A Quick Guide on Security for Human Rights Defenders

Introduction

IBON International's core work of solidarity is premised on rights-based democracy. Promotion of people's rights, contributing to developing capacities of organisations entail that we take the extra mile in the conduct of our work. Development workers are human rights defenders in the main.

As human rights defenders, we play an important role in ensuring justice, equality, transparency and accountability in societies. Our legitimate work ensures that peoples' rights and sovereignty are upheld and defended especially in the face of growing corporate greed and government corruption and abuse.

Our work as human rights defenders has always been accompanied with risks to life and security. Such risks are amplified by the current global trend of closing spaces for peoples' movements and civil society. In the Philippines, the Duterte government has been decisively and brazenly shutting down civic and democratic spaces. It is criminalizing dissent and rolling back democratic institutions and checks on Duterte's power as he imposes de facto martial rule in the country.

While many human rights defenders understand and internalise the nature of our work, there are many practical tools available to help keep us safer and manage these risks. This handbook is intended as a quick reference for suggestions and steps to improve your personal and digital security situation.

IBON International believes that human rights defenders are critical to achieving genuine progressive, equitable, and sustainable development. We hope that this handbook may help you continue your work for the protection and enhancement of peoples' rights and welfare.

Contents

Part I
Arrest and Detention

What is a warrant of arrest?

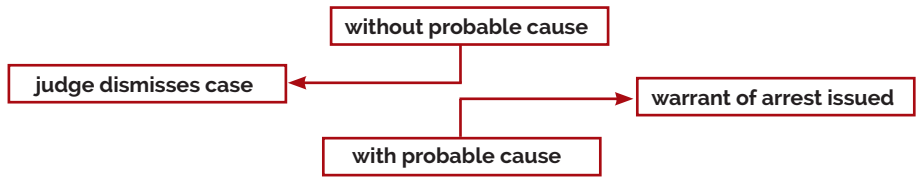
In the Philippines, a warrant of arrest is a legal document issued by a court and served by a law enforcement officer directing the arrest of a person or persons.

How is a warrant of arrest issued?

Criminal cases with a penalty of 4 years, 2 months, and 1 day imprisonment (regardless of fine) shall first undergo a preliminary investigation to gather more information about an allegation.

Preliminary Investigation Process

1. Filing of complaint against you
2. Filing of your counteraffidavit
3. Filing of reply-affidavit by complainant
4. Filing of your rejoinder-affidavit
5. Fiscal decides whether or not to file the case in court. If s/he decides to file it, the fiscal will submit an information in court
6. Within 10 days from filing of information, judge personally evaluates the resolution of the prosecutor and the supporting evidence



A preliminary investigation is a determination of probable cause--or with evidence showing that, more likely than not, a crime has been perpetrated-- and not a trial on the merits of the case.

For offenses punishable by imprisonment of less than 4 years, 2 months, and 1 day, if the case is filed with the

- Prosecutor: the prosecutor will act on the complaint based on the affidavits and supporting documents by the complainant within 10 days from filing.
- Municipal Trial Court: if within 10 days the judge finds no probable cause s/he shall dismiss the case but may require the submission of additional evidence within 10 days from notice to further determine if there is probable cause. If s/he finds probable cause s/he shall issue a warrant of arrest. If not, s/he shall, within 10 days from its submission, dismiss the case.

What do you need to know about a warrant of arrest?

- The warrant of arrest should be executed 10 days after the issuance of the court. If not served, the officer will return to the court and give the reasons why the warrant was not served. The court may issue an **alias warrant, or a warrant for a John or Jane Doe.**
- Failure to serve the warrant does not dismiss the case: it will only be **archived.**
- Warrant notice should contain the **correct spelling** and **signature of the judge.**
- One offense per warrant of arrest.

When can a warrantless arrest be made?

- When the person to be arrested has committed, is actually committing, or is attempting to commit an offense in the presence of an arresting officer.
- When the person has escaped prison/detention, or escaped while being transferred to another facility.
- When an offense has just been committed and the arresting officer has probable cause (based on personal knowledge of facts and circumstance) to believe that the person to be arrested has committed a crime

What is the procedure for warrantless arrest?

If you're arrested without a warrant, you can only be detained for

- 12 hours, for light offenses punishable by light penalties (ex. Unjust vexation).
- 18 hours, for less grave offenses punishable by correctional penalties (ex. Illegal assembly).
- 36 hours, for grave offenses punishable by capital penalties (ex. Murder, arson, kidnapping).

As a general rule, inquest proceedings – where a civilian prosecutor determines the legality of an arrest – are included in these time periods.

What happens after a person is arrested without a warrant?

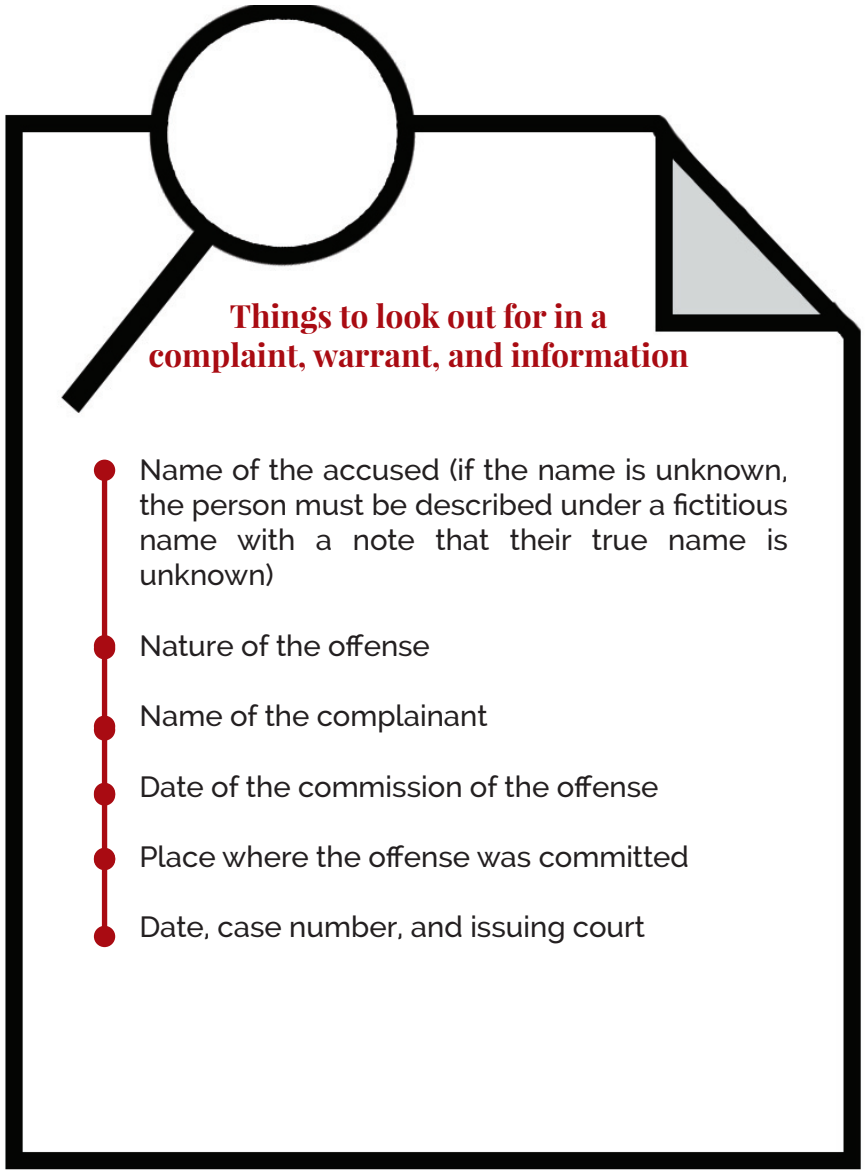
- Arrested person should be brought to the nearest police station (not a military camp or a safe house). S/he should not be subjected to any physical or psychological harm/ interrogation.

- Whatever questioning made by the authorities should be done in the presence of a lawyer of the arrested person's choice. All testimonies elicited from him/her without the presence of his/her lawyer of choice is considered inadmissible evidence.
- **The accused will be prepared for inquest proceedings (fingerprints, mugshots, and medical exam).**

What to do when arrested?

- Demand for a warrant of arrest and carefully scrutinize the contents.
- In case of a warrantless arrest, the arresting officer must state the reason for the arrest.
- You have the right to remain silent and have a competent and independent counsel of choice.
- Take note of the name/rank, number of arresting officers, identifying marks, and plate number.
- Create a scene.
- Empty your bag in public to show that you have nothing to hide and to avoid the opportunity for anybody to plant "evidence" in your bag.
- Do not sign anything.
- Demand that you need to call relatives, lawyer, doctor, priest, human rights organisations, etc.
- You can refuse to accept the services of any lawyer provided by the police or military.

- You can refuse to have your picture taken, be fingerprinted, be subjected to bodily search, or do any act which may incriminate you (i.e. physical examination) until you have appointed your lawyer.



Things to look out for in a complaint, warrant, and information

- Name of the accused (if the name is unknown, the person must be described under a fictitious name with a note that their true name is unknown)
- Nature of the offense
- Name of the complainant
- Date of the commission of the offense
- Place where the offense was committed
- Date, case number, and issuing court

What is bail?

Bail is the security given for the release of a person in custody of the law furnished by him or a bondsman, furnished by him or another individual who assumes responsibility of a bond, to guarantee his/her appearance before any courts as required.

There are four types of bail:

- Cash bond
- Property bond
- Corporate bond
- Recognizance

Who may post bail?

All persons, except those charged with offenses punishable with *reclusion perpetua*, which ranges from 20 years and 1 day to 40 years in prison, have the right to post bail before conviction.

What are the requirements for bail?

- Bond
- Undertaking
- Sketch of residence
- 2X2 photos with signature
- Barangay certificate

Part II
Search and Seizure

What is a search warrant?

A search warrant is an order signed by a judge that authorizes police officers to search for specific objects or materials at a definite location for presentation in criminal prosecutions.

What are the requirements for issuing a search warrant?

A search warrant shall be issued only upon

- Determination of probable cause in connection with one specific offense to be determined personally by the judge.
- After examination under oath or affirmation of the complainant and his/her witness.
- Particularly describing the place to be searched and the things to be seized which may be anywhere in the Philippines.

Where should one file an application for search warrant?

- Any court within the territorial jurisdiction of the crime
- For compelling reasons stated in the application, any court within judicial region where the crime was committed or where the warrant shall be enforced

When should the search warrant be executed?

If possible, it should be done during the daytime but in cases such as when the things seized are mobile or are in the person of the accused, it can be served during nighttime.

Until when is the search warrant valid?

It is valid only for 10 days, after which the police officer should make a return to the judge who issued it.

In what instances would a search and seizure without warrant be allowed?

- A warrantless search incidental to a lawful arrest
- Search of evidence in plain view, or with evidence immediately visible
- Search of a moving vehicle
- Consented warrantless searches
- Customs searches
- Stop and frisk
- Exigent and emergency circumstances
- Checkpoints
- Republic Act requiring inspections or body checks in airports
- State of Emergency
- In times of war and within military operations

What is plain view?

In criminal law, the plain view doctrine allows a law enforcer to make a search and seizure without obtaining a search warrant if the evidence of criminal activity or the product of a crime can be seen without entry or search.

When can evidence be seized in plain view?

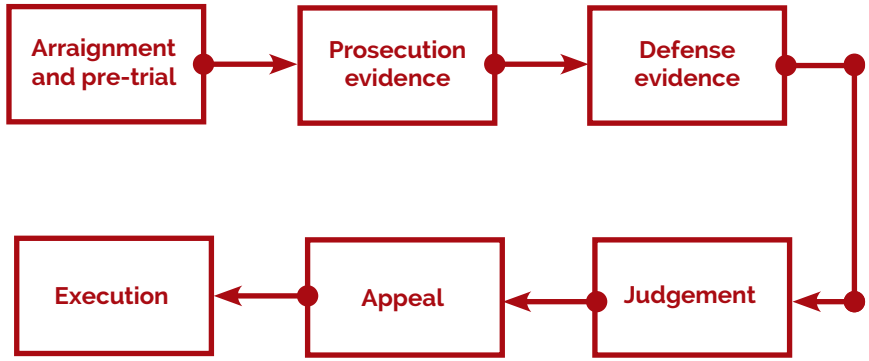
- Law enforcement official to seize.
- Law enforcement official must be in a place s/he has a right to be in.
- Discovery of the evidence must be inadvertent.
- It must be immediately apparent that what the official has discovered is evidence.

Important things to remember in case of search and seizure

- No search of a house, room, or any other premises shall be made except in the presence of the lawful occupant or any member of his/her family or two witnesses of legal age and residing in the same area.
- The officer must give a detailed receipt to the lawful occupant of the premises who was a witness to the search and seizure. In the absence of the occupant, the receipt must be left in the presence of at least 2 witnesses of legal age in the place in which the seized property was found.
- The owner of the things seized cannot be made to sign the receipt since this would be a violation of one's right against self-incrimination.

Part III

Stages of Trial



Part IV
Other Practical Tips

- If you think that your life/security is in danger, consult with your organisation.
- During an arrest or search, keep calm but stay alert and assess the situation.
- In case of an imminent or an ongoing search, take a video of your surroundings for documentation purposes.
- Practice to know and remember details (plate number, color of car, description of faces).
- Keep contacts of lawyer, friends, family who can immediately respond to your situation.
- Think of how to get out of the situation you are in without compromising your safety.
- Make good judgments based on the concrete situation.

Travel Documents and Essentials

☐ **Approved travel authorization**

☐ **Travel documents**

- ○ Passport and Visa*
- ○ Plane tickets*
- ○ Employment Certificate*
- ○ Logistics note*
- ○ Insurance*
- ○ Accommodation*
- ○ Invitation Letter*
- ○ Country briefer

☐ **Others**

- ○ Money
- ○ Travel adapter and phone

**Print three copies for self, family, and office.*

When in an overseas trip, especially when staying and traveling in crowded cities, be very vigilant and careful of your belongings. Do not simply accept unsolicited offers of "help" from strangers.

If you become a victim of theft:

- File a report at the nearest police station.
- Contact your office.
- If your passport has been stolen, contact your embassy consulate for issuance of temporary travel documents.

Contact Points

	Name	Phone	Email	Address
Organisation				
Local Host				
Family				
Insurance				
Embassy				

Organisation

Each organisation is highly encouraged to designate a Quick Response Team (QRT) and referral pathways for emergencies that may be encountered by staff on official duty travel (ODT) abroad. Establish policies and procedures on ODT and emergencies abroad, inform all staff of these, and ensure that all travelling staff know the contact details of the QRT. Each organisation should have a system to ensure that all travelling staff are monitored.

Local Host

Most of our travels are by invitation and coordinated by a local host. Otherwise, it is highly suggested for your organisation to endorse you to a network or allied contacts in your destination.

Family

Inform your family ahead on the nature of our work and the risks we face abroad. Give the basic details of your travel including itinerary, inviting group and activity. Decide which family member will be the contact in case of emergency and establish communication lines with your organisation.

Emergency Tips and FAQs

Every country has its own laws and procedures. The legal system in your destination country may be very different from the one at home. Getting support from your organisation and local host as quickly as possible is important.

Use an interpreter

Do not rely on your knowledge of the foreign language unless you are completely fluent. Ask for a professional and independent interpreter you trust. Do not take legal advice from interpreters or let them influence the way your case progresses.

What information should I share with State officers?

- Know if you have a right to remain silent. Everything you say may be used against you, so think before you speak.
- Do not offer unnecessary and excessive information.
- Make sure you understand everything. Officers may coax you into revealing private and confidential information. For legal cases, always confirm with your lawyer before you say anything.

Should I sign documents?

- Never sign blank pages. Never sign a document written in a language you do not fully understand.
- Ask for a written translation of all documents and sign only the translated copy which you fully understand.
- If there is no written translation, ask for your interpreter to translate verbally before you sign a document. Make sure you write next to your signature that you did not understand the content of the document.

I was held at the airport. What should I do?

- If you are held at the local airport, contact your organisation immediately. As soon as you land in your destination, report to your organisation and local host. In case of any delay, they will know that your last contact is at the airport.
- Respond to questions by immigration officers and airport officials in a cordial manner and present travel documents as necessary. If you are being held, ask them why, if permissible.
- In most countries, you are not entitled to an attorney during primary and secondary inspection at the airport. Keep your contact points handy and inform them if you feel your rights are being violated or if you have been detained for an unusually long period. Alert your local host immediately.
- Each country has varied reasons for denying entry to a foreigner. In case you will be deported, ask them why, if permissible.

I have been held in custody and/or arrested abroad. What should I do?

1. Know your rights.

- Ask custodial/arresting officers to explain or provide a written statement of your rights in a language you understand, when permissible.
- In case of arrest, remember the Miranda Rights that an arresting officer normally says:
  - You have the right to remain silent.
  - Anything you say can and will be used against you in a court of law.
  - You have the right to an attorney. If you cannot afford one, the State will provide for you.
  - Do you understand the rights I have just read to you?
  - With these rights in mind, do you wish to speak to me?

Ask questions to clarify your rights, when necessary and permissible. The Miranda doctrine is not a universal law but there are equivalent rights in other countries. Here are some guide questions you can ask:

- **Do I have a right to remain silent?** Could my silence be used against me?
- **Do I have a right to a lawyer?** Will the state provide me and pay for this lawyer? When can I see my lawyer?
- **Do I have a right to an interpreter?** Will the state provide me and pay for this interpreter? Is there a translation of written documents in English or a language I understand?

- **Do I have a right to consular assistance?** Has my embassy or consulate been notified? If not, when and how will they be notified? Can I contact them? Will they be allowed to visit me? If yes, when can they visit me?
- **Do I have a right to contact my family, organisation and local host?** Will they be allowed to visit me?
- **What are the allegations against me?** Will I get a written notice of charges in English or a language I understand?
- **Is the investigation complete?** If not, when will it be completed? Who is doing the investigation?
- **How long can I be held in custody?** If there is no case, when will I be released?
- **If there is a case, when will I be taken to a fiscal/ judge?** When will the trial begin? Can I apply for bail? If yes, when?

2. Notify your organisation, local host, and family.

Share important details:

- Date and place of arrest
- Where you are being detained, including prisoner number
- Names of arresting officers, if possible
- Reason for your arrest and charges against you
- Important dates and time-limits in your case
- Lawyer's name and contact details, if you have one already
- Consular representative's name and contact details

In case you cannot contact them directly, pass the information on to someone you can trust to forward to your family. This may sometimes include the prison social worker, consular representative or your lawyer.

3. Seek legal advice and services from a lawyer who is qualified to practice in the jurisdiction you are in.

- Your organisation should ensure securing a lawyer for you.
- Your local host or embassy may be able to provide you with a list of local lawyers who speak your language.
- Do not be rushed into appointing a specific lawyer on the advice of anyone with a vested interest in the case.
- Maximize time at the first instance, do not wait for the next meeting with your lawyer. Prepare by writing questions ahead and take notes of discussions. Give all the information that will help with your defense including evidences and witnesses. And ask what will make your case stronger.

4. Be wary of fellow prisoners/detainees.

- Do not share information about your case with fellow prisoners/ detainees or rely on any legal advice they give you.

5. Request for a consular representative to visit you.

- Ask your custodial/prison officer or your consulate to arrange a private visit, if permissible.
- Make sure you inform him/her of any mistreatment, document your injuries, and request to see a doctor. Keep as much evidence.
- Report other welfare issues and inform them of any medical conditions or medicines you need.
- Request them to inform your contact points (organisation, local host, family, lawyer) to update about your situation and needs.

Reminders

Be calm.
Know your rights.
Get information about your case.
Notify your contact points.

Part V
Information Security

Why is information security needed?

A non-governmental organisation/people's organisation and its staff/members receive, process and share information about its work on a daily basis. Your organisation and its staff/members need to secure vital information about your work from possible threats of unwanted distribution to, and breach by,repressive state actors and malicious private individuals.

Depending on the situation, carelessness on information security might create risks for individuals or for the whole organisation itself, including risks to security.

What information needs to be protected?

As an organisation and as individual members of your organisation, you should identify which among your files and information are for public use (e.g., finished research papers) and which are considered private, confidential, and sensitive.

Generally, information considered private, confidential, or sensitive must be accessed and distributed only within the organisation. It is also sometimes necessary to limit access to certain sensitive information within certain members of the organisation (e.g. management/officers).

How do you secure your information as an organisation?

Securing information includes physical safekeeping of documents. This should respond to possible risks such as physical damage, theft, accidental loss, and other emergencies. Connecting online allows you to reach other organisations, but also makes it possible to get your information. Care must also be exercised in limiting, or in some cases preventing, dissemination of private, confidential, and sensitive files and information through online channels.

How can your organisation improve the physical storage and security of information?

There must be systems to handle organisational documents and files.

The organisation's staff/members are crucial in safekeeping an organisation's documents. There must be an administrative personnel whose primary tasks are handling and keeping such documents. But all of the organisation's members handle different kinds of information about daily operations and are all responsible for keeping these accessible only to the necessary people.

What if people ask me about personal but private information?

Networking and advocacy require conversations about your work, and about certain people within your organisation.

But you have the right to kindly refuse giving private details about individuals from your organisation. For example, if you are asked by an unidentified individual, especially through a call/email, about personal information such as personal addresses or private phone numbers, you should not give these to the said unknown person/unverified entity. Secondarily, identify who is seeking the information.

PUBLIC	PRIVATE	CONFIDENTIAL	BEHAVIORAL	SENSITIVE
Full Name	Civil Status	Previous Employer	Favorite Food	Photo of Children or Pets
Birthday	Age	Elementary School	Photo at a Social Event	Photo of Your House
Current Employer	Personal Email Address	High School	Favorite Movies	Mother's Maiden Name
Current Job Designation	Personal Contact No.	Year Graduated From College	Favorite Hangouts	First Pet
Work Email Address	Photo With Family	Years in Current Office	Favorite Music	Location of Hometown
Photo of Yourself	Photo With Friends	Place of Birth	Photo Doing Hobbies	Photo of ID

Security protocols and policies on storing, handling, and accessing information to prevent unwanted breach must be in place and put into practice.

This includes creating secure back-ups of essential organisational files. Also needed are protocols to control access to your office premises and where crucial information is stored. This means, for example,keeping track of the identities of non-staff members entering office premises and limiting their physical access to the office if the situation demands. There must also be protocols on securing files in case of emergencies.

Physical infrastructure adequate to security needs must be present, from sturdy and secure containers for files, quality locks on office doors and gates, wired security cameras especially on strategic areas of offices (e.g., location of finance files, entrances, exits), with the location of the drives storing security footage known only to relevant personnel.

How can your organisation enhance online and device security?

These must also be tackled as an organisation, first and foremost. There must be measures to ensure security in

office devices, and care in the use of internet access and online platforms, from browsing, to e-mail, grouplists, cloud storage services (e.g., Google Drive), social media andother communications channels.

There must be staff/members of the organisation primarily tasked to handle information technology concerns, including digital security. All staff/members must be aware of secure online habits, and practice them (see next section).

Online security protocols and policies must also be in place and maintained.

What general measures could you take as an organisation to safeguard devices and internet connections?

Depending on the organisation and situation, measures could be but are not limited to

- Internet connections - Have secure passphrases on office internet/WiFi connections. To minimize risks, limit computers that work on confidential files (e.g. finances) from connecting online.
- Blocked websites - Set risky websites to be blocked, prevent unnecessary online traffic.
- Cloud services - Limit the use of cloud services for storing sensitive organisational files.
- Organisational accounts - Regularly change passwords for the organisation's social media channels, e-mails.
- Platforms that track your data - Move away from platforms that heavily track user information (e.g., Google platforms such as Gmail, Google Drive, and others).

Appropriate infrastructure must also be present, such as firewalls for the organisation's servers and website/s. Maintenance of computers and office devices that connect online is also important.

How to secure your information, as an individual with respective devices?

As individual staff/members, you have to secure the information stored in your devices, and that you are following your organisation's security protocols and policies. To assist your organisation, there are already a variety of things you can take note.

Checklist: To do's in information security when travelling abroad

- ☐ Preparations: Make time to check your laptop files and phones when flying out. Ensure that you don't have confidential files with you.
- ☐ Before travelling (from and back to your country): Maintain secure communication lines for contacting your organisation, and/or partners who will be on standby in case of an emergency.
- ☐ Upon arrival abroad: Buy a SIM card for a personal internet connection instead of using public WiFi hotspots, especially when in sensitive security situations.
- ☐ While abroad, going abroad: Follow dos and don'ts in browsing online, such as using a VPN or TOR browser if you have no choice but to connect to public WiFi hotspots, etc.

How can you ensure the physical security of your workplace?

You should be conscious that nobody has unwanted access to the devices you use at work, and if applicable, your workspace. Be careful of not leaving your work or even personal devices unlocked at your desks/workspaces. Refrain from leaving your devices unattended in public places. This is in addition to practicing the measures your organisation has established.

What are the dos and don'ts to enhance the security of your devices, including mobile ones?

In your laptops/office computers, you could take a variety of steps.

Anti-viruses and anti-malware. Do install an anti-virus and an anti-malware on your computers, such as Avast and Malwarebytes. These applications can block malicious files from infecting your computer. Do remember to scan your computers using your anti-virus and anti-malware applications regularly.

Computer settings. Adjust your computer settings to limit the information being shared to companies or whoever might be trying to access your devices. You could begin by going to your Settings/System Preferences. Don't allow the following:

- Location – "Allow access to location on this device" to "Off"
- Microphone – "Allow access to the microphone on this device" to "Off"
- Camera – "Allow apps to access your camera" to "Off"

Summary:
Do's and dont's for individual devices and browsing

On your computers/mobile devices:

- Do install an anti-virus and an anti-malware on your computers, and remember to scan regularly.
- Do create strong passphrases, and have different ones for your accounts and for your devices.
- Do back up those files vital to your work.
- Don't allow unnecessary tracking of your device activity by turning off automatic access to location, camera, and microphone. In mobile, don't allow unnecessary mobile application permissions.
- Don't be careless about private, confidential, and sensitive files; encrypt them if necessary.

On connecting online:

- Do use a VPN, browser applications, and search engines that commit to not tracking your information, especially when using public WiFi in airports, cafes, or malls.
- Do adjust browser settings to prevent others from tracking your internet activity.
- Don't use online banking when using public internet connections.
- Don't click pop-ups (and immediately close them if accidentally clicked) and suspicious emails and sites.
- Don't unnecessarily disclose on social media where you are or who you are with.

Secure passphrases. Passphrases are more recommended than passwords, as password-cracking applications used by malicious individuals will find longer phrases more difficult. It is advised to choose phrases that are familiar enough to you but not predictable to other people. Combine uppercase and lowercase letters, numbers and special characters to increase password difficulty.

It is important to have different passphrases or passwords for different accounts. It is never advised to re-use a password. This is applicable to your computers, mobile devices, social media and e-mail accounts, and others. Changing passwords regularly is also important, especially if you feel that your accounts have been breached.

There are also applications you can use to keep different passphrases and passwords, such as KeePass (see "Some suggested applications" box below).

Keeping files. Ensure that you identify which information stored in your computers and devices is public, and which is private, confidential, and sensitive. Do back up those that are vital to your work. Don't leave private, confidential, and sensitive files in your computers and devices easily accessible. If necessary, do encrypt them (see "Other tips related to information security" on how).

For mobile devices such as cellular phones, the ones above also apply, but in addition:

Mobile applications. These can be found in your Settings. Do turn off those that are not necessary in certain applications, such as permissions to your microphone, location, messages, or contacts. For instance, if it's a photo application, there is no reason for it to access your messages or your location.

What are the do's and dont's when connected online?

First, it is highly important to practice an online browsing habits that minimizes unnecessary and malicious exposure of your information to third parties. Second, some choices of applications, email clients, and browser add-ons will also help. But, not practicing safe browsing habits despite having good applications still increases threats to your online privacy.

Browsing, searching online.

- Be careful to not click pop-up advertisements or even banner advertisements. In the settings of your browser application, disable saving passwords, be sure to click the options to block pop-ups, and the "do not track" option.
- Refrain from downloading suggestive applications being offered by websites.
- It is strongly suggested that you use "Incognito Window or Private Window" available from your choice of browser. For example, the Firefox incognito window clears your search and browsing history when you quit the browser.

Google-related platforms are known for tracking your browsing to sell it to advertising companies. Moving away from Google Search is encouraged; instead, you may use more private search sites such as DuckDuckGo, making them your default search engine. Instead of Google Chrome, Mozilla Firefox is one suggested browser application. TOR Browser is an option for additional anonymity especially in public WiFi connections (see "Some suggested applications" below).

In your browser, use add-ons such as AdBlock Plus to block ads. Privacy Badger as another way to stop third parties from tracking you.

E-mail.

- Always be careful of taking note of senders, attachments, and links. Common suspicious e-mails include winning contests you haven't entered, or instructions to change your bank account passwords online. Like in browsing, refrain from clicking on suspicious emails, or on the links in these e-mails.
- It is best to separate work from personal email accounts as a security measure. If somebody needs to communicate with you about work concerns, be sure to give them your work email account, and e-mails about personal concerns to your private e-mail accounts.

Shifting from Google Mail is also recommended, as they analyse even your email content to "customize search results" among other purposes. You may shift to Protonmail. Also, use a non-browser based email application, such as Thunderbird.

Social media and instant messaging.

- Refrain from unnecessarily sharing information. This includes passport details, bank account details, and even your location. Of course, these also include files from your work that are considered private, confidential and sensitive.
- If information about a trip, event or meeting is not immediately for the public, it is sometimes better to avoid posting photos and details as they happen (e.g., "at the moment" posts).
- In cases where online instant messaging is unavoidable, use applications such as Signal (see "Some suggested applications"). Also, avoid interlinking your social media accounts (e.g. Facebook) as a user account in other applications.

Using public WiFi/internet connections.

- Anyone can connect to public internet connections, including individuals wanting to spy and get your data.
- If you have no choice but to connect to public WiFi hotspots in airports, cafes, malls, you may want to make your browsing "anonymous" by using a Virtual Private Network (VPN).

A VPN basically masks the unique label of your device (your "internet protocol (IP) address") to prevent "eavesdropping" on your internet use.

- Never log in sensitive accounts, such as your bank account, on public connections.

Other tips related to information security

Backing up files. USBs are the easiest storage device for backing up your files but their portability can also mean they can easily be lost. It is advised that you have at least three back-up files on three different storage devices (e.g., USBs, hard drives, etc) with two readily available where you work, and one secured on the side.

Encrypting files. Encrypting files means securing them in your storage devices, with password protection. Sometimes you may need to encrypt your private, confidential, and sensitive files. You may use applications such as VeraCrypt. If so, do not forget and never share your password to not lose your access to your secured files.

Securely delete files. Deletion by clearing out your computers' Recycle Bins still leaves some data that can be traced by other parties with the right recovery applications. If the situation demands a more thorough deletion of private, confidential, and sensitive files, you may use applications such as Eraser.

Some Suggested Applications

Malwarebytes
(Anti-malware application)

ProtonVPN
(Free VPN, needs a protonmail account)


Mozilla Firefox (Browser)


KeePass (Password Storage)


Signal (Encrypted messaging)


Eraser (Secure deletion)


TOR (Browser)


VeraCrypt
VeraCrypt (File encryption)


DuckDuckGo
Duckduckgo.com (Search engine)

References:

Karapatan, http://karapatan.org/files/BUST%20CARD%20ENG_TAG%2020170313.pdf

Miranda Rights, http://www.mirandawarning.org/whatareyourmirandarights.html

Fair Trials International, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/320911/Annex_8_-_FTI_-_Arrested_in_another_country.pdf

Computer Professionals' Union. 2019. Information Security Training Workshop. Training held at IBON International, Quezon City, Philippines.

Karapatan. 2019. Human Rights and Security Training Workshop. Training held at IBON International, Quezon City, Philippines.