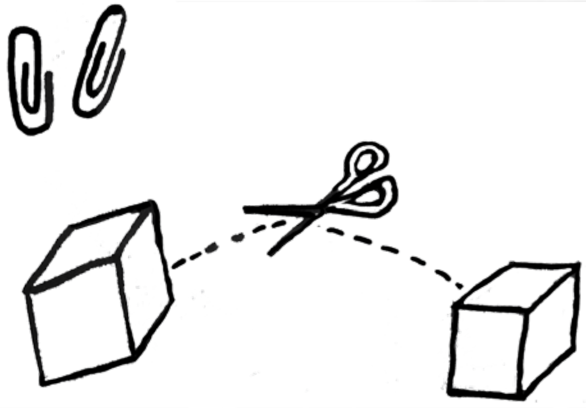
*Things to consider*

Transferring files over the internet is another form of online communication, and most of the same vulnerabilities and protection tactics apply. There are a number of additional issues with email attachments, online file sharing, and cloud services, to be aware of.

- Email attachments are a common way to spread **malware**, including targeted malware. Malicious actors sometimes even send encrypted attachments; be especially suspicious of emails which include the password to decrypt the attachment.
- Many common file-sharing or cloud platforms offer **only SSL encryption** to protect the data exchanged over these platforms. SSL encryption has several vulnerabilities which have been exploited to access user data. Furthermore, it often allows owners of the platform to access the content shared by users and their data for their own interest, or as requested by authorities.
- The backup functionalities on phones, tablets, or computers generally store backed-up content **without encryption on their servers.**

*Protection tactics*

- Verify unexpected or suspicious files sent to you: check over a third, secure channel what was sent, and why.
- Use tools for secure communication that implement **end-to-end encryption.** This can reduce the likelihood of a malicious actor successfully fooling you into thinking an attachment was sent by a legitimate contact.
- Verify the **security numbers or fingerprints** associated with different devices via a third channel or during in-person meetings. This helps to prevent social engineering or 'man in the middle' attacks.
- Use **file-sharing and cloud services** which offer end-to-end encryption and share passwords over a third secure channel with your contacts if necessary.
- When using unencrypted cloud services such as Dropbox, make sure to **encrypt data before storing it** online.



# 9/ Secure Contract Handling

*Things to consider*

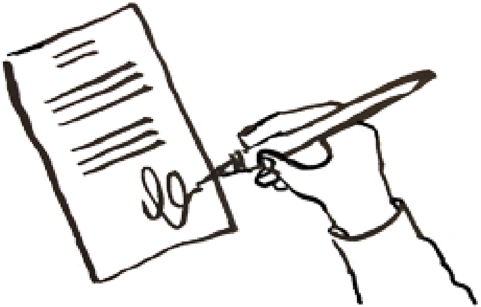
- Giving funds or other kinds of formal support to civil society and HRDs can involve risks for the civil society groups, embassy staff, and others who are tangentially involved or involved by association.
- Certain contexts are, or could become, hostile towards civil society receiving funding from foreign sources, particularly directly from foreign authorities.
- The management of information around this is particularly important for the safety and well-being of all involved.

## *Protection tactics*

Carry out an analysis to strike the right balance between transparency and discretion in accordance with your context.

The following questions and pointers may be useful for such an analysis, which is best conducted with your civil society partners before contracting:

- How much information regarding the project is best included in the contract itself? Ensure that the data to be stored on IATI **does not include personal, financial,** or any other sensitive data related to the project.
- **Who is best placed to sign the contract** on behalf of the organisation or institution being supported, and are there any potential risks associated with this? If so, how can they be mitigated?
- What platforms are used for **sharing, signing, and storing the contract** in question? Consider the tips related to Secure Online Communication, Secure File Sharing, and Secure File Storage and Deletion (cards 5, 6, & 7). Only hand over contracts to third parties if and when it is considered beneficial to do so.
- What information will be expected from the grantee with regard to **reporting**? What information is potentially sensitive and should be omitted, or securely deleted after a period of time?



# 10/ Targeted Malware and Other Attacks

*Things to consider*

- **Malicious software**, or 'malware', is any software that can cause damage to your digitally stored data, or give third parties access to it.
- HRDs, politicians, journalists, and the diplomatic community must be aware of the threat of malicious software designed specifically for espionage on them.
- This **targeted malware** typically allows **remote control access** to all files on the device, as well as the ability to record all keyboard uses or switch on the camera and microphone, without alerting the user to what is happening.
- This kind of infection with malware happens in several ways, including **links or attachments** sent via messaging services or email which download the software to their devices once clicked or opened. **Wi-Fi access points** and business centres in hotels frequented by 'targets' are sometimes used to infect them with malware.
- Another targeted attack commonly used against civil society is known as '**phishing**'. Phishing means using cleverly designed emails or false websites to trick users into clicking on a particular link, downloading a programme, or giving their login or other details to an attacker.

*Protection tactics*

- Installing an **anti-malware** programme on all devices is a vital basic practice. Remember to keep software updated.
- Use **link expanders** to see the real addresses of suspicious, shortened URLs.
- Make **regular backups**, ideally daily, or at least weekly. This greatly reduces the impact of data loss, which can also be caused by malware, or ransomware. Make sure that any encrypted data is also backed up in encrypted form.
- Use communication applications which allow for **verification** of device **'fingerprints'** – and verify the 'fingerprints' of your contacts' devices.
- Do not connect to **public Wi-Fi** offered in hotels, conference venues, or other places frequented by civil society, journalists, dissidents, or opposition politicians.
- When you are subjected to a targeted malware attack or suspect you have been, contact your local IT support as soon as possible and raise the issue as appropriate within the office.

# 11/ Phone Tracking and Surveillance

*Things to consider*

Mobile phones are invaluable resources for work and can also be of great use for security: in an emergency situation, they are the first tools that many will reach for. However, they do have vulnerabilities.

- A mobile phone is like a tracking device: its **location is constantly communicated** to the company that runs the network. Even this basic location data has been used by authorities to identify and harass participants in protests as well as for general surveillance.
- 'Normal' phone calls through the mobile phone network, as well as SMS messages, are transferred across the network without much encryption. This means that they can be recorded, listened to, stored, and read easily by those who control the network. Third parties can also use tools such as **IMSI catchers** to 'listen in' on the phone calls and SMS messages passing through.
- Smartphones have hardware features that can facilitate surveillance such as GPS and batteries that cannot be removed. Smartphones are often the subjects of **targeted malware** attacks, which can essentially make them remotely controlled.
- Some apps such as voice-activated personal assistants may expose users' private lives to the opportunistic **surveillance of the large tech companies** which run them, and whomever they are legally obliged to share their collected information with.

*Protection tactics*

- **Avoid normal calls and SMS**: only use them to exchange sensitive information in exceptional circumstances, such as in emergencies.
- Use a **Faraday bag** to block your device from the mobile network and obscure your location (at least via the mobile network) and block radio signals. Keep in mind that a Faraday bag does not prevent the microphone from functioning and recording, and that Bluetooth and Wi-Fi should be switched off manually.
- Check whether HRDs are comfortable keeping their mobile phones with them before meeting with them and **leave devices in a different space** out of earshot of your conversation.
- Install and use a **Virtual Private Network (VPN)** on your phone.
- Exercise extreme **caution with any links or files** that are shared with you via SMS or messaging services, and do not open them unless you were **explicitly** expecting them.
- **Switch off all apps** that might be abused for recording conversations, such as Skype. **Remove** apps that you do not actively use from your phone.

# 12/ Security Concerns Related to In-Person Meetings

*Things to consider*

- In-person meetings with civil society may have a number of security implications, particularly in an environment where authorities are hostile to such contact.
- The risks attached to in-person meetings vary significantly depending on the **context**.
- In certain contexts, explicit contact between embassy staff and civil society offers **visibility and legitimacy** to the work of HRDs and provides protection as a result.
- Surveillance of meetings can take place through **observation** from a distance, public **CCTV**, **directional microphones**, third parties **eavesdropping** (e.g. in public places, taxis, etc), or **mobile phone** surveillance, for example.
- In certain cases, **direct interference or harassment** may also occur. While diplomatic staff are less likely to experience this, the possibility should be kept in mind while working with local staff and HRDs.

*Protection tactics*

- **Consider the particularities** of the context you are in and the best mix of transparency and visibility versus discretion and privacy. Speak to appropriate embassy staff, civil society partners, or another trusted contact to assess the risks involved.
- If meeting in a **public place**, take into consideration the possibility of **surveillance** via proximity, CCTV, or other means.
- Consider what to do with **mobile phones** and other devices during the meeting.
  - ○ Leave them in another room **out of earshot** to decrease the threat of surveillance. Use a **Faraday case** to block the radio frequency signals from electronic devices such as mobile phones, car keys, or laptops.
- Remember that offline eavesdropping tactics are still used, so be **aware of your surroundings** and people potentially within earshot of the meeting.
- Report every **security incident** that takes place before, during, or after a meeting, such as suspicious behaviour and anything out of the ordinary (someone watching, taking pictures, etc.) and encourage others to do the same.