# The IFJ's Physical Safety & Digital Security Training

## Program

### DAY 1 – Physical Safety & Security

| | |
|---|---|
| 9:30 – 10:00 | Session 1: Introduction & icebreakers |
| 10:00 – 10:30 | Session 2: Experience & expectations |
| 10:30 – 12:00 | Session 3: Understanding safety vs security |
| | Break during session 3 |
| 12:00 – 13:00 | Session 4: A risky profession - digging up trouble |
| 13:00 – 14:00 | Lunch |
| 13:30 – 14.30 | Session 5: Safety in the field |
| 14:30 – 15.30 | Session 5 continued: Risk assessment & safety planning |
| 15:30 – 15:45 | Break |
| 15:45 – 16:45 | Session 5 continued: Risk assessment & safety planning |
| 16:45 – 17:00 | Session 6: Wrap up |

### DAY 2 – Digital Safety & Security

| | |
|---|---|
| 9:30 – 9:45 | Session 7: Recap: Check expectations |
| 9:45 – 10:45 | Session 8: Risk hunting for digital security |
| 10.45 – 11:15 | Session 9: Malware & basic protection |
| 11:15 – 11:30 | Break |
| 11:30 – 12:45 | Session 10: Understanding digital risk |
| 12:45 – 13:45 | Lunch |
| 13:45 – 14:45 | Session 11: Protecting emails |
| 14:45-15:00 | Break |
| 15:00 – 16:00 | Session 12: Mobile phone safety |
| 16:00 – 18:00 | Session 13: Risk assessment planning |
| 18:00 – 18:30 | Session 14: Wrap up, evaluation & close / certificates |

**Day 1** **Session 3: Handout 1**

# THREATS

## Threats faced by journalists in the line of duty in Pakistan

- Non-state actors - including armed groups
- State actors - including security forces, agencies and government officials
- Professional negligence
- Foreign agencies and victims of terrorism
- Killing of journalists in targeted attacks (from armed groups and security forces)
- Threats to life, family and property
- Bombings, including suicide attacks
- Criminals, drug traffickers and smugglers
- Different pressure groups, including political, social and business
- Kidnapping (by both armed groups and security agencies)
- Lack of experience and conflict reporting skills
- Lack of interest by media organisations to provide security to staff in volatile regions
- Lack of in-house safety protocols for managers and journalists in media houses
- Lack of safety trainings
- Ignorance or lack of understanding of professional ethics
- Threats from organised gangs
- Restrictions on freedom of movement and access to information
- The Frontier Crimes Regulations (FCR): special laws relating to KP/FATA

## Causes of threats

- State authorities
- Terrorism, terrorists and the prevailing security situation
- Lack of understanding on safety issues by media
- Lack of attention to professional ethics by media
- Lazy journalism – leading to negligence or inattention to facts
- Lack of investigative skills among journalists
- The drive for breaking news impacting due verification of facts
- Lack of interest by media organisations to take journalist security seriously
- Biased reporting. Not taking all sides of the story into account. Being partial to the ideas of one group (militants, religious and political) at the cost of others.
- Absence of professional neutrality in handling news stories
- Improper reflection of cultural taboos, values and sensitivities in reporting
- Exposes on issues of governance and corruption
- Sensational and exaggerated reports
- Targeting a specific ideology or school of thought in a story
- Lack of safety training in areas where journalists have known biases and views
- Conflicts of interests and lack of professionalism in journalists – where journalism gives cover to other personal pursuits
- Bribery or unprofessional payments - journalists working as "public relations officers" for militant groups, political parties, political administration, and even as informants of intelligence agencies for financial gains, leaving them vulnerable.

Intermedia, 2011, Practicing Safe Journalism in Conflict Conditions: A Safety Guidebook for Pakistani Journalist: http://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Intermedia.pdf

**Day 1:** **Session 4: Handout 2**

## How to reduce threats: Practical Steps

**INDIVIDUALS:**

- Good, balanced reporting
- Professionalism
- Move away from harm
- Stay impartial, objective and independent
- Don't sensationalise
- Observe cultural sensitivities
- Practice ethical journalism
- No story is worth dying for
- Sensible movements
- Protect your identity
- Careful use of language
- Verify sources
- Research and plan ahead
- Be aware of hostile zones
- Travel safely
- Safety in field
- Strength in numbers
- Mind map your entry and exit
- Leave footprints
- Have contacts that can help
- Give right of reply
- Be careful with bylines and content

**MEDIA ORGANISATIONS:**

- Training
- Professional guidelines
- Ethics training
- Safety protocols
- Analysis of existing threats
- Advocacy for independent journalism/safety

**NATIONAL & INTERNATIONAL:**

- Dialogue between media and state authorities
- Holding state agencies accountable
- Bringing perpetrators to justice
- Laws and mechanisms
- Training eg state forces on role of media
- Civil society advocacy and cooperation

Intermedia, 2011, Practicing Safe Journalism in Conflict Conditions: A Safety Guidebook for Pakistani Journalist: http://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Intermedia.pdf

**Day 1:** **Session 4: Handout 3**

## Essential guidelines for reporting and planning for safe and secure journalism

*Importantly: No story is worth dying for!*

- Plan ahead, plan carefully
- Mind map your entry and exit
- Leave footprints on assignment
- Have contact who can help
- Follow ethics
- Stay objective
- Stay impartial
- Stay independent
- Strengthen your network
- Strength in numbers
- Give opposition the right of reply
- Produce balanced reporting
- Give a variety of people's perspectives
- Mind your language
- Think about your bylines and content – is it safer to not use one?
- Train newsroom staff

Intermedia, 2011, Practicing Safe Journalism in Conflict Conditions: A Safety Guidebook for Pakistani Journalist: http://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Intermedia.pdf

**Day 1:** **Session 4: Handout: 4**

## Assessment Workshop: Physical Environment

**Your Building**

| **Vulnerability** | **Source of risk** | **Risk level (low, medium, high)** | **Possible solution** |
|---|---|---|---|
| Describe the physical layout of the office. Include its location to other businesses or homes in the area and access to the street | | | |
| Are access points and entries protected with lockable entry? | | | |
| Do employees stand outside near doors to smoke, take calls and leave the doors open? | | | |
| Number and gender of employees on-site between 10pm and 5am | | | |
| Describe the nature and frequency of client/ customer/ passenger/ other contact | | | |
| Does the office have security protocols for allowing visitors that may not be known to all staff? (ID check, cell phone deposit, metal detector) | | | |
| What is the security history of the office and environment? | | | |
| What physical security measures are present? | | | |
| How does your office monitor office visitors prior to giving them entry to the office? | | | |
| Has security training been provided to employees? Has it been effective? | | | |

**Inside the Office**

| Vulnerability | Source of risk | Risk level (low, medium, high) | Possible solution |
|---|---|---|---|
| Describe the physical layout of the office. | | | |
| Number and gender of employees on-site between 10pm and 5am | | | |
| Can guests in the office see computer screen(s), whiteboards or other places where business information is visible? | | | |
| Are meetings held in open spaces where visitors might hear? | | | |
| What physical security measures are present? | | | |
| Are network devices like your routers, hubs or modems kept in secure rooms or cabinets? | | | |
| Do staff members use file-sharing services that are not controlled by office (eg DropBox)? | | | |
| Are your desktop computers and laptops attached to a security cable with a lock to prevent theft? | | | |

**Mobile phones**

| Vulnerability | Source of risk | Risk level (low, medium, high) | Possible solution |
|---|---|---|---|
| Do staff have sensitive information stored on mobile phones (photos, interviews, essential contact information)? | | | |
| Do staff use long/secure passwords? | | | |
| Are staff protecting the data on their phones with encryption? | | | |
| Do staff use text messages to share work information? | | | |
| Do staff use applications like ChatSecure to send instant messages? | | | |
| Do you or your colleagues make backups of ‘crucial’ phone data and keep the | | | |

**Day 1:** **Session 5: Handout 5**

## The five basic principles of personal safety - SAFER

1. SITUATIONAL AWARENESS.
    - In conflict zones you must accept the risk you are taking and always be aware of threats that already exist. **Always be suspicious and cautious!**

2. AVOID ROUTINE AT ALL TIMES

3. FOLLOW SECURITY PROCEDURE AND PROTOCOL.
    - Set a standard policy and standard operating procedure and stick to it. Make sure the procedures fit with your editorial task they have to be realistic.

4. EXERCISE COMMON SENSE AND COMMON KNOWLEDGE.
    - Know your surroundings and safe havens. Gain knowledge of the present threat.

5. REMAIN ANONYMOUS AND ALWAYS SHOW CONFIDENCE LIKE YOU BELONG THERE.
    - Always show alertness when in public places. Assess the situation, react and make safety decisions based on your personal judgment - not your fixer or anybody else! Always avoid confrontation and being drawn into any type of threatening position. If you do get into problems remain calm and try to defuse the situation before it escalates. If this does not work disengage and make your way to a safe location asap.

**Day 1:** **Session 5: Handout 6**

## Guidelines on safety for reports covering conflict

**No story is worth dying for:** Question your motives for covering a story. What, and whose purpose, will the story serve? Can the story wait and maybe be told another day, in a better way?

**Plan ahead, plan carefully:** Study the situation you will be working in: risks, chances of safety, and which way circumstances may go. Always assume the worst and be prepared for it in a situation of conflict.

**Mind map your entry and exit:** A journalist should have working knowledge of all routes, roads, byways and streets. While you can carry a map with you, often emergency situations allow little time to consult them. Look at them before you go to field and have a mental image of the major roads and routes.

**Leave footprints:** Call friends and family from locations as soon as you arrive, keep them informed about your movement so they know where you were last and with whom. This can help save time for helpers in case you need to be rescued or traced in a hurry.

**Have contacts that can help:** Keep handy contacts, phone numbers, addresses of media and media support organisations, colleagues and friends in the community who may be able to help you quickly in times of trouble. Do not jeopardise their safety by association with you – anything irresponsible or unethical you do will have consequences for them because you have the list of contacts with you.

**Follow ethics:** You are there to serve the community. Help people trust each other by being truthful, independent, fair, impartial, transparent and accountable for your work.

**Stay objective, impartial and independent:** Do not become part of the story – report only facts. Secondly, do not allow yourself or someone to turn you into their spokesperson or use you to propagate their stance – your position of influence as a journalist and access to information flows from community's trust and interest. Don't violate that trust. Lastly, do not give in to pressure tactics or accept bribes, favours and other inducements at the cost of your independence, reputation and safety.

**Find strength in numbers:** When you go out to report, go with a group of journalists. It is easy that way to be identified as a reporter and easier still because conflicting parties cannot bear pressure on you of any kind when you are there as a group. This is especially important for freelance journalists who usually have little to no organisational support.

**Give right of reply:** Stick to facts with proof and evidence. In case of a controversy or allegation, always give the party that is accused of a wrong the chance to reply in the same report.

**Be careful with bylines and content:** If you are in the newsroom, do not give byline/dateline in case of a sensitive story or threat, nor change content, even words and quotes, which distort sense of stories.

**Mind your language:** stay mindful of the meanings and connotations that words convey to avoid misunderstandings.

Intermedia, 2011, Practicing Safe Journalism in Conflict Conditions: A Safety Guidebook for Pakistani Journalist: http://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Intermedia.pdf

**Day 1:** **Session 5: Handout 7**

## The Do's and Don'ts of staying out of harm's way

**Before reporting:**

- Know where you are going, and what to expect.
- Consider identifying your vehicle as "media" and travelling with other journalists.
- Have reliable local contacts, or travel with someone familiar with the area.
- Dress appropriately. Do not carry anything that may look like a weapon.
- Keep close people informed about your journey.
- Consider how to report on violent areas from a safe distance.

**What to take with you:**

- Additional water, food and fuel for emergencies.
- Maps, emergency first aid kit, batteries, contact numbers, reliable charged phones.
- Program an "ICE" number into your phone: person to call "In Case of Emergency".
- Papers identifying you as a journalist and who you work for.
- Extra cash, a short wave radio to keep in touch with events and a white flag.

**What to do on location:**

- No story is worth your life; do not endanger yourself or others.
- Be polite and treat people with respect. If threatened, get out – fast.
- Do not move into an area where a bomb has exploded.
- Do not leave your vehicle unattended.
- Avoid bias – operate as a professional journalist.
- Balance risks against benefits before going anywhere dangerous.

**If you get into trouble:**

- Contact your union and alert colleagues, editors, friends and family.
- If detained, explain your role as a civilian journalist.
- Never resist if you are kept hostage or someone holds you at gunpoint.

**As soon as you receive a threat:**

- Document the circumstances by which threats were received including date, time and persons involved. Where possible, save them for evidence.
- Let others know immediately – your superiors, colleagues and family.
- Seek support from unions, press clubs, press associations, media groups and international organisations.
- Report it to the police in writing, citing the circumstances and possible source.
- Ask for police protection but only when absolutely necessary and if police in your area can be trusted.

**If you have received threats before and they remain unsolved:**

- Keep emergency numbers ready; have them on your mobile phone's speed dial.
- Inform those close to you about where you are going, your intended time of arrival and expected return.
- Do not travel alone
- Meet unfamiliar contacts in public places and tell your office of your plans.
- Vary your routes and routines to be unpredictable.
- Know the different entrance and exit points of places you visit.
- Be careful with phone calls, text messages and other forms of electronic communication that can be tracked.
- Identify safe havens and have them ready for emergencies.
- Know your rights
- Be prepared, not paranoid.

Intermedia, 2011. Practicing Safe Journalism in Conflict Conditions: A Safety Guidebook for Pakistani

**Day 1:** **Session 5: Handout 8**

## Riots and Public Disorder

**Preparation and planning**

- What is the aim of the task
- Location
- The reasons for the demonstration
- Background of the parties involved.
- Security force presence and their tactics. Types of threat, i.e. tear gas, guns etc
- Protective measures.
- Permissions and documentation to cover the demonstration.
- Could journalists be targeted specifically by protestors or security forces?
- Time needed to be in the field
- Gender and Cultural Safety issues.
- Equipment required. Protective equipment, first aid, maps, size of camera equipment to be used, communication and tracking equipment, logistical supplies (such as food and water),
- Transport and vehicle placements during the demonstration.
- Contact Lists. News desk and emergency services, local hospitals, security force commanders, embassies (if required), local sources and contacts.
- Intelligence and analysis. Know what to expect and how to get assistance, especially in the case of an arrest or detainment.
- Use of social networks to locate riot location and incident occurring good resource for intelligence. Remember the authorities are also use these sites.
- Reconnaissance. Time spent on research and reconnaissance is never wasted. Detailed Recce of the planned demonstration area.
- Safe Locations. Knowing safe rendezvous points and areas of extraction.

**Contingency planning**

- Action in the event of a casualty.
- Safe havens, rendezvous points if separated and areas of low threat.
- Escape routes.
- Procedures in the event of an arrest or detainment.
- Being overrun by the protestors.
- Camera/filming equipment confiscation.
- Transport related issues, such as the loss of a vehicle.
- Procedures in the event of a personal or sexual assault.
- Loss of communication, GSM Signal and equipment.
- Long term detention in a remote location or foreign country.
- Embassy and Consulate support in the event of an incident.

Intermedia, 2011, Practicing Safe Journalism in Conflict Conditions: A Safety Guidebook for Pakistani Journalist: http://www.fes.de/themen/menschenrechtspreis/pdf/mrp2012/Intermedia.pdf

**Day 1:** **Session 5: Handout 9**

## IFJ Safety Guidelines for Covering Demonstrations and Civil Unrest

**Preparation**

1. Plan in advance. Know what to expect. Know how to get assistance. Know where the safe areas are.
2. Establish pre-arranged contact points
3. Bring a cell phone and preferably a satellite phone with emergency numbers pre-set for speed dialing.
4. Carry first aid kits and learn how to use them.
5. Bring eye protection.
6. Wear loose natural fabric clothing as this will not burn as readily.
7. Wear colour distinctive clothing from police forces and army.
8. Wear comfortable and good shoes.
9. Carry a small backpack with enough food and water to last for a day. Backpack can be used as shield against rubber bullets, water cannons and rocks.
10. Bring your prescription/non-prescription medication. Take in original, labelled containers from pharmacy.

**At the scene**

11. Always remain in team. Safety is in numbers especially at night.
12. Always carry press identification but conceal it if it attracts unwarranted attention. Do not introduce yourself as a member of the press, you do not want to agitate the crowd further.
13. Take as few notes as possible not to attract attention.
14. Always arrange interviews outside of the riot area itself.
15. If you are a reporter you don't have to be in the crowd as long as you can see what's happening. Walk along side of the protesters. People who throw stones usually do that from the middle of the mass of protesters where they can blend back into the crowd.
16. If you are a photographer or camera operator, try to shoot from a higher vantage point.
17. Run if you see policemen running towards you in riot gear.
18. Do not pick anything up. If you pick up a rock the protesters have thrown, you can get arrested because it might look as if you are going to throw it. If you pick a tear gas canister, you will badly burn your hand.
19. Do not resist arrest.

**During riots**

20. Stay calm and focused when things get most intense.
21. Be prepared to run away from smoke, fire, police and flying objects in general. Do all this while your head is down.
22. Tear gas. Position yourself upwind if there is a possibility that tear gas will be used. If you are hit by tear gas, run away breathing as little as you can. Once safe, take the bottle of water and flush your eyes. People with asthma, respiratory problems or infections, pregnant women, anyone ill or with a poor immune system, seizure disorders, eye infections, contact lens wearers should avoid tear gas by all means.
23. If you wear contact lenses, the irritating gases will get trap between the lens and the eye and may increase the amount of damage and irritation. Always prefer glasses.
24. Rubber bullets. If you can't run or duck behind something, turn your back against the police, get down on your knees, keep your head down and protect your face.
25. Water cannon. Turn around, cower down, close your eyes and make a tent in front of your nose and mouth so you have air left. Be aware you can be swept away by the water.
26. Work with the team and keep a mental map of your escape route if things turn bad.

**Advice in case of Arrest**

- Know your rights: you have the right to remain silent and to be assisted by a competent and independent lawyer of your choice.
- You have the right not to be subjected to torture, intimidation, deceit, other forms of harassment
- You have the right to be informed of these rights and to be told that you say may be used against you in court
- If you are detained, you must be treated as a human being and you are entitled to due process.

**Conduct at Checkpoints and Roadblocks**

- Always be polite.
- Avoid confrontation.
- Identify yourself as a journalist.
- If on foot, approach the checkpoint with only necessary papers on hand.
- When in a vehicle, keep windows and doors locked; do not alight unless told to do so.
- Never try to film without permission.
- If soldiers or militia manning the checkpoint are hostile or nervous, offer sweets or cigarettes.
- When showing your identity card, let them also see photos of your wife and children to bring out the more human aspect of your work.
- Let them know that people know where you are and that you are expected back.
- Make them understand that you are not a threat.
- Stay polite but be alert especially for soldiers who seem to be listless and would not look you in the eye.

**Day 1:** **Session 5: Handout 10**

## Pre-assignment security assessment

**1. Assignment description**
Identify dates of travel, itinerary, and names of staff members, freelancers, and others participating in the assignment.

**2. Risk analysis**
Identify potential security risks associated with the assignment.

- *2.1 Hostile subjects*
  Assess the chances that you, your team, or the local contacts interacting with you on the ground will be targeted for surveillance or attack. Identify potentially hostile actors and possibly relevant hostile actions or attacks.

- *2.2 Location risks*
  Identify risks associated with reporting in the location, such as outbreak of hostilities/escalation of conflict; abduction/kidnapping; interactions with hostile authorities (problems crossing borders/checkpoints, arrest, detention); physical or electronic surveillance; confiscation/misuse of sensitive information; health risks; dangers associated with various means of transportation; common crime.

- *2.3 Security for local contacts*
  Identify risks that people working or interacting with you (local translators, drivers, sources, witnesses, etc.) may face.

- *2.4 Research risks*
  Address the risks associated with conducting your work, such as conducting interviews, taking photographs, filming etc understanding any documents and photographs may have evidentiary value.

- *2.5 Profiles*
  Explain how your own profile, the profiles of other members of your team, and that of your news organisation may increase or decrease the risk.

- *2.6 Information reliability*
  Explain whether the team has access to the latest security updates for the area and the degree to which the available information may be outdated or otherwise limited.

**3. Proposed measures to minimize risk**
Describe measures that will be taken to minimize the risks associated with carrying out the assignment.

- *3.1 Lodging*
  Identify all hotels and other types of accommodation. Explain why the proposed lodging option is considered safe. Indicate whether the lodging has functioning communication (phone lines, Internet access). Provide contact information.

- *3.2 Transportation arrangements*
  Describe transportation arrangements. If using public transport, indicate associated risks and how they will be addressed. If hiring a car, explain how the driver has been or will be selected. Provide the driver's information.

- *3.3 Communication*
  Describe whether you will use an international cell phone, local cell phones, satellite phones, land lines, and/or portable radios, and describe any problems associated

with the use of each. Will the team have regular Internet access. Identify the best means of communication with headquarters.

- *3.4 Profiles*
  Describe whether you plan to operate with a high or low profile and the risks with each approach. Describe how you will enter the area and present yourself at various situations (at the border, at checkpoints, during other interactions with authorities). If there are risks associated with the team members' individual profiles (such as ethnicity, race, gender, or sexual orientation), describe how they can be addressed.

- *3.5 Research and other activities*
  Describe how you plan to carry out safe reporting for you and your subjects. Indicate whether specific measures are necessary to ensure anonymity of certain subjects.

- *3.6 Security of information*
  Specify measures to protect sensitive information while on assignment. Indicate measures to ensure the security of information in case confiscated or otherwise compromised.

- *3.7 Security of others*
  Describe proposed measures to ensure security of people working or otherwise interacting with your team.

- *3.8 Other security measures*
  Describe any additional security measures necessary to minimize the risks associated with the mission. These may include health risks, evacuation etc.

**4. Check-in procedures**

Specify check-in procedures for the assignment:

- Regularity and times; specify both the time in the area of travel and the time at location where the security check-in person is based.
- Method
- People responsible
- Procedure for action in case you or your team does not check in. The usual security interval for check-ins is one hour, meaning follow-up action will be taken if after one hour from specified check-in time.

In addition, specify:

- Those responsible for receiving check-ins, when they should notify the supervisor;
- If and when should the news organisation try to reach emergency contacts;
- What further action should or should not take place (which may include notifying relatives, notifying other media, or contacting the embassy).

**5. Contacts**

Provide all contact information for the following:

- Staff travelling on the assignment
- Staff conducting check-ins
- Supervisors and other back-up contacts in headquarters
- Non-staff participants (consultants, interpreters, drivers)

**6. Emergency contacts**

Contacts in-country:

- Indicate a designated in-country security contact;
- Provide a list of additional contacts U.N. or humanitarian staff, local NGOs

CPJ, https://cpj.org/security/assessment_form.pdf

**Day 1:** **Session XXX: Handout 11**

## Says Who? Getting the Right Source in Conflict Reporting

**Be strenuous and self-critical in assessing your sources**

- Ask: are they in a position to know the information they are giving you?
- Or are they reliable?
- Or are they passing on hearsay?
- Would your reporting stand up to rigorous fact checking or other independent scrutiny?
- Are corroborating sources truly independent or each other?
- If you are reporting from a document, do you have it in your possession or have you only been told about it?

**Are your sources transparent?**

A solid news story allows the audience to form its own judgement on its reliability and accuracy based on the sources provided. Clearly identifying sourcing is essential in stories about conflicts, disputes or any controversy. It is the journalist's own protection against accusations of bias or partiality and add credibility.

**How do we know?**

- Sourcing addresses the question 'how do we know?' and requires active attribution.
- We would know '12 people died in fighting' either because somebody told us or because we personally counted the bodies.
- But if a guerrilla leader is the source, how do we know he is telling the truth?
- The key is to identify sources clearly so that the reader can come to his or her own conclusions
- If you are writing about a conflict, make every effort to speak to both sides, and to find a non-aligned source for independent assessment
- If you are writing a reaction piece, for example, about a military operation, speak to a diverse selection of people on the street, as well as experts
- If you are writing from a specific location, bring the reader there by presenting some notable details. Make clear to the reader that this is you, the journalist, on the spot
- If the article is based on a report or document, do everything you possibly can to gain access to the original, and to have sources confirm its legitimacy. Be transparent and tell the reader, for example 'according to a document seen by this reporter' or 'according to a document obtained by this newspaper'

**The two source rule**

- The golden rule of sourcing is that to treat something as publishable, you need to confirm it from at least two reliable and independent sources.
- Independent sources should be independent.
- If you have only one sources for a particular detail but you it is important to report or there is a good reason to believe it is true, then write it as 'source A says' or source A alleges'
- Where you know a fact to be in dispute, make it clear that different people have different opinions
- Using a single source in such a case depends on assessing the reliability of that source and the likelihood of the facts being correct. In such cases, the source should almost always be named. Sometimes of course, only one person can know some

**Authoritative/relevant source**
A good source is always someone in authority who is in a position to know. A defence minister is clearly an authoritative source on matters of defence policy; so is a senior official in his ministry, especially if you use the person's name.

**No sourcing**
Specific sourcing is not necessary if information is not disputed by anyone, for instance when relaying a clear historical fact, such as 'Pakistan became an independent republic in 1947' But remember that many historical 'facts' are disputed, so be careful.

**Official sources**
An official source is someone with access to information because his job, although not necessarily the person in charge. A police officer might be an official course about a security story, a civil servant on a story about government policy handled by his or her department, a UN or NGO worker for a story about humanitarian affairs they are on and so on.

When sources are unnamed, describe their position as closely as possible. If the deputy in the example above refused to allow you to name him, referring to him as 'a senior official at the Ministry of Economy' is, again, better than simply 'an official'.

**Passive sourcing**
Passive sourcing should be avoided. Terms such as 'it was understood', 'it was reported' or 'it was believed' are not appropriate for good journalism.

But 'Radio Pakistan reported' is fine if that is the source. 'Everyone knows that' is definitely not a valid source.

**Sourcing opinions**
If the story involved a dispute between two or more parties, and only one side of the dispute is immediately available, use sources for facts not opinions and make sure it is clear that the story has been sourced from only one party.

Finally, remember the rules of impartiality and balance. Your report should not take sides in the dispute, and must take care to present the opinions as viewpoints, not as facts. If you are writing a critical report, you must allow the other side a fair response.

**Anonymous sources**
If a source is unwilling to put his or her name on the record, be sure you are not giving them a free license to spread lies and rumours. They may have a legitimate reason, such as fear of reprisal for speaking out.

If they won't put their name to something they have said, think carefully whether you are willing to put it in your story under your own byline too.
A simple two-question test before using anonymous sources:

1. How much direct knowledge does the source have of the event?
2. What, if any, motive might the source have for misleading us, 'spinning' the story, or hiding important facts that might alter our impression of information?

**Day 2: Pre-Workshop Questionnaire** **Handout 12**

## Digital Security Pre-training questionnaire

1. Have the participants attended digital security training before?
2. Do participants have access to a technical specialist who can help them with digital safety tools and practices outside of class?
3. Has anyone in your organization had a device stolen or confiscated? Has anyone lost a device with sensitive information on it?
4. Has your organization ever been a victim of a cyberattack (virus, loss of data, communication interception, email/social network hacking, website shutdown)? Please provide a brief description of the event(s).
5. As far as you know, has your organization been under surveillance?
6. Are you able to supply laptops for each participant in the training?
7. If yes, will the laptops be examined for viruses or other malware prior to the start of training?
8. What operating systems will the participants be using? (And are the operating systems genuine?)
9. Will an Internet connection be supplied during the training?
10. If so, will the connection be shared with your organization's staff?
11. Is the connection sufficient to support a video stream from YouTube that might be used for demonstration purposes?
12. Is the Wi-Fi connection secured with a password?
13. If so, does the Wi-Fi access point use WPA2 encryption to protect the activities of participants?
14. Will each participant have a smartphone?
15. What mobile phone brands/networks will the participants be using?
16. Is the use of encryption legally permitted? (Is there a ban on the use of VPNs or the use of software that encrypts data that is stored on a PC)?

**Day 2:** **Session 7: Handout 13**

## Digital Security in a nutshell:

- Protecting devices from malware and hackers
- Protecting information from physical threats and sensitive files on your computer
- Secure passwords
- Recovering from information loss
- Destroying sensitive information
- Keeping online communication private
- Anonymity and bypassing censorship on the Internet
- Protecting yourself and your data when using social networking sites
- Using mobile phones and smartphones as securely as possible

**Plan for safety**

- Know what to protect
- Understand the Threat
- Make a Plan

**Protect Communications**

- Mobile devices
- Internet connections
- Email and instant messages
- Meet in person

CPJ and Danny O'Brien, Information Security: https://cpj.org/reports/2012/04/technology-security.php

**Day 2:** **Session 8: Handout 14**

## Planning for digital safety - assessing digital risk:

Assessing risks is a process of:

- Identifying valuable assets (e.g., contact lists, research data, interview notes or audiovisual files)
- Determining what threatens those assets
- Assessing when and where the threats are likely to hit
- Weighing the potential consequences
- Questions commonly used in the process
- What is valuable that needs to be protected? (E.g., phones, laptops, important articles and photographs)
- How likely is it that specific information or a device is in danger?
- What are the most likely sources of threat to that material? What are the human threats (such as thieves or someone who could confiscate equipment), infrastructure threats (such as pirated software or poor power supplies), and environmental threats (such as natural disasters)?
- What is the potential impact of an individual device or type of information being lost, stolen or destroyed? Would the impact be big or small?
- What can we do to mitigate the risks?

When assessing risks, it may help to think of your environment in layers:

- Neighborhood
- Outside the office
- From the front door
- At your desk
- Your digital "space"
- Your human network

A safety plan is your response to the threats you have identified. Questions that may help formulate your plan include:

- What risks can be eliminated entirely and how?
- Which ones can be mitigated and how?
- Based on their likelihood and significance, which risks should be addressed first?

Things to keep in mind:

- Be inclusive in your planning
- Be judicious with permissions and access

**For Further Learning:**
Guide: "How to Protect Your Information from Physical Threats" (Security in-a-box).
Guide: "Threat Assessment & the Security Circle" (Equalit.ie).
The SSD Project: "Risk Management" (EFF.org).

Internews, 2012, Speak Safe: Media Workers' Toolkit for Safer Online and Mobile Practices: http://www.internews.org/research-publications/speaksafe-media-workers-toolkit-safer-online-and-mobile-practices

**Day 2:** **Session 9: Handout 15**

## Basic Protection checklist

**Tips for securing your PC and Online Accounts**
A clean and protected PC is fundamental to your digital privacy. If your PC is infected with a virus or if it doesn't take advantage of some common safety features, other efforts to protect your data may be undone. Here are some common recommendations to get you started in making your PC and online accounts more secure:

- **Get an anti-virus software**
- **Update everything**
- **Enable Automatic Updates**
- **Make sure your PC's firewall is on**
- **Use strong passwords**
- **Encrypt everything**
- **Protect accounts with two-step verification**
- **Think first!**

**Prevent malware**
**On a PC:**
Download and install one application from each of the following categories:

*Anti-virus*
- AVG
- Avast!
- Avira

*Anti-Spyware*
- Super Anti-Spyware
- Spybot Search & Destroy
- Adaware

*Scanner/remover*
- Malwarebytes Anti-malware
- Trend Micro HouseCall
- Microsoft Safety Scanner

Update the applications you installed. Run a complete scan

**If sharing a PC:**

- Confirm that your User Account is protected by an anti-virus application
- If you share a PC at your news office, discuss with your office administrator about adding anti-spyware and malware protection, if it isn't in place
- If you work from or blog at an IT café, you can bring your own protection (AVG Rescue Disk and Microsoft Safety Scanner run off a USB flash memory stick to check public PCs for malware)

**Update everything**

- Update the operating system. In Windows, enable Automatic Updates
- Enable automatic updating for your anti-virus and other anti-malware applications
- Visit the home pages of the programs you have installed to confirm you have the latest version or consider using an application like Secunia PSI to check for you
- Set a repeating reminder to check for new updates

**Turn on your firewall**

- Confirm that your PC's firewall is turned on
- If you want extra protection, install an additional, free firewall like Comodo. You can find a step-by-step guide to using Comodo at the Security in-a-Box website, run by Front Line Defenders and Tactical Technology Collective

**Day 2:** **Session 9: Handout 16**

## Dealing with computer viruses

**Viruses are a BIG problem:**
Tens of thousands of computer viruses have been recorded.
Very short "survival time" for an unprotected PC.

**Who makes viruses?**
Some hackers do it for money (e.g. Confickr).
Some are developed as a service for intelligence (e.g., Ghostnet).
Some ... just because (e.g. ILoveYou).

**Common myths:**
Only Windows gets viruses.
Smartphones don't get viruses.
An anti-virus will always clean an infected PC.

**Make two backups:**
One nearby, one off-site.
On a regular basis (e.g., weekly).

**Block unintended installations:**
In Windows, make sure UAC (User Account Control) is running.

**On a mobile device:**
Locate free anti-virus for your platform at the official app store for your device.
Don't install applications, wallpapers or ringtones you don't need.

**ALWAYS UPDATE!**

**When all else fails and you are infected:**
Copy essential files that were not included in your most recent back-up to some external media. Write down any license or purchase information related to paid applications (if you have any). Make sure you have your installation disk. Re-install the operating system and applications

Internews, 2014, Safer Journo: Digital Security Resources for Media Trainers:
https://www.internews.org/sites/default/files/resources/SaferJournoGuide_2014-03-21.pdf

Front Line Defender, Security in a Box: Tools and Tactics for Digital Security:
https://securityinabox.org/en

**Day 2:** **Session 10: Handout 17**

## How Vulnerable Are You? A Digital Security Quiz

Do you know how secure your digital identity is? Answer the questions below to discover how vulnerable you are to digital fraud and get some tips on how to protect your online presence.

**Do you know how strong your passwords are?**
**If you answered No: Oh dear!**
The temptation to create simple passwords is understandable. They are, however, extremely easy for hackers to crack. Passwords made up of a mixture of letters, numbers, and special characters are much safer. “123456 and password are still among the most popular passwords on the web”

**Do you use different passwords for different accounts?**
**If you answered No: Uh oh!**
Using the same password for numerous accounts makes it especially easy for hackers to gain access to all your personal details. If you struggle to remember multiple passwords, consider using a password manager.

**Do you use a pattern to lock your phone?**
**If you answered Yes: Not great…**
We should all have passwords on our mobile phones to protect our data and photos if it is lost or stolen, but screen-lock patterns may not be ideal. Greasy finger marks on your mobile screen can give away your pattern to the eagle eyed. Patterns are also easier for prying eyes to remember.

**Do you have a short screen-lock time on your mobile devices?**
**If you answered No: Oops!**
You may find the need to constantly unlock your phone a minor annoyance but it’s important to set a short screen-lock time. A few extra seconds could be all it takes for a thief to gain access to all your valuable personal information.

**Do you use 2-step verification on your important online accounts?**
**If you answered No: Not great…**
An additional layer of security may seem like a hindrance but 2-step verification, which usually involves a code being sent to your mobile via text, can prevent even the wiliest of hackers from accessing your most precious data.

**Have you checked recently what personal information is published on your social media accounts?**
**If you answered No: Not great…**
Your email, phone number, date of birth and home address are all very useful information to would-be identity thieves. Don't make their lives easier by offering them valuable information on a plate.

**Do you have remote wipe set up for your mobile devices?**
**If you answered No: Oh dear!**
If you haven’t set up remote wipe and your mobile gets into the wrong hands, it could land you in trouble. “31% of mobile phone users have had their phone stolen at least once”

**Do you check your phone bill for unrecognized charges?**
**If you answered No: Uh oh!**
A common new threat to mobiles is toll fraud. Once installed on your phone, malware sends messages from your phone to premium services.

**If you answered No: Not great…**
Most of us have antivirus software on our computers but how many of us have it on our mobile phones? Another common oversight is failing to keep it updated. Installing viruses is a common way for thieves to access our personal information.
“61% of people haven't installed antivirus on their phones”

**Do you keep the software on all your devices up to date?**
**If you answered No: Uh oh!**
Viruses and malware can exploit vulnerabilities in operating systems, software and apps to gain access to, and control, your devices.

**Do you always check the web address (URL) of sites before you enter personal information?**
**If you answered No: Uh oh!**
People looking to steal your personal information can copy the design of well-known websites down to even the finest details. The only thing they can’t directly copy is the website’s URL. Always double check you’re in the right place before you enter any private information.

**Do you know how to spot suspicious emails?**
**If you answered No: Oh dear!**
Emails, social media accounts and mobile phones are all easy targets for hackers. If they get access to your accounts they can send blanket messages to all your contacts, enticing them to download links to harmful software. You can easily be on the receiving end too. If it looks weird, don’t click it.

**Do you ever access banking or shopping sites over a public wi-fi connection?**
**If you answered Yes: Oops!**
Paying a bill while on the move may seem super convenient but any information sent over a public connection is fair game for hackers and potential thieves.

Source: http://simplisafe.com/resource/digital-security/

**Day 2:** **Session 10: Handout 18**

## Digital security risk assessment

**Identify the risks**

A. Are you covering a sensitive topic?

When are you going to be at greatest risk? When will your sources be at the greatest risk of targeted surveillance? While researching and investigating the story? After submitting it? After the story goes public?

How are you preparing yourself for possible increased surveillance? How are you helping your sources prepare?

B. The location of your assignment

What is known about government surveillance/censorship of the web and mobile communications in that area? What are the laws around free speech and the right to privacy, if any? What's been published about the persecution or rights of journalists, whistleblowers or activists because of their online activity?

C. Who are the adversaries likely to pose a threat to your digital security?

An adversary could be anyone trying to stop your work or who poses a threat as a result of it. What do you know about the people or organisations that could be potential digital adversaries? Think of them in two ways:

INTENTIONAL ADVERSARIES: These could be government, businesses, criminal organisations or individuals opposed to your work or to media exposure. Think of who may face some cost (legally, reputationally, professionally, etc.) as a result of your assignment.

UNINTENTIONAL ADVERSARIES: This can include random hackers targeting a service used by thousands of people including you. It could include someone hacking a wireless network you happen to be using at the time. It could also be the theft of your equipment.

D. What ways will these threats be manifested?

Unencrypted communication: In this situation, anyone monitoring your online or mobile traffic can access all the information you're sending and receiving.

**Metadata**: Many tools and services keep logs about who you're communicating with, the date and time and subject lines. Files you create, edit or share can also contain metadata about you and your work.

**Geo-tracking**: Your mobile phone is (and your computer could be) revealing your location so long as it's turned on. Removing the battery (if possible) and letting any reserve power die out is one way to ensure your phone powers down completely.

**Malicious software**: Your phone or computer may contain software you don't know about that's giving other parties access to it and anything stored on it.

Theft or confiscation of your equipment: When it's out of your sight, someone else could be accessing your device's contents, making copies of it, or loading malicious software to remotely access it later.

**Hacking attempts**: Network spoofing, man-in-the-middle attacks and other methods could be used to capture or redirect your internet activity and record what you're doing.

**Mass surveillance**: Many governments and companies monitor and record online activity. Some will trade this information among allies and partners.

**Targeted surveillance**: If you're working on a sensitive topic over a long enough time, you'll

**Your other online activity**: It may sound obvious, but using social networks whilst working on something discreet can be a bad idea. You may be unwittingly linking your work with your personal life, revealing more about yourself to potential adversaries than you should be.

**Your contact's digital trail**: All the above items refer to areas where you can reveal your own digital trail. Even if you're practising good digital security, your contacts may not be. Be careful how much personal information you share with them. Assess how you'll encourage them to be safer.

**The risks you may face**

Look at the possible digital risks from the perspective of what you're trying to protect. This should fall under two main headings:

**Identity**: This could be your own, or the identities of people you'll be on contact with. Is it important that the content you're working with isn't traceable to someone's real identity? Write down the various identities of all involved and what could happen if an adversary knew they were assisting you. If you think that this could put you under threat, then you should focus on behaviours, tactics or services that offer more anonymous methods to communicate.

**Data**: This could be text, images, video, spreadsheets or anything transmitted electronically. Could someone use this content to harm you or others, or stop your assignment before you're finished? Write down all the ways this data could be used. If you think that it could be used against you, you should prioritise strong encryption for all your data at risk.

https://rorypecktrust.org/resources/digital-security/digital-risk-assessment/outline-and-identify

**Day 2:** **Session 10: Handout 19**

## Web browsing security

**These can be identified:**
IP addresses
MAC addresses
Websites have identifiers, too.

Our browsers have “fingerprints”

**Applications and Settings can help. Start with your Web browser:**
Don’t store passwords in the browser.
Don’t save history or cookies.
Run CCleaner or BleachBit when done with session.
Install the add-ons called HTTPS Everywhere and NoScript (Firefox).

**Day 2:** **Session 10: Handout 20**

## Elements of a strong password

- **Make it long:**
  - You should try to create passwords that include 10 or more characters. Some people use passwords that contain more than one word, with or without spaces between them, which are often called passphrases.
- **Make it complex:**
  - Combination of characters. You should always include upper case letters, lower case letters, numbers and symbols, such as punctuation marks..
- **Make it practical:**
- **Don't make it personal**
- **Keep it secret:**
  - Do not share your password with anyone unless it is absolutely necessary. If you must share a password with a friend, family member or colleague, change it to a temporary password first, share that one, then change it back.
- **Make it unique:**
  - Avoid using the same password for more than one account.
- **Keep it fresh:**
  - Change your password on a regular basis, preferably at least once every three months.

### Remembering and recording secure passwords

You also have the option of recording your passwords using a tool like KeePass that was created specifically for this purpose.

It is important to use different types of characters when choosing a password. This can be done in various ways:

- Varying capitalisation, such as: '**My naME is Not MR. MarSter**'
- Alternating numbers and letters, such as: '**a11 w0Rk 4nD N0 p14Y**'
- Incorporating certain symbols, such as: '**c@t(heR1nthery3**'
- Using multiple languages, such as: '**Let Them Eat 1e gateaU au ch()colaT**'

Passwords can also take advantage of more traditional mnemonic devices, such as the use of acronyms. This allows long phrases to be turned into complex, seemingly-random words:

- 'To be or not to be? That is the question' becomes '**2Bon2B?TitQ**'
- 'We hold these truths to be self-evident: that all men are created equal' becomes '**WhtT2bs-e:taMac=**'
- 'Are you happy today?' becomes '**rU:-)2**d@y?'

The table below is based on Passfault's calculations. Passfault is one of a number of websites which allow you to test the strength of your passwords.

| Sample password | Time to crack an everyday computer | Time to crack with a very fast computer |
|---|---|---|
| Bananas | Less than 1 day | Less than 1 day |
| Bananalemonade | 2 days | Less than 1 day |
| BananaLemonade | 3 months, 14 days | Less than 1 day |
| B4n4n4L3m0n4d3 | 3 centuries, 4 decades | 1 month, 26 days |
| We Have No Bananas | 19151466 centuries | 3990 centuries |
| W3 H4v3 N0 | 20210213722742 centuries | 421046 |

Front Line Defender, Security in a Box: Tools and Tactics for Digital Security: https://securityinabox.org/en

**Day 2:** **Session 11: Handout 21**

## Encryption

Even if you normally protect your user account with a decent password, that doesn't truly protect your data if someone decides to swipe your device.

### iOS 8

If you use iOS 8 – Apple will now automatically encrypt all personal data. Applications such as Messages, Mail, Calendar, Contacts, Photos and Health data values use Data Protection by default and all installed app receive the protection automatically.

### OS X 7 (Lion)

Apple supports full-disc encryption with FireVault 2

To encrypt your drive after the fact, go to the Security & Privacy pane in System Preferences, and select the FileVault tab. Click Turn On FileVault and you'll be offered a pair of options: store the key used to unlock your disk somewhere yourself, or choose to store it in your iCloud account. A local recovery key keeps that key off of another company's servers, but leaves you without recourse if you lose it and you're locked out of your system. If you do store your key in iCloud (or even if you don't, for that matter), we strongly recommend enabling two-factor authentication for your Apple ID.

### Android

Android devices are yet to be encrypted by default - You can still encrypt any relatively modern version of Android pretty easily—these specific steps work for Nexus devices or anything running near-stock Android, but the process should be similar if your phone is using a skin.

Open the Settings app, go to Security, and then tap "encrypt phone" to get the process started. Your phone may ask you to plug it in or charge the battery to a specific level before it will give you the option to encrypt, mostly because interrupting this process at any point is likely to completely corrupt your data partition. You'll need to protect your phone with some kind of PIN or pattern or password if you haven't already, and as in OS X your phone will probably require it before the operating system will boot.

To confirm that your phone was encrypted, go to Settings and then Security and look for a small "Encrypted" badge under the "Encrypt phone" menu item. If your phone already says it's encrypted, you may have one of the new post-Lollipop phones that came with encryption enabled out of the box.

### Windows

Windows is a complex operating system that runs on what is by far the widest range of hardware of any operating system here, so encryption is more complicated. We'll be focusing on the built-in tools included in modern versions of Windows, but if they don't work for you there are lots and lots of other third-party drive encryption programs you can look into.

There's a very small chance that the Windows system you're using is already encrypted by default, at least if you have the right combination of hardware and software. That goes for users of Windows 8.1, and Windows 10 computers who sign into their systems with Microsoft or Active Directory accounts and whose hardware meets the following requirements:

- Support for the Secure Boot
- A Trusted Platform Module (TPM). The feature requires TPM 2.0, and most current

- Hardware and firmware support for Windows' InstantGo (formerly Connected Standby) feature. InstantGo allows a sleeping system to wake up periodically and refresh certain data, like e-mail messages or calendar events. Your smartphone already does the same sort of thing.
- InstantGo comes with its own set of hardware requirements, including a solid-state boot volume, NDIS 6.30 support for all network interfaces, and memory soldered to the motherboard. The system must also rely on passive cooling when in Connected Standby mode, even if it normally uses a fan.

This encryption method is also used by the handful of Windows RT systems that made it out the door.

The benefit of this method is that it's automated and it's available with every edition of Windows, including the Home editions. The bad news is that those hardware requirements are pretty stringent and there's no way to just add them to a computer you've already bought. And the Microsoft account requirement may rankle if you have no desire to use one.

Now head to the Control Panel and open up BitLocker Drive Encryption. From here, you can either use a USB key that will need to be plugged into your computer to unlock the drive every time it boots. Or you can come up with a special password, separate from your account password, that you type at boot to unlock the disk. Backup keys can be saved to an external drive, your Microsoft account, or to some other file on another local or network disk.

Arstechnica, 2015, Phone and Laptop encryption guide: Protect your stuff and yourself - http://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself/2/

**Day 2:** **Session 12: Handout 22**

# Tips for securing your mobile phone

Mobile phones are attractive targets for thieves and others. They contain call logs, contact lists, photos and other sensitive data. In addition to keeping your phone with you at all times, here are some common recommendations to get you started in making your mobile phone or smartphone more secure:

- **Lock it with a strong password**
- **Delete sensitive information**
- **Encrypt what you keep**
- **Use privacy software**

It is important to start with the understanding that mobile phones are inherently insecure:

1. Mobile phones are easily stolen or confiscated.
2. Mobile Phones are like Radios. This means that they broadcast their location to cell towers and, as a result, allow owners' locations to be tracked and targeted. In early 2014, the Ukraine authorities used this ability to send warning text messages to demonstrators at a political rally that turned violent.

1. More and more people want to monitor us. Monitoring software has now made it to ordinary consumers.
2. Your service provider can record "metadata":
    - Your location.
    - Calls (duration, to what number).
    - Text messages.
    - Use of Web services.
3. Handsets have unique identifiers called IMEI numbers (International Mobile Equipment Identity). This number does not change even if you change your SIM card (the part of the phone where your phone number is stored).

**Other ways to protect your location and movements:**

Alternative SIM cards and online phone accounts will make the tracing process more difficult, but there are costs and complications.

It is easier often to borrow a phone or pay a cabbie for the quick use of their mobile.

Phoning from a public phone or the office should not be overlooked. It might actually allay suspicion considering the legitimate cause to make enquiries and the channelling of the call through a switchboard.

Even better – try to meet face to face – and leave your phone in the office.

Internews, 2014, Safer Journo: Digital Security Resources for Media Trainers: https://www.internews.org/sites/default/files/resources/SaferJournoGuide_2014-03-21.pdf

Front Line Defender, Security in a Box: Tools and Tactics for Digital Security: https://securityinabox.org/en

**Day 2:** **Session 12: Handout 23**

## Mobile phone security

Mobile phones can be powerful tools for activists, but they can also be incredible liabilities if the government or security forces are actively working with telecoms to track you.
If you think you are being closely watched for high-profile activities, it's recommended that you don't use mobile phones to communicate. Conduct meetings face-to-face.
Ultimately, the risks you take are up to you: if you don't think you're being targeted as a high-profile activist or as part of a larger surveillance campaign and want to use your phone to communicate with fellow activists, record photos and video, or pass on information, you can use the following tactics:

- Create and use a **code word system** to communicate with fellow activists. Use "beeping" as a system for communication with fellow activists (calling once or twice and hanging up in order to let someone know you've arrived at a location, are safe, etc.)
- **Don't use the real names** for fellow activists in your address book; give them numbers or pseudonyms. This way if your phone or SIM card is taken by security forces, they don't have your entire network of fellow activists in hand.
- **Bring back-up SIM cards** with you to protests if you know they are being confiscated and it's important that you have a working cell phone with you at an event. If you have to get rid of a SIM card, try to physically destroy it.
- **If your phone can be locked with a password, use it**. This can also be your SIM card's PIN number: SIM cards comes with a default PIN number; if you can, change the default PIN number and enable PIN locking on your SIM. You'll then be required to enter a password (your PIN number) each time you use your phone.
- If you think a protest is going to meet with an increased crackdown by security forces, you may want to **put it in airplane mode while at an event**; you won't be able to send or receive calls, but you can still capture video and photographs and upload them to online sites later. This tactic is also useful if you think security forces are cracking down on everyone with a cell phone at an event. Later on the government can request call/SMS or data records for all individuals who were in a particular location at a particular time in order to perform mass arrests.
- **Turn off location tracking and geotagging** for various applications unless you are using this feature as part of a targeted project to geotag certain media at an event as part of an action. If you are using your cell phone to stream video live, turn off the GPS/geotagging option (Directions for Bambuser.)
- If you have a phone that runs on the Android Operating System, you can use a number of tools to **encrypt web browsing**, instant messaging, SMS, and voice calls via the tools created by the Guardian Project and Whispersys. When using your mobile device to browse the web, **use HTTPS** whenever possible.

http://wefightcensorship.org/article/practical-guide-protecting-your-identity-and-security-when-using-mobile-phoneshtml.html

Day 2: Session 13: Handout 24

## Digital and mobile security (INSI)

Although the internet, social media and mobile devices provide countless benefits for newsgathering, these tools also present significant security risks to journalists. It is essential that journalists know how to protect their digital data.

### Online security habits

- Never leave your computer with your e-mail open or any other personal information. Turn off your computer when you're done with the day's work - do not leave it connected to the internet overnight. Never allow someone to see your computer's screen over your shoulder and keep in mind that your office or workplace computer could be under surveillance.
- Change your passwords often (every two weeks in high risk environments) and be sure to use at least six characters, including * and #. Do not use names of family members, pets, or personal dates. Be sure to not repeat the same password across several accounts.
- Keep your passwords secret and don't write them down or list them in your mobile phone contacts.
- Use a computer which you do not connect to the internet to store valuable information. Do not allow anybody to plug a USB drive into this computer.
- Limit the information you post to Facebook or other social media sites, like photographs of family and friends, or other personal information. If you have a Twitter account, never post information that could be used to identify you.
- When surfing the web, enter the URL address in the browser and avoid clicking links that appear in pop-ups, e-mails or on social media. Always ensure that you use https:// to browse websites, and your email in particular.
- Use a different SIM card and phone for work, and block GPS locating options. Remember, text messages are not secure and are monitored in many countries.
- Never handle confidential information on computers in cybercafes, or when using public wi-fi in cafes, airports or other public spaces. Ensure that you sign out properly and don't leave your username in the browser.
- Do not respond to requests for personal information or open attachments in your e-mail from people you don't know.

### Technical aspects

- Use the latest anti-virus and anti-spyware software available.
- Enable a personal firewall to stop certain kinds of information from being transferred off your computer.
- When sending important information, use encryption software like the GNU Project so only the recipient can open it.
- To maintain anonymity on social media and the internet, download the free Tor program. Tor keeps others from knowing your physical location, your browser activity, reading your instant messages, or remotely accessing your Windows, Mac, Linux, Unix or Android powered device.
- When chatting on Gmail or Google Talk, select the option "off the record" to keep your conversation from being saved.

For more information on protecting yourself on the web, download Global Voices' step by step guide to publishing you work anonymously on WordPress blogs or visit Security in-a-box: Tools and tactics for your digital security by the Tactcal Technology Collective and Frontline Defenders.

**Mobile security**

Consider what potentially sensitive information is on your mobile device - it is not just the information on your mobile phone, but also your communications and contacts that are potentially compromised.

**General risks**

Your mobile device is operated by your mobile network operator - which can record certain types of messages you send, as well as other activities. When your phone is switched on, you can be traced (triangulated from the mobile phone towers nearby that record your phone's signal).

**Voice calls**

- Be aware that voice calls to contacts or sources can be eavesdropped - for instance, by an app installed without your knowledge, or by network personnel who could pass on recordings to someone outside the operator (either legally or illegally).
- Consider using basic phone, without apps, rather than a smartphone.
- If you choose to use a smartphone, use an encrypted application (like VOIP) instead of calling through a mobile network

**Photos, videos and MMS**

- You may face risks if you use your phone to capture and share multimedia content. The date, time and location of when and where you took a photo or video may be saved as part of the descriptive information, or EXIF data. If you upload photos or videos to a website, the descriptive information could be preserved, meaning that anyone could see where, when and with what phone you created the image.
- Remove identifying information from your mobile images
- You can also change certain account settings on your mobile device when uploading images

**SMS/text messaging**

- SMS messages are not encrypted, so anybody who intercepts the messages can read your SMS. Sent or received messages stored on a phone or SIM are vulnerable if the phone or SIM is lost or stolen.
- Set the SMS storage on your phone to very low or none
- Turn off the option to save outbound messages and delete messages regularly
- Consider using an encrypted messaging app instead of SMS

http://www.newssafety.org/safety/advice/digital-and-mobile-security/

**Handout 25:**

## GLOSSARY

**Avast!** – A freeware anti-virus tool.

**Bluetooth** – A physical wireless communications standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short wavelength radio transmissions.

**Circumvention** – The act of bypassing Internet filters to access blocked websites and other Internet services.

**Cookies -** These are small files added to your computer by various websites you visit. These files are what create a tailored experience when you're on a website and can also transmit information from one site to the next. Managing these is important if you're concerned about web services looking at these to analyse your online activity.

**Email client -** An email client is a program on your computer or mobile that downloads, displays and sends email.

**Encryption** – A way of using mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key.

**End-to-end encryption -** When both parties are using the same encryption, this is called end-to-end. It's by far the most secure because it encrypts both sides of the conversation.

**Firewall** – A tool that protects your computer from untrusted connections to or from local networks and the Internet.

**Free and open source software (FOSS)** – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it.

**Geo-tagging -** This is functionality that lets websites and programs see where you are. Mobiles use this to identify your location and provide service. Social sites use geo-tagging to make it easier to share your location with your friends. As a freelancer, there are likely many times you don't want this information being public, and you may want to disable this on social networks and take precautions about when and how you use your mobile.

**Hacker** – A malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely.

**HTTPS -** HTTP is the protocol for accessing web pages, and HTTPS is a more secure method for accessing them. It encrypts pages you load in your browser in an attempt stop third parties from being able to see what you're looking at on the web and stop hackers from being able to modify content as it appears in your browser. It also acts as a verification that the content was actually provided by the URL you accessed

**IMEI** – International Mobile Equipment Identity. This is a unique identification number for a mobile phone's handset and is separate from a customer's phone number, which is contained in the SIM card. The IMEI number is sometimes used by service providers to block devices that have been reported as stolen.

**IP Address -** Every device connected to the internet is assigned an Internet Protocol (IP) Address. This unique number is used to identify the location of a computer accessing a the user of an address provided they are keeping logs of this. When it comes to mobiles, this is certainly the case.

**ISP -** This is an abbreviation for ‘internet service provider.’

**Jailbreaking -** This often refers to removing limitations on what you can install on your smart phone. Sometimes called “rooting” it allows you to disable pre-installed security that keeps non-approved software from being added to your phone.

**Malware** – A general term for all malicious software, including viruses, spyware, Trojans, and other such threats.

**Metadata** – Information related to digital communications and media that may not be visible to the user, but may contain identifying details. For instance, phone calls may include the date and time of a call, a photograph may contain the location where a picture was taken or the model of camera used. A document may contain the name of the PC that created it.

**p2p -** Peer-to-peer (p2p) is a way to organise computer communications, creating ad-hoc networks with very little infrastructure. Each computer connected to a p2p session acts as both a server and client, allowing each user to privately share files and communicate.

**PGP -** This is short for “Pretty Good Privacy” and is a method for encrypting and decrypting anything from email messages to computer directories. It’s also often used for signing emails as a way of verifying the authenticity of the sender. Users send encrypted messages that require keys to access and view, keeping third parties or unintended recipients from being able to view the contents of a message.

**Proxy** – An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy.

**Service provider** – A company, either private or public, that provides mobile phone service or Internet service to customers.

**Single site browser (SSB)**
This is a program, often for mobiles, dedicated to accessing web pages from a single source. These keep your social activity in a box, away from the rest of your work.

**SIM card** – A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM cards can also store phone numbers and text messages.

**Spyware -** This is a specific type of program often installed on a device without the owner’s knowledge and collects information about the device’s usage, which is accessible to someone else.

**SSL -** It literally stands for “Secure Socket Layer,” but that’s not as descriptive as explaining what’s going on. SSL, and more recently TLS (Transport Layer Security), are methods that provide computer security over the internet using electronic cryptography. These methods are used in many websites, email services and instant messaging and voice-over-internet programs.

**Terminal -** All computers have this, but few people look at it. It’s where you can type raw commands into your computer to run tasks

**Tor** – The Onion Router is an anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you visit from anyone who may be monitoring your Internet connection, while also disguising your own location from those websites.

**Two-step verification** – A method of protecting a Web account that requires the user to provide two kinds of information when signing in, instead of just one password.

**VPN** – A virtual private network. VPNs use software on a PC or mobile device to create an encrypted connection with a server on the Internet. VPNs do not provide anonymity and users' online activity is visible to the VPN service provider

**VOIP -** Voice over Internet Protocol (VOIP) is software that enables users to call each other over the internet instead of using a telephone or mobile phone network.

Front Line Defender, Security in a Box: Tools and Tactics for Digital Security: https://securityinabox.org/en

Rory Peck Trust, A digital security glossary: https://rorypecktrust.org/resources/digital-security/the-basics/glossary

## Additional Handouts

**Safer social networking**
**General tips on using social networking platforms safely**

Mansour and Magda are human rights defenders from North Africa. They are organising a march, to take place in the middle of a large city. They want to use Facebook to publicise the event. They are worried that the authorities could be tipped off and that anyone who shows an interest could be traced. They plan to use Twitter during the march to give updates on the progress of the march. But what if the police could monitor the tweets, and deploy squads to intercept marchers? Mansour and Magda plan how to share photos and videos of the march without revealing people's identities, because they worry that participants could face persecution.

- **Always ask the questions:**
    - Who can access the information I am putting online?
    - Who controls and owns the information I put into a social networking site?
    - What information about me are my contacts passing on to other people?
    - Will my contacts mind if I share information about them with other people?
    - Do I trust everyone with whom I'm connected?
- Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine. See our guide on **How to create and maintain secure passwords** for more information.
- Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.
- Consider using **separate accounts/identities**, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine. See our guide **How to destroy sensitive information**.
- **Access social networking sites using https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site. See our guide **How to remain anonymous and bypass censorship on the internet**.
- Be careful about putting too much information into **your status updates** – even if you trust the people in your networks. It is easy for someone to copy your information.
- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts**! You

- Be cautious about how safe your content is on a social networking site. **Never rely on a social networking site as a primary host for your content** or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

Front Line Defender, Security in a Box: Tools and Tactics for Digital Security: https://securityinabox.org/en