The IFJ two-day Physical Safety & Digital Security Course

Aims:
While physical safety is usually given some consideration journalists in Pakistan, the nature of the environment for regional journalists remains extremely challenged. So too, digital security issues are leaving more and more journalists exposed and few have considered the risks to their digital assets and the potential consequences of losing control of them.

The two day course covers the following topics:

1. Risk assessment
2. Working safer in the field – professionally, physically and digitally
3. Making safety plans for journalism work – out in the field and online

The course also aims to equip participants with skills and knowledge to increase their personal safety and digital security in their journalism work on a day to day basis and also making threat assessments in preparing for their work.

Who is the course for?
The course is primarily designed for regional journalists who are out in the field or managing journalists in the field who have training capability to share and train others.

How the course works:
The course is designed to be conducted over two days with approximately 20 participants. These Trainers Notes are a step-by-step guide for how to conduct the course.

The Course Outline identifies each session, and refers the trainer to these Training Notes, Powerpoint and Handouts. The Course Outline should be reprinted for participants without the italicised directions to the trainer.

Why it is needed:
Risk assessment is a systematic process of taking stock of safety and security and physical and digital assets, identifying layers of risks and vulnerabilities, and coming up with a plan to address them.

This module will include some tools for assessing digital and physical threats and will encourage participants to consider:

- The value of their work and the information they depend on for their work (e.g., contacts).
- Personal habits that may put their work at risk.
- A practical level of safety and privacy in an office.

Each session is stand alone, so trainers can design a course of shorter duration if time is restricted.

Session 1: Trainer's Notes
Introductions and Icebreaker

Duration: 30 minutes

Aims:
To introduce participants to each other, find out a bit about each other's experience in the media, understand expectations and introduce the concepts of the course.

Materials:
Blank white paper
Clip board and clips
Marker pens
Post It Notes

Trainer's note:
Successful icebreakers are very useful to break down a formal atmosphere as well as people's normal shyness about meeting strangers. At this point the workshop trainer may introduce him or herself and briefly outline any administrative details such as:

- Workshop duration
- Breaks
- Toilets
- Lunch break

Session activity #1

Step 1:
Welcome the participants to the workshop introduce the trainers and other staff.

Step 2:
Express interest in knowing who the trainees are. State that they will now try a method of introduction, which will give them a chance to practice interviewing and presenting information.

Note to the Trainer: Ask participants to pair up, preferable with someone they don't know

Step 3:
Using the flipchart or multimedia, display the following points. Ask participants to take five minutes to interview each other and obtain the following information:

- Name
- Place of work/organisation
- Background, such as education, work experience etc
- Years of experience
- Beats
- Hobbies and interests
- A secret about your partners that no one knows or a threat they have had at work

Note to the trainer: Ask each participant to take ONE minute to introduce his/her partner, sharing the above information with the group. When introducing each other, the partners should come forward to the centre of the room. Also, ask the participants to add a prefix to the name of the partner that begins with the same letter as the name. This will make it easy for everyone to remember names while also help break the ice. For example: Bold Badar, Smart Sadar, Level-headed Lubna etc.

Ask each person to write their name and descriptor on the coloured cardboard in front of them if that is available. Then each person must introduce themselves (only about 30 seconds per introduction).

Step 4:
Ask the trainees what they enjoyed the most about the exercise. Emphasise that two way interaction communication is always more interesting than one way communication. We are there to gain energy and learn skills from one another.

Step 5:
The training also needs to establish some guidelines for acceptable behavior. Once they are agreed to, they can be posted in the room, and distributed to the participants to be included in their folders.

The guidelines should cover, but need not be limited to the following:
Training times: Agree on the start and end of sessions. This includes breaks and lunchtimes. Times can be flexible, and may change each day, but once agreed, need to be adhered to.
Presence: Participants need to be physically and mentally present for all sessions – not on the internet, checking email or posting to social networks during sessions. Mobile phones should be on silent, so they can get calls and messages and respond later.
Posting: Digital security trainings for media workers and activists generally are off the record. However, if the training does not pose a risk to the organizers, participants and trainers, the Chatham House Rule can be applied. The Chatham House Rule states: "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." When applied to social media, the Rule dictates that only what was said at an event, without identifying the speaker or another participant, can be tweeted or posted.
Security: The security of everyone involved, including that of participants, trainers, organizers and donors, is important. The participants need to agree that they will refrain from practices that will put fellow participants, organizers, trainers and donors at risk or exposure.
Downloads: Participants cannot monopolize the bandwidth of the class. This means turning off any torrent-related software and – unless it is the subject of a lesson – applications like Dropbox, Google Drive or OneDrive that generate background traffic, and closing social networking applications like Facebook, Twitter and Skype.
Respectful participation: Showing respect (for each other) and taking responsibility (for their own learning) are two non-negotiable rules before the training begins.

The set of guidelines agreed to by the participants and trainers will be a contract that participants and trainers will use before, during and after the training.

Step 6:
Explain to participants' inspiration and creativity will be encouraged throughout the workshop

Handout – Day 1: Session 1 - Program
Powerpoint - Slides: Title Slide

Session 2: Trainer's Notes
Experience and expectations

Duration: 30 minutes

Aims:
This session will explore participant expectations of the training and prioritise the most relevant issues.

Materials:
White board and markers
Powerpoint
Large Post-It notes

Trainers note:
The aim of this training is to help develop the practical skills to understand, avoid and respond to security risks. It's about learning the fundamental elements of personal safety and strategies for managing personal security in remote and potentially unstable contexts.

Session activity #1
Expectations
Step 1:
Explain that it is important for the group to share their expectations of the workshop with one another and with trainers.

Hand out one LARGE post-it notes to each participant and ask participants to write up an expectation for the workshop.

Participants should put the post-it notes on to a wall where they can remain for the duration of the training.

The agenda
Step 2:
Together, participants and trainers should determine which expectations will be met by the workshop, and which may be beyond the scope of the workshop. Post the latter on the 'Parking Lot' section of the wall and explain that these expectations will be 'parked' here and that they will be addressed if time permits.

Distribute the agenda/outline and give an overview of the workshop and about the work of the IFJ.

At the end of day 1 and at the end of day 2, the group can check to see if their expectations are going to be met. If an expectation falls outside of the scope of the workshop, discuss this openly and together think how it might fulfilled at a later date or in another workshop.

We'll cover four main areas:
- Understanding safety and security
- Strategies for identifying, preventing and responding to security threats, risks and incidents
- Security context assessment and analysis
  Making safety plans for journalism work – out in the field and online

Session 3: Trainer's Notes
Understanding Safety vs Security

Duration: 90 minutes

Aims:
To assist participants understand and prioritize some of the types of threats, vulnerabilities and risks involved in the profession of journalism..

It aims to cover some of the big issues early in the workshop. Trainers need to be careful that, as much as possible, with the use of questions, dialogue group and individual work, they allow participants to arrive at their own conclusions.

It is important participants understand the concepts to begin the task of preparing for assessing risks, vulnerabilities and threats on the job.

Materials:
White board and markers
Powerpoint

Trainers note:
This **snowball** exercise aims to build understanding of physical safety issues and begin to explore any experience in the areas of personal safety and digital security.

Explain:
Now we're going to look at some of the challenges and impediments to a safe and secure working environment for you. Can you tell me the difference between Safety from Security? Or are they the same?

Get a few responses from around the room.

Powerpoint: Safety is to protect against something - Security is a state being secure

Explain:
Safety measures protect us and our property from unintended consequences like a seatbelt in a car, workplace safety procedures and those sort of things.

Security protects from something intended – like direct attacks. These are both things we face as journalists and that we need to plan and prepare for.

What is a major thing that can leave us feeling vulnerable or unprotected as journalists – one that you experience too often in Pakistan?

Get a few responses around the room

Session activity # 1:

I'd like you to write down three threats that regional journalists in Pakistan are exposed to or that you have been personally exposed to directly or indirectly.

Give a minute or two to write down. Then go around group asking for their responses and writing them on the butcher's paper.

Examples of common threats from SAMSN digital hub:

- Hazardous Conditions
- Arrest/detainment
- Accidental death or injury
- Abduction/going missing
- Torture/Killing/Injury
- Threats to life/family/property/informants
- Intimidation
- Sexual assault
- Economic/political/social pressure
- Harassment
- Legal issues – defamation, blasphemy
- Censorship or media regulations
- Email intercepted or data stolen
- Computer hacking
- Control of movement
- Forced into exile
- Restrictions on access
- Theft
- Accidental Damage
- Media
- Extremists
- Natural Disasters
- Malicious Actions

Note to the trainer: Make sure they begin to think of safety and security not only in terms of physical safety but also in terms of digital safety. You may need to draw this out more if they are not used to thinking about security online.

Ask questions of the group when different concepts come up – how many people have also had a similar experience.

What about fears or worries on the job – these are important too?

*** Handout 1 - Threats**

Explain and illustrate on the white board:

Threat = the possibility of harm

Draw: a stick figure of a person with arrows all around

Threats can be dangers directed at an individual, group or an entity from an external source

Draw: A house and a bigger building representing a workplace

Threats can also be something that causes harm or control over you – draw a sad face on the person and impact on the way we do our jobs or manage our lives and well-being.

Session activity # 2 - Buzz Group Question

Explain:

What about our vulnerability as journalists. Is that the same as a threat? They sort of sound the same don't they?

With the person next to you I want you to come up with three things that make us exposed or vulnerable as journalists. These are things we do or perhaps don't do that may expose us to harm.

Give them two minutes to come up with items then afterwards ask each of the groups to say their answers. Every time an answer is repeated put a tick next to it to see which ones get the most hits.

Vulnerabilities:

- Human error and weakness
- Gap in understanding
- Poor local knowledge
- Gender issues
- Lack of security awareness
- Poor policies/procedure/protocol
- Professional skill/negligence
- Frequency of threats/predictability
- Your working environment
- Failure of equipment
- Experience
- Training
- Type of reporting we do
- Poor professional practices
- Ethics
- Sensationalism
- Biased reporting
- Work pressures for breaking news
- Perception of journalists or news organization

Draw out the discussion to fill in the gaps. Every time something is repeated give it a tick.

Explain:

Vulnerability = exposure to harm

Vulnerability represents the weaknesses or gaps in our personal protection. This is about things that we are in control of to some extent.

Powerpoint:

Vulnerabilities come from our:

- Knowledge – or lack of it
- Our experience in the field
- Where and how we operate – remember media workers are exposed to things that many others aren't!

Can we see a relationship between the two?

So what do all these threats and vulnerabilities that we've identified have to do with one another? What happens when you put them together?

Note to the trainer: Draw out answers to bring to the next discussion of risk. Eg, Vulnerabilities is in our control while threats is external

Write: RISK on the board – then draw arrows pointing to THREAT and VULNERABILITY.

Explain:
Considering our threats and vulnerabilities that we've discussed. What are some of the risks we take or expose ourselves to when we are working as journalists?

Now in the same pairs I want you to write up three risks that regional journalists in Pakistan are exposed to or that journalists choose to expose themselves to in the course of their jobs.

Note to the trainer: Give them five minutes to discuss and come up with the reasons they chose these. Write some of the answers on the board.

Risks:

- Reporting on sensitive or controversial issues – state and non-state actors
- Political climate
- Economic climate
- War zones - Battlefield hazards such as crossfire, landmines, cluster bombs, booby traps, and artillery and air strikes
- Going into crowd situations – demonstrations/rallies - sexual assault, theft, tear gas, violence
- Terrorist bombings/suicide attacks
- Travelling - traffic hazards (the leading cause of unnatural deaths worldwide)
- Religious situations/violence
- Border crossings and other interactions with potentially hostile or undisciplined armed groups
- Physical surveillance leading to abduction or identification of sources
- Electronic surveillance and interception of information or sources
- Trusting people - sources, drivers, fixers, witnesses, and others
- Exposure to crime
- Natural hazards, such as hurricanes and floods
- Getting sick - health risks ranging from water-borne diseases and contagious diseases and viruses

Explain:

Risk is a product of both threat and vulnerability. When you know that there is threat and you are vulnerable, and you do not ensure measures to protect yourself

So it's when we as journalists purposefully go into a dangerous situation. **Risk is intentional**

Session activity #3 - Identifying Risks – Role Play (60 minutes)

Step 1: Break the participants in four equal groups combining reporters, sub-editors, editors and producers, men and women. Assign each group with one of the following topics, discuss and answer the following questions.

Powerpoint: Use powerpoint slide to illustrate the areas they are working on.

Group One: Pressures or threats from outside the organisation (and the sources of the pressure) that can create safety issues

Group Two: Pressures or vulnerabilities from within the organisation (and their sources)

Group Three: Reporting practices or risks that can prove hazardous and what can be done about them

Group Four: Editorial practices that can jeopardise the safety of staff and what can be done about them

Step 2: Give the groups 30 minutes to work on their flip chart presentation. They must use visual aids and be presented by at least two members of the group. Groups can choose to focus on one issue in detail or outline up to five scenarios/issues that journalists have to deal with.

Step 3: Explain that 30 minutes will be spent on identifying risks and prioritizing them. They might also choose to present the issues as a role play. They will be given 10 minutes maximum to present their work and must use visual aids.

Step 4: Presentations by groups. Ask why and how they came to that conclusion together. Determine which are the top three issues from those we identified that are most relevant?

Step 5: Asks the class to prioritize the risks based on the likelihood of each threat and what level of impact the threat could have. For example, earthquakes are potentially devastating no matter where they occur (high impact), but they may be rare in some regions (low likelihood).

Note to trainer: The goal of this exercise is to provide participants with a team-based approach and some tools to begin a risk assessment for their workplace. The trainer guides the participants through the following steps:

Explain:

Essentially journalism is a dangerous profession – we know that. Quite often there are challenges to the stories we want to tell and from people who mightn't want that story told or who might want to derail your story or investigation.

What are our options when faced with risk? Write answers on board – leading to these conclusions:

- **Accept or understand it**
- **Avoid it**
- **Transfer it**
- **Reduce it – Standard Operating Procedures and training**
- **Ignore it**

Powerpoint: The frog in the boiling water scenario

Summarise:
When media personnel spend long period of time in areas of conflict, they can sometimes lose sense of security and risk, i.e. complacency, thinking it won't happen to them.

When personnel spend long periods of time in conflict zones they suffer from what is known as 'frog in the boiling pot syndrome'; the frog feels the water getting hotter but does not jump out of the water in time when the water reaches boiling point, by then it's too late and it dies.

Risk habitation is something journalists come up against frequently. Although they are aware that the risk is increasing and safety is deteriorating, they do not withdraw or reinforce security measures until an incident has happened. This is a dangerous and potentially fatal way of managing risk and personal safety.

This is something we need to overcome if we want to be safe and secure and continue our important work as journalists – both online and offline.

Session 4: Trainer's Notes
A risky profession – digging up trouble

Duration: 60 minutes

Aims:
To allow participants to explore risks of journalism that presents as well as some of the challenges, pressures and impediments to a safe profession. This will serve as an introduction to the need of protocols and guidelines on safety.

Materials:
White board and markers
Powerpoint

Trainers note:
This begins with a short role-play scenario for the group to respond to straight after the break.

Session #1 – Role play

Among two trainers, one plays an editor of a television station and another a reporter. The reporter will pick someone from the participants as a cameraman during the role play. (Note: if two trainers are not available, trainer can play the editor whereas one of the participants can play the reporter and other a cameraperson.)

The editor goes in front and reporter remains on the other side of the room. The editor is seemingly in the hurry and murmuring something. S/he then takes out his mobile and makes a call waiting anxiously for other side to pick up.

Reporter: Good morning, sir!
Editor: Where the hell are you? There is an unconfirmed report of a bomb blast in the center of the city. Do come over immediately.
Reporter (seemingly excited): Ok sir. Right there in a few minutes.

He then runs towards editor, asking one of the participants (cameraman) to take out camera, prepare the crew for live broadcast and be ready. And, says 'hi' to the editor.

Editor: Have you got your crew ready? Please leave. Go to the market and I want live broadcast in 5 minutes! I need close-ups and good stories.

Reporter: Yes, sir. I am on my way. You will see me on TV in 5 minutes.

Ask:

What do people think about this scenario? Sound familiar?

The aim is to encourage the group's responses on what is wrong with this picture.

Explain:

The world is an increasingly dangerous place for journalists. On average, more than 30 journalists are murdered every year, and the murderers go unpunished in nearly nine of 10 cases.

Hundreds of journalists each year are attacked, threatened, or harassed. Many are followed or have their phone calls and Internet communications intercepted. More than 150 are behind bars at any given time, some without being charged with a crime. The whereabouts of at least 35 journalists are unknown. Throughout the profession, journalists face emotional stress whenever they cover stories involving

In the Asia Pacific:

- 135 journalists died in the line of duty in 2014
- 39 of those died in the Asia Pacific region
- 35 of those were targeted killings

Pakistan was the deadliest country in the region with 19 killings in 2014

Balochistan has had the dubious distinction of being the world capital of enforced disappearances where more than 2,000 journalists, singers, teachers, lawyers have been forcibly abducted, tortured, killed and dumped since 2009 – in just five years, as many as in Chile during the reign of Augusto Pinochet!

Across the country, journalists in Pakistan are exposed to a variety of threats.

Powerpoint: Pakistan examples

But part of the problem is not just external forces as we've discussed.

Journalism is a risky profession. But are there things we can do to make it less risky?

Session activity #1
Individually, take a few minutes to come up with THREE things we can do as individuals to reduce risks that journalism presents.

Give one minute to do this.

Take one answer from each person. If an answer is already listed, they should come up with another. Write the answers on the board.

As Individuals in our journalism and daily life

- Minimising harm
- Good reporting
- Professionalism
- Moving away from harm
- Stay impartial
- Don't sensationalise
- Observe cultural sensitivities
- Ethics
- Sensible movements
- Protect identity
- Use of language
- Safety in field

- Sources
- Research
- Awareness of hostile zones
- Travel safely
- No story is worth losing your life

In our reporting this means:

Accuracy

1. Always ask people how to spell and pronounce their names
2. Saying things out of context

Objective

1. Don’t let opinions, biases or dislikes affect what you write
2. Report what you see, not what you think or assume may have happened

Impartiality

1. Don’t side with any groups or parties, politically or otherwise.
2. Stay independent: don’t give in to pressures such as bribery, favours and force to give a story a slant that is partial to one part or the other

Attribution

1. Try not to use anonymous sources – unless you have a very good reason.
2. If you can’t reveal a source tell the audience why

Balance

1. Talk to all people or groups party to a story, if possible. If not possible in the same story, being their opinion in a follow up story.
2. Bring diverse views about an event or development. Give audience views from people of diverse backgrounds and comments so they can judge for themselves

Clarity

1. Short sentences, one idea per sentence, easy language
2. Simplify concepts, give clear stances and positions and their possible implications for conflict or peace

Verification

1. Follow the three sources rule for verifying information
2. Ask for contacts of sources so you can call them if something is not clear or you need to ask to complete your story

Avoid Sensationalism

1. Do not exaggerate, do not present your opinion or someone’s else as fact
2. Do not appear to baser instincts but Inform to educate

***Handout 2 – How to reduce threats: Practical Steps**
Handout 3 – Essential guidelines for reporting and planning for safe and secure journalism

Session activity #2
Now in groups of two, I'd like you to discuss and present different ways that media organizations, news staff etc can work to reduce the risks journalists are exposed to.

Take 5 minutes to discuss. Go around the room taking something from each pair.

Media organisations
Trainings
Guidelines
Ethics
Safety protocols
Analysis of threats
Advocacy
Dialogue
Holding state agencies accountable
Bringing perpetrators to justice
Laws and mechanisms
Training
Risk assessments

Note to trainer: At beginning of exercise hand out the assessment worksheet

Explain:
As media personnel we are often compelled to expose, in the interest of the public, issues that some want to keep a secret and to report events or statements that are not tolerated by other parties. As media activists we must represent media personnel who are subjected to victimization and campaign for the people's right of information and expression. risky and hazardous profession when compared to other professions. In Pakistan, assassination, abduction, assault and intimidation of media personnel were continually reported. Today media personnel in Pakistan and at the international level are facing great danger and risk while doing their professional duty.

Journalism as a profession is always full of risks and dangers as journalists are not only seen as the crusaders of truth but also as villains by some elements in the society who seek to earn power, money or fame by undesirable means.

Some risks are very much a part of our jobs day to day – they simply can't be avoided.

But as journalists and members of the media we do have a responsibility to ourselves and others that we prepare and consider risks adequately.

Exercise #1: Starting a Safety Plan
(30 minutes total, with 10 minutes to present findings)

This exercise builds on the previous session. The trainer guides the participants through the following steps:

Note to the trainer: Divide participants into two teams and alerts the teams they will have 20 minutes to build on the work they just concluded.

Ask Team A to brainstorm some of the regular risks to staff in their organization when they are out in the field. Participants should list these on a single list of chart paper. Team A should take the following into consideration:

- Assuming they may not have all the answers, who are the key people they could ask for help and recommendations?

Ask Team B – the work environment - to create guidelines that their office (or any office) might follow when trying to conduct a comprehensive risk assessment and the safety plan (or action plan) to implement recommended solutions. Team B should take the following into consideration:

- Who are the key colleagues who would have to be involved in any comprehensive risk assessment? (Generic titles are fine: e.g., "managing editor.")
- Who will have to make key decisions in order for safety-related changes, such as new policies, to be implemented?
- What would a reasonable schedule look like?
- What tools could be used in the office to educate colleagues about changes in security policies when they are rolled out?

Ask teams to present their findings.

*** Handout 4 – Assessment workshop: Physical environment**

Concluding questions:

1. What sort of problems did you discover in your assessment?
2. Did you find any holes in your current safety and security arrangements?
3. What are the things that let journalists down in the field?
4. What sorts of things work best for journalists and media organisations to minimize the risks and dangers of the profession?
5. Are there some best practice models out there?
6. What about the impact of unprofessional or unethical practices – should they be part of a plan?

Session 5: Trainer's Notes
Safety in the Field: Practical Tips[1]

Duration: 165 minutes

Aims:

The aim of this session is to assist participants in applying theoretical and experiential knowledge and practices to devise practical strategies to improve safety and security.

Materials:
White board and markers
Powerpoint
Poster paper

Trainers note
This is one of the longest sessions during the two-day workshop, but since the participants are up and about, physically active and acting out practical tips and situational awareness, talking your way enacting role plays etc, it will not seem too long.

Lecture – 60 + 15 minutes
Activity – 90 minutes

Explain:

All of us use some strategies when we sense risk – talk ourselves out of danger, basic self-defence, avoidance and deterrence techniques. In this session, we will share these strategies with the group, and also systematize the best practices.

So what do we do when we are preparing to do a story?

Write down the answers on the whiteboard:

- Research
- Make contacts
- We talk to people
- Make travel arrangements
- Check our health
- Understand out threats, vulnerabilities and risks.

<u>Importantly we make a plan of action</u>

[1] Two-Day Training Manual for Pakistani Media on
Journalists' Security, Safety and Rights Monitoring, Produced by **Intermedia Pakistan** and **Civic Action Resources.** Authored by **Aurangzaib Khan**

Powerpoint: Preparing for an assignment
*** Handout 5 – The five basic principles of personal safety**

Standard operating procedure in the field – do's and don't of preparing for an assignment. This is a long presentation – the trainer should ensure that discussion, questions and responses are encouraged.

Use the PowerPoint to explain the various tips on handling and surviving threats to personal security. Don't lecture but reduce each PowerPoint to a 'mini lecture' – Keep the sessions small, interactive and invited feedback.
Note to trainer: This includes: **Safety in crowds or riots; Safety if shooting happens**

Plan in advance for crowds, riots or demonstrations

- Gather intelligence in advance about the likely crowd movements, flash points and safety routes.
- Investigate the scene in advance to select vantage points and alternative ways out.
- Knowing where people belonging to different ethnic or religious communities live may determine your travel routes in and out of the area.
- If you team is separating, pre-arrange contact points and times and try to have a direct means of communication
- Carry press ID, however if you think that may attract unwanted attention, conceal it.
- Carry a cell phone with an emergency number pre-loaded on the speed dial facility of your phone in case of emergencies
- If tear gas is a possibility try to position yourself upwind, and have a wet towel and water available to cover your face. If you cannot carry a gas mask, then citrus fruit such as a lime or lemon, squeezed over the affected area, will help to neutralise the effects of irritants
- You also need a means of extinguishing the flames if you are splashed with petrol from a Molotov cocktail

Improvise

- A magazine/newspaper can be put under a jumper as a make-shift anti-stab vest
- A hardened baseball hat can protect your head

In an environment where tear gas is likely to be used, eye protection should be considered. Swimming goggles or industrial eye protection should be sufficient

- If firearms are likely to be used, wear the same protective clothing as in war zones
- Carry first aid kits and know how to use them
- Wear loose natural fabric clothing: this will not burn as readily as synthetic material. Wear long sleeves, long trousers and a high collar. This will expose as little of your body as possible to the effects of irritants in tear gas
- Carry a small backpack with food, water and materials to last you for at least a day.

Positioning

- Think about how to position cameras and reporters to get an overall view of the scene. Higher up is better.
- There should be more than one way to leave a position.
- If you are filming, it can be a positive disadvantage to get into the crowd and be too close to the action. If you are a reporter who is not filming or taking picture you do not need to be in the crowd. So long as you have a clear line of sight and can catch the sounds.

During the event

- If you are part of a team, stay together or withdraw together.
- Better to withdraw too early rather than too late.
- If you are working as an individual, ensure that you have a good means of communication with someone who can get help if need be. Set up your phone so that 'last number redial' is to source of instant help.
- Try to keep a mental map of the main exit routes, prominent locations, security force locations and the nearest hospital facility, and keep checking this.
- If you fear footage, sims or digital memory sticks will be seized, carry dud items in your pocket and hide your used material as soon as you take it from the camera. In high-risk situations, team up with another photographers so that you can look out for each other. You may be rivals – but you are also colleagues
- If you are working alone, either as a reporter or a photographer, try to remain aware of when you are becoming the focus of a crowd, rather than just part of it. You may be at risk even if the crowd is not hostile. Do not be tempted into taking unreasonable risks.

After the event

- Debrief in the newsroom so lessons are learned for the next occasion.
- Protect your footage or material. What is the law in your country about the right of security forces to demand film and video material? What is the policy for your news organisation? If it is not possible to protect material within the country, is it possible to set up a system so that film of civil disturbance is archived outside the country?
- Remember that your ability to do your job safely is adversely affected if the police are given access to your material after demonstrations and civil unrest. You are put at serious risk, if those taking in a riot see you as part of the evidence gathering process.

Terrorist attacks

- Journalist face the same risks as all civilians from terrorist attacks and sometimes face extra risks when they become targets for bombs or shootings. Attending the scene of a killing or a bombing also carries risks.
- Grieving crowds may turn on media staff because they believe them to be callous, or to try to prevent whoever carried out the attack gaining publicity.
- The breaking news scenario is common in Pakistan – where one bomb may be set off to bring the emergency services to the scene, when a bigger bomb is detonated. All those who operate behind police cordons, whether police officers, paramedics or journalists, are at risk of being killed or injured by secondary bombs

Explain and summarise:

Review the key points:

- Always check your vulnerability
- Always use countermeasures
- Only when you understand the risk can you put an appropriate safety strategy together

Understand those who threaten you:

- Information warriors – national entities who target information.
- National intelligence collectors
- Terrorists – Political goals and secrecy
- Organized crime – mafia – cyber cartels
- Hackers – Major enabler and source of damage

Look at the venerability's in you daily news gathering:

- Human error and weakness
- Poor security awareness
- Common sense and common knowledge
- Policies and procedure
- Predictability

First of all, we have to know our threats, vulnerabilities and risks in order to prepare for them.

Session activity #1
This section is divided into risk assessment and safety plan exercises. We recommend the trainer set aside approximately 60 minutes for the first exercise and 30 minutes for the second.

Participants should be told at the outset that the purpose of the exercises is to help them start a practical risk assessment and action plan.

Ask participants to answer the dos and don’ts in relation to planning in advance, preparedness, positioning, improvising and survival tips etc.

Explain:

Always prepare a security assessment in advance of a potentially dangerous assignment.

The plan should identify contact people and the time and means of communication; describe all known hazards, including the history of problems in the reporting area; and outline contingency plans that address the perceived risks.

Diverse sources should be consulted, including journalists with experience in the location or topic, diplomatic advisories, reports on press freedom and human rights, and academic research.

Editors working with staffers or freelancers should have substantial input into the assessment, take the initiative in raising security questions, and receive a copy of the assessment. An independent journalist working without a relationship with a news organization must be especially rigorous in compiling a security assessment, consulting with peers, researching the risks, and arranging a contact network.

An example of a security assessment form is available for download here and for review in Appendix GReinforce the notion that keeping safe is not rocket science, but something all women have done at some point in their lives.

Encourage the group to work out each scenario in details or as role plays.

They should also use the security assessment handout as a guide.

1) *A Baloch journalist plans to travel to investigate a tribal dispute and potentially meet leaders. However, the journalists’ media organisation has had some criticism as being biased to one side.*

2) *A reporter has been working with a high-level, confidential source on a potentially dangerous story with national and possibly international security implications.*

3) *A reporter and photographer have been assigned to cover a sudden communal riot. Shootings in the region are not uncommon.*

4) *A female reporter has been specifically requested to undertake an interview with a member of a banned religious extremist group. It is not clear who she can take with her or the location of the interview.*

5) *A journalist is based in Peshawar and has been regularly covering news about the Taliban and the military action against the Taliban. He has interviewed senior Taliban leaders, triggering threats. After a major attack where Taliban reporting was banned, the journalist received warnings that if stories about them were not printed that action would be taken against him. How should the newsroom and journalist respond?*

6) *A local journalist has been approached by a high-profile international journalist and news crew to collaboration on a story, which involves travelling into conflict areas.*

Conclusion (15 minutes)

Trainers use this wrap-up session for informal questions to the group, reviewing the material that has been covered in the module. The following questions may help participants think about using what they have learned:

- Outside the work environment, do you think risk assessments have a practical use for you personally?

- Based on some of the topics we've discussed, is there anything that you know you do, or that you see in your office, that you would change immediately?

- What do you think will be the biggest challenge in trying to conduct a risk assessment and create a Safety Plan for yourself or the organization that you work with?

- What challenges do you foresee in implementing the safety plan?

- Some people have said that physical security, personal (data) security and network security are not separate things, and instead are dependent on one another. Would you agree?

*** Handouts 6 – Guidelines on safety and reports covering conflict**
Handout 7 – The Do's and Don'ts of staying out of harm's way
Handout 8 – Riots and Public Disorder
Handout 9 – IFJ safety guidelines for covering demonstrations and civil unrest
Handout 10 – Pre-assignment security assessment
Handout 11 – Says Who? Getting the right source in conflict reporting

Session 6: Trainer's Notes
Wrap up: recap expectations, agenda for tomorrow and close

Duration: 15 minutes

Aim:
The aim of this session is for participants to check where they are up to midway through the course.

Trainers note:
Use this session to recap what has been discussed, to check expectations (by referring to the notes pasted on the wall from Session 1), to explain the agenda for Day 2 and to wrap up the day's work.

Hand out pre-training questionaire for digital work

It is advised that you distribute the questionnaire in person to avoid using less secure methods.

1) Have the participants attended a 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) Will each participant have a smartphone?
7) What mobile phone brands/networks will the participants be using?
8) 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)

- **GIVE ALL PARTICIPANTS PRE WORKSHOP QUESTIONNAIRE FOR DAY 2**

Session 7: Trainer's Notes
Recap, check expectations, agenda for Day 2

Duration: 15 minutes

Aim:
The aim of this session is for participants to check where they are up to midway through the course and see which points they are picking up from the training.

Trainers note:

Use this session to recap what has been discussed, to check expectations (by referring to the notes pasted on the wall from Session 1), to explain the agenda for Day 2 and to wrap up the day's work.

Explain
Yesterday we had a mix of lectures, discussions, plenty of information sharing and group work. Today, building on that information, we are going to begin to think about safety and security in digital framework.

What were some of the things we talked about?

- Safety
- Security
- Insecurity
- Threats
- Vulnerability
- Risk
- Risk assessment
- Preparing for assignments

Risk assessment is a systematic process of taking stock of safety and security and physical and digital assets, identifying layers of risks and vulnerabilities, and coming up with a plan to address them.

Also that:

- Personal habits that may put their work at risk.
- A practical level of safety and privacy in an office.

Look to the program today – run through with participants.

Today is about looking at safety and security through the digital networks and devices that are part of our lives as journalists.

Session 7 – Handout 13 – Digital Security in a nutshell

Day 2: Session 8: Trainers Notes
Session 2 – Risk hunting

Duration: 60 minutes

Aim:
Learning the importance of backing up and protecting sensitive data and moving data safely. Can also touch upon encryption.

Materials:
Key or unlocked padlock
Laptop
Wires/cables
Power plugs
External drive
Sticky notes
Camera
Flash drive
Chart paper
Marker pens
A dedicated space that can serve as the "risky space"
Equipment and furniture that can be used in the "risky space"
But first, an exercise

Trainers note
This session is aimed to draw out the participants' knowledge and own experience and procedures in protecting their information. Encourage each person to contribute his or her "method." Ask them why they do what they do. The idea is to find out if they are taking these steps consciously.

Session activity #1 - Risk hunting for digital security – 20 minutes
This activity invites participants to explore a mock room or a "risky space" (a place that has been set aside in the training venue, or a separate room) to identify potential risks to equipment and data. In this activity, the space is prepared in advance and the trainer will keep a list of risks that have been intentionally left for participants to find.

Preparation
Prior to the start of the class, the trainer prepares the "risky space" with several risks left intentionally visible. It is not essential that furniture match the work spaces of participants, but the closer to an authentic work space, the more effective the activity is likely to be. These might include:

- Open windows.
- Door with key hanging from the lock.
- Laptop(s) without a locking cable on a desk.
- Wires or cables for devices that have been strewn on the floor where someone would need to step over them.
- Power plugs dangling loosely from a power strip near paper.
- Open desk drawers, with an external hard drive sticking out.
- Passwords written on a "sticky note" or other paper taped to a monitor or onto the surface of a desk.
- An open bag with a smartphone, camera or other valuable device exposed in it.
- A flash drive, left in a computer's USB socket.

- Computer left unattended with active Outlook, Gmail, Skype or other communication application open and visible.

Note for trainer: This is only a list of suggestions. This can be modified to fit the requirements of the participants and a risky habit practiced by participants that trainers want to draw attention to.

Explain:
The purpose of this session is to learn ways to identify risks to journalists and their electronic devices. Since journalists often have to be good investigators, this activity should be perfect for them!

The trainer then:

- Invites participants to walk up to or around the prepared space (or view a prepared photograph) for five minutes and take notes of risks they see.
- Organizes participants into groups of two or three and asks them to work together to share their findings with each other, and to then take five minutes to write their observations on a sheet of chart paper.
- Reminds participants that some “risks” will be obvious while others may not be obvious to all members in the group, and encourages discussion among participants to explore their views.
- When 10 minutes are left in the activity, asks teams to take turns presenting their “risks list” and to explain why individual items on the list might create a risk.
- Takes some time to point out any prepared risks that the group has not identified.

Discussion – 10 minutes
If time remains, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion. Encourage each person to speak up. It is likely that some have thought carefully about the issues; others may not have thought too much. This exercise will likely reveal some interesting practices, which makes for a rich discussion.

Questions:
Did anything in the exercise remind you of your office or your workspace?
Did it look similar? Very different? In what ways?
Why do you think risks like these are common in newsrooms or workspaces?
Do you think these risks only affect the person using the workspace or would other people in the office be affected by these risks? How?
What kinds of risks are present in public spaces? Do you see similar issues in IT cafes, for instance?

Do you know of examples where:
A journalist’s personal safety was compromised? Do you know what happened?
A journalist’s property or data was compromised? How did that happen?
What kinds of precautions do you take to protect your physical safety or the safety of your work?
Has anyone in this group conducted a risk assessment? If someone has, ask the person to explain how he or she went about in the exercise.

Powerpoint: Digital security in a nutshell

- Protecting devices and information from physical threats
- Secure passwords
- Destroying sensitive information
- Keeping online communication private
- Anonymity and bypassing controls on the Internet
- Protecting yourself and your data

Keeping data safe
Lecture – 15 minutes
This section includes recommended case studies, key messages and some materials to help get the point across. The following case studies examine digital safety risks that would not have been included in the opening activity (Risk Hunting) and are included to raise awareness about a broader set of challenges.

A. Sharing Files Can Put Lives at Risk
As journalists, we're constantly researching and sharing information. Even as we take steps to ensure the protection of our data, this case reminds us that it is just as important, internally within the media organization, to pay attention to who has access to that information. This is especially important to remember when reporters rely on the Cloud to share files.
Story:
A newsroom in Afghanistan was using Dropbox for file sharing. It was a collaborative news project and everyone working on each of the investigative stories had access to all the files and folders, including sensitive information. No one was keeping track of what was in the shared folder, who had access to specific files, and which of the many members could share or had shared which folders with other individuals not connected to the project.
During the course of investigating the story, one of the team members was asked to leave the news organization. As he left, he returned all the hardware (including laptop, camera, and flash drives) that he had in his possession. However, no one remembered to revoke his permission to the Dropbox folder.
The outgoing team member joined another news organization and published an article that used all the information that his former colleagues had so painstakingly collected. In the process, he also revealed the identity of a source that wished to remain anonymous and sensitive information that could be traced to the source.
The source had to be spirited out of the country.

B. Loose Lips and Open Devices
The first case study was an example of one sort of risk – losing control of data stored online. The one below looks at the loss of control of data in a physical environment.
Story:
An international media training organization was conducting a digital security training for Libyan activists and bloggers in Turkey. The organizers openly discussed where the training was being held, how many were to be involved, the names of participants, the equipment participants were carrying, and the equipment they were to be given upon arrival, etc.
When the training was completed and the participants were crossing the border to return home, they found that a new checkpoint had been established with the specific purpose of searching them. The reporters were carrying laptops, cameras and flash drives with encryption programs, and circumvention and anonymizing tools. Their vehicles were searched, their laptops confiscated, and three of the training participants were taken into custody by the border security forces.
One reporter was eventually set free, but the other two died in custody.

Discussion:
Ask participants what they think the journalists and their organizations could have done differently?

For Case Study A:
What could the Afghan news organization have done to ensure that they did not lose control of their information and to reduce the chances of damage? Could a policy of updating the list of people with access to shared folders have helped? What would you do in a similar situation?

For Case Study B:
In your opinion, where were the vulnerabilities? Should the people who were affected not have trusted their own colleagues? What would your suggestion be to the organization when running a similar training in the future?

Explain:
Journalists, especially those working in high-risk areas, handle sensitive information, including contact lists, research for articles, photographs and interviews.

Journalists keep much of this information stored on mobile devices, computers, and in the Cloud (Dropbox, etc.), it is important for them to learn about these two helpful habits:

- Backing up – protecting against loss.
- Encryption – protecting against misuse/abuse.
- Backups protect digital data from disappearing and encryption protects data from unauthorized access.

Summarise and question – 15 minutes

- What kinds of confidential information do journalists normally keep on computers? On their smartphones?
- Among those items, what would be the most important? What might happen if someone confiscated it?
- Has anyone among the participants lost sensitive information? How did that happen?
- Does anyone know of any cases related to this topic?
- What do people in the room do now to protect the information on their PCs and phones?
- Do participants back up their data?
- Do you use Dropbox or Cloud storage? Do you think there may be weaknesses?

Depending on the security environment, any file can be considered sensitive.

So that means we need to have control where information is shared and sent. Information should not be shared with anyone outside of a need-to-know basis, and controls should be in place to ensure that people receiving information do not share it repeatedly.

Reviewing access and changing passwords at regular intervals is a good idea.

In some places, just having programs like VPN can be cause for arrest like China, Iran, UAE and many Middle East and Gulf countries. In 2011, Pak Telecom Authority issued a notice banning encrypted VPNs. Sensitive information on devices can be a target and a reason for profiling and arrest.

Consider two sayings: “Even walls have ears” and “Loose lips sink ships.”

*** Session 8 Handout 14 – Planning for digital safety – assessing digital risk**

Session 9: Trainer’s Notes
Malware and basic protection

Duration: 30 minutes

Aims:
The aim of this session is for participants to understand the implications of equipment being infected with a virus or other malware. They will understand practical approaches to preventing infections on PCs and in detecting fake emails.

Trainers note:
This session will include providing participants with theAvast! Anti-virus application and learn to keep operating systems and software up to date.

Ask:
Has anyone heard of computer viruses?

What is the most common ways that our computers get infected by viruses?

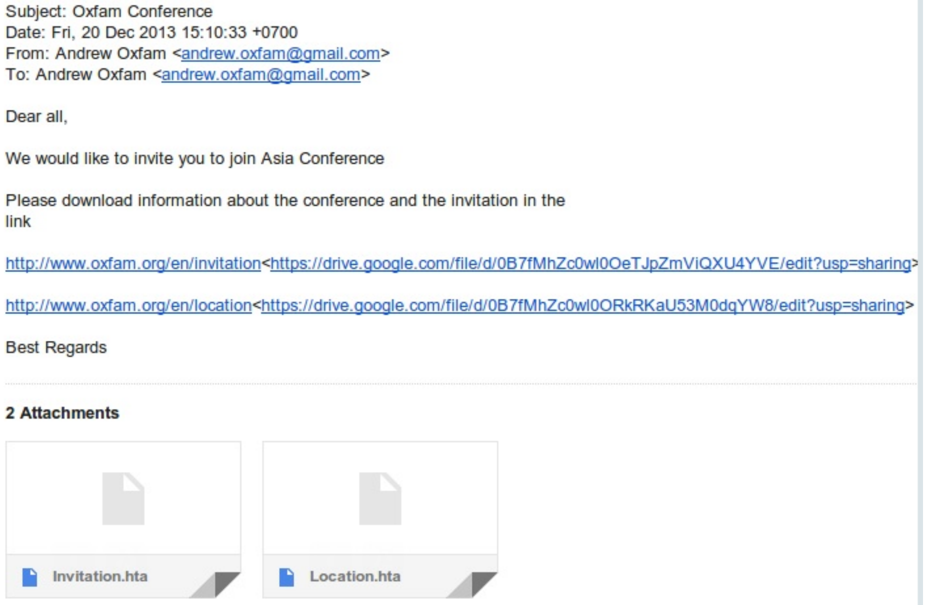
If participants offer the suggestion “email”, you can move directly onto the next step of the activity. If not explain.

Explain

When a PC becomes infected with a virus or other malware, journalists can lose control of their equipment, email accounts and other data essential to their work.

Nasty “worm” infections can actually spread out across an entire newsroom office network. The consequence for practically doing our jobs are significant: an infected computer can provide a hack access to sensitive communications, research and other files.

Powerpoint: Screen shot



Subject: Oxfam Conference
Date: Fri, 20 Dec 2013 15:10:33 +0700
From: Andrew Oxfam <andrew.oxfam@gmail.com>
To: Andrew Oxfam <andrew.oxfam@gmail.com>

Dear all,

We would like to invite you to join Asia Conference

Please download information about the conference and the invitation in the
link

http://www.oxfam.org/en/invitation<https://drive.google.com/file/d/0B7fMhZc0wl0OeTJpZmViQXU4YVE/edit?usp=sharing>

http://www.oxfam.org/en/location<https://drive.google.com/file/d/0B7fMhZc0wl0ORkRKaU53M0dqYW8/edit?usp=sharing>

Best Regards

2 Attachments

This is a copy of the email that was received by the Electronic Frontier Foundation, which shows the email that was received by that organization and a journalist at the Associated Press.

“Something doesn’t feel right about this email, but I don’t know what it is. Can you help me figure it out?”

Note to trainer: At this point, you should work your way down through the email to look for issues. Participants should be allowed to spot the problems first, but if they need some help, this list identifies some of the problems:

- What about the sentences in this email? The text in the email has several typos in it. For instance, there are no periods at the end of sentences and the sentences may seem awkward to native English speakers.
- How about the email address of the person who sent this email? It appears to be andrew.oxfam@gmail.com. Is there anything strange about that? Would Oxfam be more likely to have its own email, such as “oxfam.org”?
- This email asks the recipient to click on links to get some information about an invitation.
- Those links are the very long (blue) strings of letters and numbers near the bottom of the email. Does anything seem odd about them? The links appear to point to “www.oxfam.org” (notice that there is a difference between the website address and the email address of the person who sent this email). However, when the details of the links are examined, it’s possible to see that the links actually point to a different location, a shared file in someone’s Google Drive folder.

Ask:
What do you think might happen if you clicked on one of the links?

Answer:
The EFF determined that the links would cause the PC to install a virus.

This targeting is especially interesting because it demonstrates some understanding of what motivates activists. Just as journalists are tempted to open documents promising tales of scandal, and Syrian opposition supporters are tempted to open documents pertaining to abuses by the Assad regime, human rights activists are interested in invitations to conferences. For greater impact, the attacker should have included an offer to pay for flights and hotels!!

The trainer writes two words on the flipchart:
“Malware” – malicious software
“Phishing” – could draw a little fish with a mean face

Does anyone know what these two words mean?

“Malware” is what infects your PC. The word is a combination of “malicious” and “software,” and it refers to viruses of all kinds.

“Phishing” is the electronic equivalent of fraud. It is the tricking of a user into clicking a malicious link or exposing private information, such as a password, by presenting him or her with a fake email, instant message or website that appears genuine. This is a common way our computers can become infected.

Discussion – 15 minutes

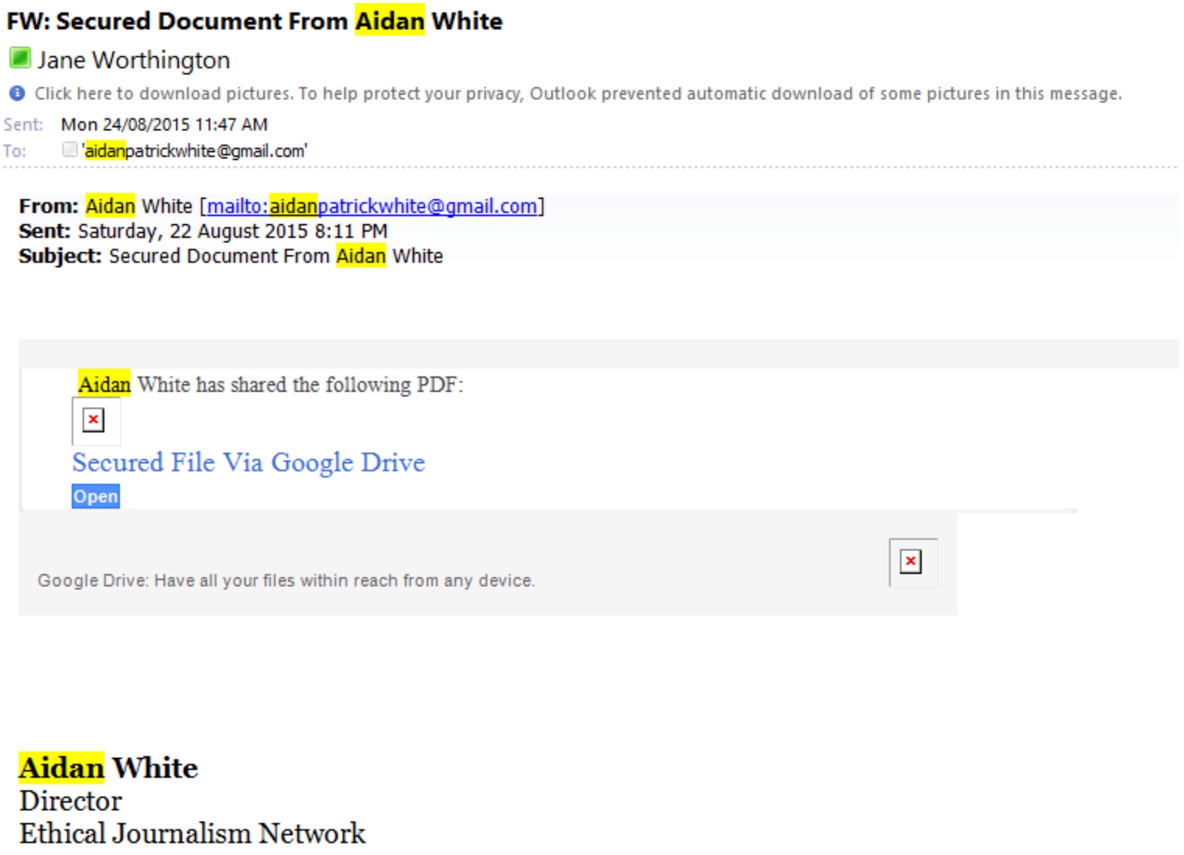
The following questions may help start the discussion.

Write the answers on the whiteboard or flipchart:

Ask: Has anyone in the group had their PC infected? What happened as a result?

How can our PCs get infected by a virus?
- From infected hardware (such as USB sticks).
- From unlicensed or cracked software (e.g., fake download sites).
- By clicking malicious links to download viruses (e.g., fake advertisements).
- By downloading them through malicious email attachments.
- Through social engineering attacks (i.e., impersonation).
- By downloading them through scams on social networking sites.

How do we get phished?
- Through e-mails that ask you to log in to your online banking account.
- Through e-mails that ask you to log in to your social network accounts (e.g., “tvvitter.
- com” instead of “twitter.com”).
- Through private messages on Twitter with shortened links that bring you to a fake login screen.
- Through Facebook wall posts and links that bring you to a fake login screen.



FW: Secured Document From Aidan White

Jane Worthington

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Sent: Mon 24/08/2015 11:47 AM
To: 'aidanpatrickwhite@gmail.com'

From: Aidan White [mailto:aidanpatrickwhite@gmail.com]
Sent: Saturday, 22 August 2015 8:11 PM
Subject: Secured Document From Aidan White

Aidan White has shared the following PDF:

Secured File Via Google Drive

Open

Google Drive: Have all your files within reach from any device.

Aidan White
Director
Ethical Journalism Network

What would you do if you received the email we looked at? (What would you tell a friend to do?)
We recommend:

- Deleting the email,
- If someone on staff or a friend is very advanced with technical issues, show it to them to see if they can determine where it came from. Was it from another country or did it come from your city, indicating you were the target?

Ask:
Are there any applications or browser add-ons that you know of that could help?

How many people in the group have an antivirus application installed on their PC? What antivirus applications are you using? How did you choose the antivirus application you are using?

How many people here regularly update their operating system? Can you tell us why you do that?

If you do not update your operating system, can you tell us why? (Are you concerned the piracy police will come visit you???)

Does anyone here have an antivirus application installed on their smartphone?

Notes for trainer: Using the examples above, trainers can help participants reflect on their own practices that may be putting their sources at risk.

Some questions that may help:
Do you click on all attachments that arrive in your Inbox?
If so, why? And has that led to your computer slowing down, crashing, losing data, etc.?
If not, why have you stopped before clicking?
Have you worried about malware infection? Why? Do you have information that would make you vulnerable to such infections?
If you have experience with malware, in what form has it arrived? As an attachment?

With the case study concluded, the trainer now directs participants to the handout to look at how we deal with viruses

- Four helpers
- Anti virus
- Anti-spyware
- Malware
- Firewalls

And remember!

- Update everything
- Protect your data

Explain:

Digital attacks on journalists continue to increase in both quantity and sophistication.

In China, foreign correspondents have seen their personal computers infected with surveillance software that was concealed as attachments to carefully fabricated emails. Authorities in countries from Ethiopia to Colombia have accessed reporters' telephone, email, and text conversations. Government players are not the only ones who use digital surveillance and sabotage; large criminal organizations increasingly exploit high-tech opportunities. Opportunistic or "patriotic" computer criminals also target journalists working with valuable or controversial data.

In the end, good information security is rarely about fending off sophisticated attacks and Hollywood-style hackers. It's usually about understanding what you have to protect and the motives and capabilities of those who might want to disrupt your work, then developing consistent habits based on those assessments.

Ultimately, journalists, editors and producers need to change their working habits.

This means having a working knowledge of basic encryption, surveillance techniques and IT hygiene so that whistleblowers and other sources can contact you with confidence – so it will not be straightforward to identify them or access journalists' records.

It also means that as journalists you must understand that you are automatically surveillance targets in everything you do.

Perhaps this means learning more skills.

But importantly you need to know when electronic communications should be abandoned altogether.

*** Session 9 Handout 15 – Basic protection checklist**

Session 9: Handout 16 – Dealing with computer viruses

Session 10: Trainer’s Notes
Understanding digital risk

Duration: 75 minutes

Aims:
The aim of this session is for participants to begin to think about safety and security through a digital framework and understanding what kind of digital trail they might have.

Materials:
Masking tape or colored chalk.***
Chart paper and markers.
Ensure that there is enough space for people to walk around freely (in some cases, a parking lot may be useful).

Trainers note:
Use this session to recap themes of safety and security and understanding the risks we take and the vulnerabilities we have in our digital sphere.

Preparation:
The trainer will need to create a list of statements (see below for suggestions) and these can be written on chart paper – prepared before the session.
Each will have a vertical line drawn below each, with one side marked “Completely Disagree” and the other side marked “Completely Agree.” If paper is not available, the questions can be read aloud.

Statement Suggestions (need to be short, straightforward and easily understood):
“The less information I share, the more secure I am.”
“My research for stories is not sensitive information.”
“If someone has agreed to be my source, his or her identity does not need to be protected.”
“It is likely that my computer or phone will be stolen or searched at some point.”
“My data is safe because my computer is password-protected.”

Explain:
Anyone working on sensitive projects or in conflict areas like journalists in regional Pakistan, are also coping with governments, security forces and groups who would probably prefer the information you might carry stays out of the public’s knowledge.

Session activity #1 - Spectrogram
Duration: 15 minutes
This activity poses statements related to the session topic and asks participants if they “agree,” “disagree” or are “in between.” The purpose is to chart the “spectrum” of opinions in the room and also help participants explore a range of views.

Steps to Creating a Spectrogram Exercise:

1. Ask participants to arrange themselves in a curved line (in the shape of the letter “C”). Colored chalk or masking tape on the floor are good for indoor spaces.
2. One end of the line represents “Completely Agree” and the other “Completely Disagree.”
3. Once participants understand this, read out a statement from the list of statements and ask the participants to place themselves somewhere along the “spectrogram” between “completely agree” and “completely disagree.”

4. *Note to trainer:* Some participants may need to think about and try out several spots before making a final choice.
5. Trainers then randomly select participants and ask why they have placed themselves in a given position. Have they experienced something similar, or did a friend or colleague?
6. After one or two participants respond, others in the room may wish to change their location – the participants are allowed to change their position.
7. Once everyone has found their spot, trainers place large "+" and "-" signs immediately below the statement and write down the apparent "score" based on where most people are standing.
8. Then trainers move to the next statement and repeat steps 3 through 6 for each statement.
9. At the end of the exercise, the trainer enlists the help of the participants to post the statements and the numbers on the wall.

Note to trainer: This exercise encourages trainers and participants to form opinions about topics, to recognize that one topic can be measured in different ways and that it is safe to change one's opinion!

Discussion – 15 minutes
With the activity completed, trainers may wish to have participants sit in a circle or semicircle, so they can address one another. The following questions may help start the discussion.

Someone can write some of the answers up on a flipchart.

Ask:

- What kinds of confidential information do journalists normally keep on computers?
- On their smartphones?
- Among those items, what would be the most important? What might happen if someone confiscated it?
- Has anyone among the participants lost sensitive information? How did that happen?
- Does anyone know of any cases related to this topic?
- What do people in the room do now to protect the information on their PCs and phones?

Powerpoint: Pakistan study

A study investigating digital security and journalists commissioned by the Internews and conducted by Bytes for All in 2012 showed a widespread lack of awareness of the security risks Pakistani journalists and bloggers face in their online activities.

B4A interviewed 37 journalists and 15 bloggers from across the country.

Three-quarters of those surveyed had personally experienced a security issue due to their work yet most of the respondents were unaware of the security risks they face in their online activities, such as email interceptions and data theft. Nor were respondents aware of the widely available strategies and tools that could protect them in the digital space.

While the vast majority of journalists use the internet in their work and take basic precautions such as installing anti-virus software and using strong passwords, they were largely unaware of secure tools such as IP blockers, which can be set up to block access to one's website from computers or networks that have certain internet protocol (IP) addresses, such as from particular government entities, and virtual private network (VPN) services, which encrypt and tunnel all data between the user's computer and another computer to minimize interception.

Journalists also chose email services, blogging and microblogging service based on ease of use and ability to customize rather than security.

An overwhelming 90.4% of respondents reported that they have never received any training in how to ensure their digital security.

As cyber-attacks become more commonplace and journalists regularly face issues such as having their emails intercepted or data stolen, having their websites attacked or hacked and having their identities exposed against their wishes, digital security training becomes even more critical.

Explain:

Digital security isn't just about you as journalists, who else does our digital security impact on? List can include:

- Colleagues
- Fixers
- Sources
- Yourself
- Your family
- Your friends/neighbours

Letting your contacts list or itinerary fall into the wrong hands can put you or a source at risk. Allowing your tools to be confiscated, destroyed, or interrupted can prevent you from pursuing a story at all.

It might can uncover your sources. It can expose colleagues who may be still out working in the field after you've gone home. It can also put family members in danger if you're working in a small community.

Powerpoint: Data falling into the wrong hands

Session activity #2 – How vulnerable are you?

Distribute each participant with a red card (for answering NO), a green card (for answering YES and if available, a Yellow card for answer I don't know. Ask for a volunteer to help you "score" the participants based on their responses.

Ask: Let's just do a quick run around the room to test people's knowledge on your digital vulnerability.

Remember: Saying "yes" is not always the right answer!

Do you know how strong your passwords are? Yes
Do you do different passwords for different accounts? Yes
Do you use a pattern to lock your phone? No
Do you have a short screen lock time on your mobile device? Yes
Do you use two-step verification on your important online accounts? Yes
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 OR using a mobile application installed and authorised in your phone to generate a code which then acts as second password, can prevent even the wiliest of hackers from accessing your most precious data.
Have you checked what personal information is on your social media accounts? Yes

Do you have a remote wipe set up for your mobile devices? Yes
If you haven't set up remote wipe and your mobile gets into the wrong hands, it could land you in trouble. Remote wipe is ability to erase all your personal data on your phone in the case of losing the phone or other events.
Do you check your phone bill for unrecognised charges? Yes
Do you have anti-virus software on all your devices? Yes
Do you keep your software up to date? Yes
Do you check web addresses on websites before you enter any personal information? Yes
Do you know how to spot suspicious emails? Yes
Do you ever access banking or shopping over public wifi? No

*** Session 10 – Handout 17 – How vulnerable are you?**
*** Session 10 – Handout 18 – Digital security risk assessment**

Session activity #3 - Creating strong passwords

Explain:
Strong password protection is by far the best general security you can give your data. But choosing an unbeatable password is harder than it sounds. Many people are shocked to discover that their ingenious choice is actually among the most popular passwords.

Some software allows attackers to rapidly test them against a password-protected device or service. Traditional password choices quickly succumb to these attacks.

Just like physical locks, they are useless if they can be easily picked. Likewise, if your password is "password" or if it's the same as your username or if it's 1234 or ABCD, it won't take much effort to unlock whatever you are protecting.

Recommendations:

- Make it long
- Make it complex (see the list of top 25 passwords)
- Don't make it personal (a passphrase taken from your favourite book is less secure if everybody knows which book is your favourite!)
- Don't use the same password for more than one account

There are a few tricks, however, that might help you create passwords that are easy to remember but extremely difficult to guess, even for a clever person using advanced 'password cracking' software. You also have the option of recording your passwords using a tool like KeePass that was created specifically for this purpose.

Powerpoint: to show ways to do a password

Using passphrases:

Consider using a passphrase instead of a password. One way to pick a passphrase is to think of an obscure quotation or saying which others are unlikely to associate with you.
* WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.
* Wow...doestcst = Wow, does that couch smell terrible.
* Ltime@go-inag~faaa! = Long time ago in a galaxy not far away at all.
* uTVM,TPw55 OR utvm,tpwstillsecure = Until this very moment, these passwords were still secure.

Random words:

Another approach is to pick a sequence of words truly at random. Seven or eight words picked this way will create a strong password, but the longer the password, the more likely it is to resist an automated attack. Mentally assembling these words into a humorous story or picture can make such passwords easy to remember.

Powerpoint: Correct horse battery staple

Varying fonts, numbers and symbols:
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**'

Mnemonic devices:
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:-)2d@y?**'

These are just a few examples to help you come up with your own method of encoding words and phrases to make them simultaneously complex and memorable.

IMPORTANT NOTE: A password of more than 8 characters with combination of alphabets (capital and small letters), numbers and special characters is good one.

A little effort to make the password more complex goes a very long way. Increasing the length of a password even just by a few characters, or by adding numbers or special characters, makes it much more difficult to crack. For demonstrative purposes, the table below shows how much longer it may take a hacker to break a list of progressively more complex passwords by trying different combinations of the password one after another.

Powerpoint:

Sample password	**Time to crack with 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 B4n4n45	**20210213722742 centuries**	**4210461192 centuries Passfault**

Explain:
Any of these methods can help you increase the complexity of an otherwise simple password.

Of course, the time it would take to crack any of the above passwords would vary widely depending on the nature of the attack, and the resources available to the attacker. Moreover, new methods to crack passwords are constantly being devised. All the same, the table does demonstrate that passwords become vastly more difficult to break by simply varying characters and using two words or, even better, a short phrase.

The table above is based on Passfault's calculations. Passfault is one of a number of websites which allow you to test the strength of your passwords. However, while such resources are good for demonstrating the relative efficiency of different types of passwords, you should avoid introducing your actual passwords into these sites.

If you use a lot of passwords, consider a password manager - like KeePass – software that will generate unique passwords and store them securely under a single passphrase. Make sure that single passphrase is a strong one.

Finally, understand that there is always one way that attackers can obtain your password: What is that?

- They can directly threaten you with physical harm.

If you fear this may be a possibility, consider ways in which you can hide the existence of the data or device you are password-protecting, rather than trust that you will never hand over the password.

One possibility is to maintain at least one account that contains largely benign information, whose password you can divulge quickly. Software like TrueCrypt offers this as a built-in feature. This approach relies on giving a convincing performance and the account's contents being convincing.

Session activity #4 – Create a password (5 minutes)
For fun, you can test various passwords in Microsoft's password checker to see how adding capital letters, numbers and special characters affects password strength. (As with any online password-checker, though, you should not use real passwords you intend to save!)

Explain:
Attackers can obtain your password by threatening you with harm. Consider maintaining an account that contains innocuous information, whose password you can divulge under duress.

Exercise #5: Setting Up Two-step Verification

If internet / laptops are available, participants can set up two-step verification for their Gmail or Facebook account otherwise show the video of setting it up and distribute handouts.

Video: https://www.youtube.com/watch?v=H1b6oumaMgU
Handout: Setting up Two-Step Verification

*** Session 10 Handout 19 – Web browsing security**
Session 10 Handout 20 – Elements of a strong password
https://securityinabox.org/en/guide/passwords

Session 11: Trainer's Notes
Protecting email

Duration: 60 minutes

Aims:
The aim of this session is understanding how our online communications are extremely exposed and learning to communicate more safely with sources and colleagues.

Importantly, participants should be encouraged to use two-step verification.

More advanced or digitally exposed participants should be encouraged to think about introducing end-to-end encryption.

Skills: How to use browse safely

Materials:
Markers
Blank postcards
Envelopes (two sizes)
Index cards, or premade cards for elements in the Web (see the list immediately below: "Sender," "Access Point," etc.)

Trainers note:
This module involves the distribution and demonstration of software that may not be permitted in some countries. It is strongly recommended that trainers research local laws that govern Internet access in the country in which they are training. In some countries including Pakistan for instance, the use of encryption (including VPNs) is not permitted.

Explain:
Journalists depend on email for a variety of sensitive tasks, but may not realize that sending an email is like sending an old-fashioned postcard: As the postcard gets passed around through the postal system, it can be read by anyone who holds it.

Session activity #1 – Postcards and candy thieves
The purpose of this activity is to illustrate the journey of most email and to introduce one method for protecting the contents of email. (Based on the "The Postcard Game," appearing on LevelUp.)

Preparation:
Step 1:
The trainer makes one card for him or herself but does not show this to the class. The card should have an illustration that indicates the trainer is a "villain," such as angry eyes or pointy horns.

Step 2:
Before the training begins, the trainer prepares two envelopes. Both need to be filled out with the following information, as if they were letters:
From: me-user@yahoo.com
To: you-user@gmail.com
Subject: Urgent and Important
Address: Email 101, Snowdonia

Trainer notes:
Ask participants to organize themselves into a U-shaped line (this works best with up to 10 participants, or subgroups that size).

Ask for two volunteers, one at each end of the "U," to represent two friends who are email pen pals or "friends."

Assign the remaining participants to play other parts of the Internet, with each person wearing or holding a card that identifies them as:

- Sender
- Wi-Fi access point
- Local ISP (ISP = Internet service provider)
- National ISP
- Mail Service: Yahoo!
- Mail Service: Gmail
- National ISP
- Local ISP
- Wi-Fi access point
- Recipient

Distribute the cards in such a way that the mail (Yahoo! and Gmail) services are at the "bottom" of the U and standing next to each other.
Ask one participant to pretend that he or she lives in a country with Internet restrictions and possible surveillance.

Conducting the Activity:

Notes to trainer: Compliment participants for their "dramatic representation" of the Internet and ask them to prepare themselves for their most difficult dramatic role: depicting a typical journey for an email message. Guide participants through the following steps:

1. The Sender is asked to write a message on an index card, which is then put in an envelope that was prepared before the event.

2. The Sender then passes the envelope to the person representing a Wi-Fi access point, who holds it while the trainer explains:
    - As a sender is sending an email, the first place that the bits of the email travel to is the Wi-Fi access point.
    - This access point is like the router in an office. If the office has a network administrator, that person is able to see the traffic on the network and can likely see the information on the outside of this envelope (To, From, Where, etc.).
    - Sometimes people talk about "secure connections" and something called "HTTPS." If we assume that is the case here and that the network administrator cannot read the contents of the email, then what can he or she see?

3. The Wi-Fi access person hands the card along to the Local ISP person. The trainer explains:
    - This is the company that you or your organization pays in order to get Internet access.
    - Everything you do on the Internet goes through the company's servers.
    - It has the ability to record activities and, like your network administrator, can see everything on the outside of the envelope.
    - If it is your email service provider, it can see the contents of the message, too.

4. The Local ISP person hands the card to the National ISP person. The trainer explains:
    - Very often, local ISPs are small companies that rent equipment and bandwidth from national providers. Those national providers might be private companies or they might be state institutions.
    - Just as with the Local ISP, everything you do on the Internet goes through the National ISP's hands. It has the ability to record activities and, like your network administrator, can see everything on the envelope.

5. The National ISP person hands the card to the Yahoo! person. The trainer explains:
    - The email here has arrived at Yahoo! because our Sender is a Yahoo! customer and the Sender's address is a Yahoo! address.
    - Staff at Yahoo! have the ability to read everything in the postcard including the message.

6. The trainer asks the Yahoo! person to open the envelope and remove the letter inside.

7. The Yahoo! person hands the letter to the Gmail person without an envelope. The trainer explains:
    - Because our Recipient has a Gmail account, Yahoo! has to hand over the email to Google. Sometimes, these connections between really big email providers aren't protected.

8. At this point, the trainer reveals his or her own card, showing a menacing cartoon face and steps between the Yahoo! and Gmail people. The trainer explains:
    - This is what some people are concerned may be happening in one of the NSA surveillance programs.

9. The Gmail person holds onto the letter. The trainer explains:
    - Just like at Yahoo!, the staff at Gmail have the ability to read everything in the postcard including the message. And the postcard will sit around until someone picks it up. That could be a long time!

Ask:
The trainer asks this question: How long do you think Yahoo! and Google will hold onto this postcard even after it is delivered?

Answer:
"FOREVER" - These companies have copies on many servers so that you don't lose your email. And they are required by law in some countries to maintain those copies for six months or longer!

The trainer now announces that the Recipient has logged on, and asks that the postcard be sent through the remaining people in the chain:

The Gmail person sticks the letter into the second envelope.

The trainer congratulates everyone for a job well done. Yahoo!

Session activity #2

The trainer now asks participants to remain in their spots and explains that they will now look at one method for protecting emails – including the content of emails.

Notes to trainer: Hold up a bag of candy and announce that the Sender wants to send it to the Recipient, but (with a smile) doesn't trust the other participants to deliver it.

Then produce a small box which can be closed or locked with a real or fake key and place the candy inside, closes the lid and locks the box.

Explain that you don't have the key to open the box.

Send the box down the line of "Internet" representatives, explaining that this is like sending an email that has been sealed with PGP.

When the box is received at the end, the last person produces a key and unlocks the box. Hopefully, they share the candy with the rest of the participants!

Note to trainer: In this exercise, trainers need to alert participants that there are additional steps, or "nodes," that we have skipped, including national gateways, in order to keep the illustration to a reasonable size.

Discussion – 15 minutes
With the activity completed, task the following questions. Trainers are welcome to add to this list or improvise as they see fit:

- Were people in the group aware of how many steps an email takes before it reaches its destination?
- Was it clear to the participants that sending an email to a person actually means sending it to an email service that holds onto it until the recipient logs on and asks to collect their email?
- In the Internet chain, who could access the name and subject of the email? Who could read the email itself?
- Who had a copy of the email?
- Was it clear to the participants that even if they have a protected connection to those services, the content of the email itself is not protected from the services?
- Who (in this country) do the participants think is likely to be interested in reporter's emails?
- What email service do they use? Why?
- Is anyone currently taking steps to protect their email? How?

Session Activity #3: Data on Computer (10 minutes)

Trainer's note: The aim of the session is to help participants understand that any browser by default saves data about use of Internet which can be retrieved by third person to understand your habits and help them to protect themselves from such data saves.

Ask: If you give me your laptop for a few minutes, what can I see except saved files such as documents, pictures, songs, program installed and videos?

If the participant says 'data about use of internet (or browsing history or browsing data)', explain the following. If they don't, ask them: Can I know what website you visited?

Explain: The web browsing history refers to the list of web pages a user has visited recently—and associated data such as page title and time of visit—which is recorded by web browser. Web browser such as Chrome, Internet Explorer or Firefox does this in order to provide the user with a Back button and/or a History list, to go back to pages they have visited previously.

In addition to the web browser software itself, third-party services can also record a user's web browsing history (completely or partially). The browser also keeps download history, cookies (), cached images and files (images and files of the internet which can be accessed offline) and may also have autofill form data (such as your phone numbers or credit card number) and even passwords.

Session activity #4 Delete your tracks on a public computer

Let's all quickly delete our current activity.

Ask:
Who knows how to do this?

Handout: Deleting Browsing History

Explain that best practices includes:

1. If you have checked your email, Facebook or Twitter account, always make sure you log out.
2. Delete all your browsing history including form autofills, cookies and passwords.
3. Close the browser.

Never store your passwords in the browser on a public computer. If you do this by accident, delete them from the browser's memory. Clearing browsing data is done differently in different browsers. A good way to avoid mistakes is to use the private browsing mode in Firefox or InCognito mode in Chrome.

Handout: No History Browsing

Discussion – 10 minutes
The following questions may help start the discussion:

Did the activity you just participated in show you anything you didn't know about the Internet?

In your work, what kinds/categories of information should be kept private when you use the Internet to visit websites?

Would we ever care about someone knowing what search terms we type into a search engine, what websites we visit, what we post in a blog or on a social network?

Do you know of examples here, in this country, where it was clear that the Internet was not private? (Trainers need to engage participants in a discussion about surveillance.)

Have you ever changed your online habits because of what you heard about online monitoring and surveillance?

Should we expect privacy when we surf the Web or should we assume that nothing is private, ever? (If participants think it is a mix, engage them in a discussion about what things they think should be private and what things are OK to be public.)

Lecture – surveillance
Duration: 15 minutes

Not only can intelligence agencies snoop through citizens' emails and phone data, but they now have the power to track and spy on individuals in areas previously thought to be safe. Surveillance technologies can be used as political tools; possibly to exploit or get rid of opponents, to make money or to further other forms of abuse.

Fin Fisher software enters a computer and resides in it, collecting files and real time transactions in the background, ostensibly for the operators of the software, such as law enforcement agencies.

Another type of dangerous surveillance software is called Fin Fly and is a simple USB stick. When inserted into a computer, it can collect information without the knowledge of the owner of that computer.

Yet another variant, Fin Intrusion, gives secret operatives access to Wifi networks in public places such as hotels, offices and homes, to collect data from any and all users using that wireless connection.

Many Pakistani journalists who have spent years looking over their shoulder for shadowy figures are only now beginning to worry about covering their digital tracks.

Write: write the following on board
These can be identified:
IP addresses
MAC addresses
More ...

Explain:
Like Caller ID on mobile phones, websites can see who is "calling" when a connection is made. One type of information they see is an IP address (Internet Protocol address) and this is what we illustrated in our Activity. Another kind of information is called a MAC address, which relates to the hardware on your PC and which we won't cover here ... and there are other things, as we will see.

Also, it's important to learn about keyloggers. Keyloggers records all the keys typed on the keyboard and can automatically emails to a preconfigured email address with screenshots and keys pressed.

Keyloggers are of two types:
1. Software that is installed as programs and many of them are found by malware scanners.
2. Hardware that is attached to the computer, typically between the wire of the keyboard and the CPU. Having a careful look at the back of the computer is the only way to find it out.

Live Demonstration:
To illustrate an IP address, the trainer visits whatismyipaddress.com
or
whatismyip.com.

The resulting Web pages will provide both the IP address and geographic location of the trainer's PC.

Websites have identifiers, too.

Every website has at least one IP address for the physical computer on which it resides. Some very popular websites are hosted on more than one computer (or server) and so they might have many IP addresses associated with their name. In any case, this is one way of monitoring which devices are contacting which websites. It is also one way authorities filter websites – they simply block an IP address.

Conclusion:
Wrap-up session for informal questions to the group.

1. Has anyone had any experience of being exposed or suffering as a result of their browsing history or data being saved on a computer?
2. Has anyone had an email intercepted or read by someone it wasn't meant for?
3. Has anyone experienced potential or real surveillance online? What form did it take? What did you do?
4. What things were most relevant to you out of this session?
5. Will you now change the way you use your computer or the Internet?

Session 12: Trainer's Notes
Mobile phone safety

Duration: 60 minutes

Aims:
The aim of this session is to illustrate the insecurity of mobile phone networks but that good habits can mitigate the risks.

Learning about risks and safety precautions to use when using mobile phones to avoid surveillance, protect data on phones and to avoid exposure of information in calls and text messages.

Importantly, this session is also about educating participants on when to leave the phone in the office.

Materials:

Explain:
A cell phone or smartphone might be a journalist's most valuable tool for work. But there are also risks to using our phones.

Powerpoint: Case study 1
Green party politician Malte Spitz sued to have German telecoms giant Deutsche Telekom hand over six months of his phone data that he then made available to media outlet ZEIT ONLINE. They combined this geolocation data with information relating to his life as a politician, such as Twitter feeds, blog entries and websites, all of which is all freely available on the internet.

This digital information provides a very interesting infographic of Malte Spitz' movements.

By pushing the play button, you will set off on a trip through Malte Spitz's life. In addition, a calendar at the bottom shows when he was in a particular location and can be used to jump to a specific time period. Each column corresponds to one day.

Discussion - 10 minutes
Were you surprised by what you saw in the Malte Spitz graphic?
Spitz' found out that his service provider kept all his data for at least two years. Do you know what the policies of your service provider are? How could you find out?
Were you surprised by how many things we keep on our phones?

Session activity #1 – What is on your phone? (15 mins)
Let's start by mapping our phones. What sorts of things do we keep on our phones.
List could include:

- Telephony information (eg call records, text messages, contacts)
- Email apps
- Social networking apps
- Media apps (video, sound and pictures)
- Browsing apps (Google, Firefox, Safari)

Note to trainer: Write categories along the top of a flipchart, or write them on stickies on the wall.

1. Divides the area (flip chart or wall) into two sections, “public”' and “private,” the difference being that “public” represents information we are happy to share publicly, and “private” being for a limited audience or ourselves only.

2. Distributes Post-it stickies to participants and gets them to write the types of information they store on their phone under each category. Gets them to categorize them in terms of whether they’re public or private and sticks the stickies on the chart paper/wall.

Once the map is created, asks participants to make observations about the type of information that is stored on the phone.

Looking at the information map, the trainer then asks participants to consider the information they don’t choose to put there, but which is automatically generated by the phone’s functioning, such as location data, call records, phone usage statistics, etc. If they are not on the map, the trainer adds them, perhaps in a different color to distinguish them.

Explain:
So as we see, our phones contain contact lists, photographs, email and instant messages, among other things. Their small size, relatively low cost and many uses make these devices invaluable for rights advocates who increasingly use them for communication and organisation.

But phones are also excellent tracking and monitoring devices.

These days, mobile devices with many more functions have become available. They may feature GPS, multimedia capacity (photo, video and audio recording and sometimes transmitting), data processing and access to the internet.

But the way the mobile networks operate, and their infrastructure, are fundamentally different from how the internet works. This creates additional security challenges, and risks for users' privacy and the security of their information and communications.

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.
3. More and more people want to monitor us. Monitoring software has now made it to ordinary consumers.
4. Your service provider can record “metadata”:
    - Your location.
    - Calls (duration, to what number).
    - Text messages.
    - Use of Web services.
5. 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).

Case study 2
Enforcement and revenue collection agencies can access call records without warrant so the case for erasing our data footprint is really strong. Revelations of governments engaging in mass surveillance programs further advance the case for upgrading our security and information-gathering protocols.

Ahmad Muaffq Zaidan, Al Jazeera's Islamabad bureau chief made a US government terrorist watch list. According to documents leaked by Edward Snowden, in 2012 the National Security Agency (NSA) indicated that it considered Zaidan was a member of Al Qaeda and the Muslim Brotherhood. Mr Zaidan strongly denied the claims that he was ever a member of either organization and was backed by his employers.

Metadata refers to location and data about communications, such as the callers, sender and recipient, location of communication devices and their unique identifiers, time and length of calls, and other data.

Just as we saw with Malte Spitze, metadata can be analysed by intelligence officers and software in order to detect specific patterns and to establish detailed profiles on particular individuals and/or groups.

Journalists are always told, whether in school or on the job, to go where the story is. To follow the trail.

Zaidan has travelled to and interviewed key figures in geopolitical hotspots, including Afghanistan and Pakistan. According to SKYNET, a problematically-named computer programme designed to analyse metadata, his movements were similar to that of couriers for high ranking Al Qaeda officials.

What this case highlights the grave dangers that the collection and interpretation of metadata hold in store for all of us.

So important to remember here is:

- Information sent from a mobile phone is vulnerable.
- Information stored on mobile phones is vulnerable.
- Phones are designed to give out information about their location.

So how can we be physically safer with our phones?
List answers on board:

- Be aware of your environment
- Who is standing nearby?
- Don't show it off
- Don't set it on the table at a restaurant. That invites theft.
- Decide what you need on the phone
- In case of theft or confiscation, the less you have on the phone, the better. It is recommended that participants make a habit of reviewing their phone's contents at least once a week.

And how can we be digitally safer?
List answers on board:

- Enable strong passwords.
- Many people use PIN codes (usually a 4-digit sequence you need to type in order to make a call). But Android, iPhone and Blackberry all support strong passwords, which is safer. You can enable these in the phone's Settings.
- Enable encryption.

- A PIN or password will prevent someone from making a call on your phone, but it may not protect data you keep on the phone – especially if you use an SD card or similar memory card with the phone.

Things to avoid:
Unnecessary applications like wallpapers and ringtones. These things are fun, but they can contain viruses.
Applications that ask for access to information they don't need.
An example might be an alarm clock application that wants access to your call logs.
Leaving Wi-Fi and Bluetooth on when not being used.
These not only waste your battery, they leave the phone open to potential attacks.

Session activity #3 – 20 minutes
Form four groups. Each team should spend five minutes drafting notes that they can use as a personal safety plan for:

- covering a controversial protest where government might be monitoring phones
- meeting an important source/contact
- communicating with the newsroom while travelling
- protecting sensitive photos or recordings obtained on your phone

This guideline may help them put their plan onto paper:
Phone calls. (How will they handle phone calls? Sample answer: "If someone from my office contacts me about something sensitive and I am standing on a crowded train, I may postpone the call until I reach my destination and can be more private.")
Text Messages.
Applications:
Apps to delete (e.g., "I will delete the 'Map my location' app.").
Apps to use with caution.
Apps to actively use.

After five minutes, the trainer asks participants to report back to the group on what they concluded as possible strategies

Summarise:
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. And phoning the source at work 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. You learn more, often discovering what is least expected. You make better judgments about whether or not you are being conned. You enable colour and context, and the content of discussion is generally more deniable. You could have always been talking about the football!

Session 12: Handout 22: Tips for securing your mobile phone
Session 12: Handout 23: Mobile phone security

Session 13: Trainer’s Notes
Risk assessment planning

Duration: 120 minutes

Aim: The aim of this session is enable the participants to assess the risks surrounding them and do the preparatory works for better safety and security.

Materials:
Markers
Chart papers

Trainers notes:

In this session, we recommend that trainers begin by explaining that the opening Activity and the subsequent Case Studies were intended to give a sense of the variety of challenges that journalists face. The remaining material in the lesson is intended to show how a risk assessment can help identify solutions to those challenges and jump-start the creation of a safety plan.

1. Risk assessment is a process that involves:
- 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.

Answering these questions not only provides a full picture of what hardware and information is at risk; it also helps a journalist prioritize what’s most important. No reporter wants to lose the work they’ve completed on their current article, for example, but they also cannot do their work without their contacts list!

Explain:
When conducting a risk assessment, it may help to think of your environment in layers:

Neighborhood:
Do your neighbors share your concerns about safety? Are there ways you can help one another to make your homes or offices more secure?

Outside:
Can anyone walk into the office? Can people reach your Internet or phone equipment from a window? Is your office Internet access point visible to people immediately outside?

From the front door.
From the front door of your home or office, can you see potential vulnerabilities? Are you sharing your project details or your ideas with visitors or people walking by the window? Could someone walking by have physical access to your network cables or to a PC?

At your desk.
Is your PC locked down with a cable or padlock, or can anyone walk off with it? Is it protected with a password? Have you taken steps to prevent dust, excessive heat or power surges from impacting the PC? Keeping your work area clean, making sure the PC is ventilated and employing an uninterruptible power supply (UPS) may help.

Your digital “space”:
Are your devices protected with passwords? Do you have any policies or guidelines that you follow when sharing materials or communicating with others?

Your “human network”.
Who do you know? Who do you trust? Who should have access and who shouldn’t?

Explain:
A safety plan identifies actions you can take to address the threats. 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?

It is assumed that journalists and their bosses won’t be able to address all threats at once. They should be prepared to schedule work on this project, just as they would on any other.

Things to keep in mind:
Be inclusive in your planning.
Your own risks may depend on other peoples’ habits. Having group discussions about safety policies is important.
Be judicious with permissions and access.
Does everyone in the office have access to all the data or devices in that office? Should they?

Start by creating a threat model, which must consider:

- What must be kept private? Specify all of the information that must be secret, including notes, documents, files, locations, and identities — and possibly even the fact that someone is working on a story.
- Who is the adversary and what do they want to know? It may be a single person, or an entire organization or state, or multiple entities. They may be very interested in certain types of information, e.g. identities, and uninterested in others. List each adversary and their interests.
- What can they do to find out? List every way they could try to find out what you want secret, including technical, legal, and social methods.
- What is the risk? Explain what happens if an adversary succeeds in breaking your security. What are the consequences, and to whom? Which of these is it absolutely necessary to avoid?

Once you have specified your threat model, you are ready to design your security plan. The threat model describes the risk, and the goal of the security plan is to reduce that risk as much as possible.

Your plan must specify appropriate software tools, plus how these tools must be used. Pay particular attention to necessary habits: specify who must do what, and in what way, to keep the system secure. Explain how you will educate your sources and collaborators in the proper use of your chosen tools, and how hard you think it will be to make sure everyone does exactly the right thing.

Also document the weaknesses of your plan. What can still go wrong? What are the critical assumptions that will cause failure if it turns out you have guessed wrong? What is going to be difficult or expensive about this plan?

Group Work: Preparing Comprehensive Security Plan (25 minutes)

Divide the participants into 3 groups. Each group shall take up a scenario and on chart paper prepare a security plan.

The scenarios you can choose from are:

a. You are a photojournalist with digital images you wants to get out of a tribal area. Limited internet access is available at a cafe. Some of the images may identify people who could be targeted by the government if their identity is revealed. In addition you would like to remain anonymous until the photographs are published, so that you can continue to work inside the country for a little longer, and leave without difficulty.
b. You are working on an investigative story about the Pakistan Army's operations in possible violation of law. You have sources inside the Army who would like to remain anonymous. You will meet this person twice to get some important document and communicate electronically. You will like to keep your source secret after the story is published.
c. You are reporting on corruption in local government, and talking secretly to two whistleblowers. If these sources are identified before the story comes out, at the very least you will lose your sources, but there might also be more serious repercussions — they could lose their jobs, or worse. This story involves a large volume of data and documents which must be analyzed.

These scenario descriptions are incomplete. Please feel free to expand them, making any reasonable assumptions about the environment or the story — though you must document your assumptions, and you can't assume that you have unrealistic resources or that your adversary is incompetent.

Presentation: 20 minutes

Session 13: Handout 24: Digital and mobile security

Session 14: Trainer's Notes
Wrap up, evaluation and close

Duration: 30 minutes

Aim

The aim of this session is for participants to check their expectations with the outcome of the course.

Trainers note

Use this session to recap what has been discussed, to check expectations (by referring to the notes pasted on the wall from Session 1).

Hand out evaluation forms and ensure they are filled while in the room.

Additional Handouts: 25 Glossary
Additional Handouts: 26 Safer social networking