**Travel**

**PREPARATION**

*BASIC*

**1. Strategic Questions**

* Ask some strategic questions before your trip
  + What is the objective of the trip? (ensure clear Terms of Reference)
  + What profile are you/your org org taking? High profile/ low profile? Why?
  + What is the threshold of acceptable risk your organisation is willing to take?
  + What about the risk to partners who you are meeting with?
  + What damage could this trip cause potential adversaries? How interested will potential adversaries be in this trip?
* Gather information about destination and partner organisations before deciding whether trip is currently safe and should be undertaken (context assessment)
* Complete a risk assessment
* Discuss trip with regional security focal point to confirm whether trip falls within threshold of acceptable risk
* Where possible, organise post-arrival context/ security briefings from partners

**2. Communications**

* Traveller to ensure they understand how to operate communications equipment.
* Buy “burner” sim-card before travel (WorldSim or Libara for example) and disposable phone. Make sure the SIM has funds on it. Often this is better than buying a local sim-card because that often requires registering the sim-card with your passport
* Check phone will function in the country travelled to
* Bring a satellite phone if necessary (e.g. if phone lines are poor or possibility of censorship during high tensions) – check they are legal in the country you are going to
* Programme essential numbers into your phone, but not sensitive numbers. Put sensitive numbers into the ‘notes’ section of your phone but need to disguise them effectively.
* Additionally, ensure you have key numbers – such as embassies - stored remotely or written elsewhere (coded where necessary).
* Note 112/911/999 Emergency number

**3. Key Documents**

* Ensure passport is valid for at least 6 months with appropriate visas and travel documents. When appropriate, photocopy passport and other documents and carry only the copy, keeping a second copy at home or office. Send a copy of your passport to your email address. Securely email other key information to yourself to ensure it is available if needed.
* Familiarise yourself with your organisation’s relevant security procedures.
* Check insurance is valid.
* Consider getting an identity card from your organisation. This could be a laminated, two-sided photo identification card with English or another UN standard language on one side and the local official language on the reverse.
* Ensure key information is shared with the right people before leaving – Human Resources? Your family? Your manager? The person responsible for managing the trip?

**4. Standard Operating Procedures**

* Discuss Standard Operating Procedures prior to departure
* Pre-agree an itinerary and communication schedule agreed with relevant colleague.
* You should carry your ‘constant companion’ on your person at all times. A constant companion includes some cash, your key documentation needed for evacuation, and a list of emergency names, addresses, phone numbers, and the names of reputable hotels along the route.
* Only minimal data should be brought with you – it should be backed up and, if appropriate, encrypted.
* If carrying sensitive information decide how to discreetly carry it in to the country. What’s your story? Prepare to answer questions at airports and elsewhere. (For advice on both of these, see the **Borders lesson**)
* If any sensitive meetings are to be held, or meetings with vulnerable human rights defenders, follow the advice laid out in the **Meeting lesson**.
* Have an alternative plan to exit the country. Do you have a ‘stand-by’ visa for a neighbouring country?
* If driving or being driven in a vehicle, follow the advice laid out in the **Vehicles lesson.**
* You should understand tools, systems and techniques for good personal security management, counter-surveillance, safe use of email etc. (training might be necessary) This may include making yourself familiar with the advice in the **Arrest** and **Kidnapping lessons**.
* Inform authorities and embassies of the trip.
* Will a curfew be respected? Will solo movement be allowed?

**5. Medical**

* You should carry a medical emergency card. Pre-check the best hospital in the area you will be visiting and also have a medical plan B.
* Make sure you obtain correct health advice, vaccinations and malaria prophylaxis.
* Check that any essential medicines required are carried.
* Inform your organisation and your travel companions if you have heath complaints that could become serious (e.g. Asthma, diabetes etc.) and how they should respond in an emergency.

**6. Equipment**

* Ensure adequate cash or other payment tools for the trip.
* Take key items of equipment
  + Travel lock
  + Computer lock
  + Door wedge
  + Tamper-proof scotch tape
  + Mobile Wi-Fi device
  + Solar charger
  + Cheap notebook from which you can rip out pages unnoticed
  + Mosquito net/ repellent etc.
* Ensure any digital equipment you take with you – phone, computer – is wiped ‘clean’. For more advice on how to do this see the **Protecting Files lesson**.

**7. “Need to Know”**

* Discuss who needs to have advance knowledge of your trip – minimising the number of people who know about your presence is a good way to increase your security. This needs to be balanced with operational practicalities and the ability to complete the assignment.
* Limit who has information (need to know) on
  + Trip plans
  + Movements, patterns, lifestyle
  + Travel modes, itineraries, professional arrangements
  + Security arrangements & procedures
  + Your organisation’s duties, associates and colleagues
* For more advice, see the **Managing Information lesson**.

**8. What now?**

**Swipe right for this lesson’s checklist.**

*RELATED LESSONS/TOOLS*

* *Borders lesson*
* *Meeting lesson*
* *Vehicles lesson*
* *Arrest lesson*
* *Kidnapping lesson*
* *Protecting Files lesson*
* *Managing Information lesson*

*FURTHER READING*

* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)
* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)
* [*2012 CPJ - Journalist Security Guide*](https://cpj.org/reports/2012/04/journalist-security-guide.php)

***Preparation Basic Checklist***

* ***Ensure clear objectives for trip***
* ***Gather information from partners***
* ***Conduct a risk assessment***
* ***Establish threshold of acceptable risk***
* ***Bring working burner phone and sim with funds***
* ***Bring satellite phone if appropriate***
* ***Program essential numbers into phone, but keep sensitive ones coded***
* ***Keep key numbers on paper also***
* ***Note emergency number***
* ***Ensure valid passport, visa, insurance etc. and securely email to yourself and trusted colleague***
* ***Consider bringing an org identity card***
* ***Understand Standard Operating Procedures and Security policy***
* ***Agree itinerary and comms schedule***
* ***Carry your ‘constant companion’***
* ***Bring minimal data***
* ***Plan what to say at borders***
* ***Plan sensitive meetings in advance***
* ***Plan for an emergency exit***
* ***Follow advice for driving in vehicles***
* ***Understand advice for situations of arrest or kidnapping***
* ***Inform appropriate authorities/embassies***
* ***Ensure you have all vaccine/ medicines required***
* ***Inform org of potentially serious medical concerns***
* ***Carry medical emergency card and check area’s hospitals***
* ***Bring adequate cash***
* ***Bring locks, door wedge, security tape, mosquito net etc.***
* ***Ensure digital equipment is wiped ‘clean’***
* ***Keep advance knowledge of your trip need to know***

**BORDERS**

*BASIC*

**1. Before You Leave**

If travelling, you should *first* follow the advice outlined in the **Preparation lesson**.

This lesson focuses specifically on how to cross borders if travelling for sensitive work or with sensitive information. In establishing the potential risk and risk mitigation measures for crossing borders, it is important to establish a few basics about the reasons for, and possible sensitivities of, your trip. It is vital to be aware of the nature of the information you will be carrying into and out of the country, and how you will carry it.

Sensitive or revealing information you may carry could include:

* Data on people at risk/HRDs you are meeting
* Travel plans
* Passwords/ access codes
* Censored/ banned information
* Organisation sensitive information
* Personal information
* Embarrassing/ incriminating information
* Legal - encryption or data not allowed for export
* Receipts
* Reports

This information may be stored in/on notebooks, publications, laptops, phones, USBs, CDs, or SD cards.

Remember:

* Only minimal data should be brought with you
* Bring a “clean” laptop and phone if possible
* Carry sensitive information and electronic equipment in hand luggage, as at least you know If it has been tampered with
* Small, encrypted USB sticks or Micro SD cards can be useful for security and being able to hide sensitive data if necessary. See the **Protecting Files lesson** for advice on how to encrypt files.
* Bring a cheap notebook in which you can rip out the pages unnoticed
* Tamper proof Scotch tape can be useful for enhancing the security of your equipment, hotel safe, laptop ports etc.
* Check pockets, wallet, bags everything before travel
* Prepare your story (More in next section)

**2. When Entering Country**

* Agree in advance with colleagues what you will say. Discuss any red lines you will not cross (e.g. giving information about high risk activists who you intend on meeting)
* In some environments, it is best not to attract attention by travelling in a group, so sit separately and approach immigration separately. (Although bare in mind that authorities often know if big organisations are coming to the country anyway.)
* Say/do nothing sensitive on plane – many human rights defenders have been arrested because they were overheard speaking about their activities.
* Provide only minimal information to immigration about activities.
* It may not be within the remit of your organisation to lie but neither should you volunteer information unnecessarily.
* Be prepared to be questioned about your activities in other countries/visas marked in your passport.
* Be polite but firm with authorities.
* Decide in advance if you are going to put the actual hotel and location where you are staying on the visa entry form. (Consider risk vs. benefit)
* Do not get separated from your belongings, especially electronic items. If they are taken away from you, you should assume that they have been compromised.
* Keep phones off until well outside airport. Airports are common areas for tracking and viruses.
* Keep Wi-Fi off if not vital – do not connect to airport Wi-Fi.
* Agree in advance with colleagues a location in the building where you will meet after immigration and a set time to turn on mobile phones if you have not met at this point and need to communicate.

**4. When In Country**

* If using a paper notebook, try to minimise any potential data loss by making up short codes that only you understand. For example, if you are meeting a high-risk activist, give them a different name and refer to them as that in your notes. Don’t mix sensitive information with easily identifiable information.
* Don’t forget about receipts, tickets, bills etc. They can link sensitive activists to your work if not carefully protected.
* Keep sensitive information in another place (e.g. interview notes in a notebook but sensitive names and locations securely emailed to yourself.)
* Type up or take photos of your most sensitive written notes as soon as possible and securely email them to yourself and/or keep them on an encrypted drive. (See the **Protecting Files lesson** for advice on how to encrypt files.)
* Avoid taking paper reports or other information from the organisations and people that you work with - if your bags are searched they will link you. Instead, ask them to give or email you digital copies if possible.
* Dispose of sensitive paper waste immediately. Avoid doing this in locations like hotel rooms or offices where it might be taken by cleaners or security staff. If necessary, soak paper in water to ensure it is unreadable.
* Minimise the amount of security related information you give to people that you meet. At meetings and during other interactions, avoid giving details of future operational and travel plans.
* Travel by different routes at different times if possible in high-risk areas.
* Avoid walking alone/at night if possible.
* Advise hotel staff not to provide information on your activities; although be aware they could be monitoring you, too.
* Try to memorize emergency phone numbers.
* Agree a simple discreet signal with any colleagues that can alert them to nearby danger. It should be something easy to do but not something that would happen accidentally.
* Always wear seatbelts!

**5. When Exiting Country**

* You should assume that you might be stopped and searched. Assume that anything you have written will be copied or read and prepare accordingly.
* Make sure all sensitive notes are typed up/ photographed and then encrypted. (See the **Protecting Files lesson** for advice on how to encrypt files.)
* To prepare for the long-term confiscation of your equipment at an exit port, you should backup key files remotely, such as to your secure email.
* Before departure, make sure to remove any sensitive paper waste from your room and dispose of it safely elsewhere. If necessary, soak paper in water to ensure it is unreadable.
* At a suitable time, speak with your colleagues (if travelling with them) about what you will say if stopped and questioned when leaving the country. It might be the case that certain parts of the trip (such as meeting with a high-risk activist) you do not want to mention to the authorities. Any plan of what you agree to say should be:
  + *Simple;*
  + E*asily repeatable*;
  + V*erifiable.*
* When leaving the country, the same principles as entering apply. Keep electronics and sensitive material on you at all times. If necessary, hide a small USB or micro SD card somewhere it is harder to find.

**6. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Preparation lesson*
* *Protecting Files lesson*
* *Backing Up lesson*

*FURTHER READING*

* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)
* [*Protection International: New Protection Manual for Human Rights Defenders (3rd Ed.)*](http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/)

***Borders Basic Checklist***

***Before you go***

* ***Identify all sensitive information and where its carried***
* ***Bring minimal data***
* ***Bring clean equipment***
* ***Carry equipment in hand luggage***
* ***Bring small encrypted storage devices***
* ***Bring notebook that you can rip pages from***
* ***Bring tamper proof scotch tape***
* ***Check bag/wallets before travelling***

***Entering country***

* ***Agree what you’ll say/ not say***
* ***Say nothing sensitive on plane***
* ***Consider approaching immigration separately***
* ***Provide only minimal info on activities***
* ***Be prepared to be questioned on passport***
* ***Be polite but firm***
* ***Decide on which accommodation to report***
* ***If separated from equipment, assume it’s compromised***
* ***Keep phones and Wi-Fi off till out of airport***
* ***Agree meeting point with colleagues***

***In country***

* ***Use codes for sensitive written info***
* ***Be careful with receipts that could link you to activists***
* ***Avoid collecting paper reports***
* ***Keep sensitive info separately/ encrypted***
* ***Dispose of sensitive notes ASAP***
* ***Minimize sensitive info you share***
* ***Change up your travel routes***
* ***Avoid walking alone at night***
* ***Ask hotel staff not to share info about you***
* ***Memorize emergency phone numbers***
* ***Agree emergency signal with colleagues***
* ***Always wear seatbelts!***

***Exiting country***

* ***Prepare for stop and search***
* ***Make sure all sensitive notes are remote/encrypted***
* ***Back up all equipment remotely***
* ***Check room/pockets/wallet for sensitive papers***
* ***Soak sensitive waste papers in water***
* ***Agree what to say at border with colleagues***
* ***Keep equipment with you at all times***

**VEHICLES**

*BASIC*

**1. Driving Guidelines**

Vehicle-related accidents are the major cause of injuries and fatalities among aid personnel. Driving in unfamiliar and sometimes difficult conditions can increase the likelihood of an accident. Other dangers include ambush, robbery and aggressive behaviour of armed personnel at checkpoints. If available and practical, all staff members should receive driver safety training.

The most important piece of security advice an aid worker or human rights defender can be given is ALWAYS WEAR A SEATBELT.

Driving Guidelines

* Park in well-lit, heavily populated areas. Close all windows and lock doors before leaving the vehicle. Have keys ready in hand when returning to vehicle. Check the back seat before entering.
* Immediately lock doors upon entry. Open windows no more than 5 cm and only those windows near occupied seats.
* Do not speed or drive too fast for conditions. Observe local driving laws and regulations.
* Avoid night driving or driving alone where possible.
* Avoid letting the fuel tank fall below half full.
* Keep a spare vehicle key in the office.
* Never voluntarily carry unauthorized passengers, especially soldiers. However, if threatened, provide the transportation. In the event of an attempted carjacking, you should not risk your life to save a vehicle.

**2. Journey Guidelines**

* In insecure locations, all staff should be met on first arrival, and on subsequent arrivals if necessary. Those meeting staff should carry identification.
* Vary the time and route of any regular journeys you make. If criminals can predict where you will be and when, it is easier for them to target you.
* In remote areas or where threats may be present along the route, select primary and alternate routes.
* Avoid areas with criminal activity or known threats. If possible avoid “choke points” such as narrow alleys.
* When possible, consult with other agencies and organizations to monitor route conditions and change routes as necessary.
* Notify others of travel times, destination, and steps they should take if you are late.
* Mark official vehicles appropriately for the area.
* Consider posting a decal on your door or window indicating guns are not permitted in the vehicle.
* Avoid transporting sensitive documents or equipment in areas prone to banditry. Arrange proper permits for transporting items that could be interpreted as useful to combatants or terrorists.
* Know how to perform basic vehicle maintenance (changing a flat tire, checking and adding fluids, etc.)

**3. Considerations**

Important issues to take into consideration when planning a journey include:

* Recent incidents on the route. \*Check the **Dashboard** for information about your area\*
* Weather
* Length of journey – time of departure/ arrival?
* Should you travel in convoy with another vehicle?
* Communications schedule
* Checkpoints en route – what is the process for passing through? (See **Checkpoints lesson** for advice on this)
* Other dangerous points en route (does the route pass through an area controlled by military, a warlord or local leader). Has negotiation been carried out and permissions obtained and understood prior to leaving? Crossings of conflict lines and through insecure areas should be rigorously checked before travelling.
* Safe ‘waypoints’ en route
* Refuelling stops
* Sustenance/ food stops
* What is your plan in the event of a car accident or breakdown?

**4. Journey Preparation**

**Drivers should:**

* Be given a clear briefing about safe driving procedures before departure
* Consider the length of journey – do you need more than one driver?
* Factor in prayer or sustenance stops if necessary
* Consider the driver’s ethnicity if going into dangerous areas

**Considerations in choosing type of vehicle should include:**

* Urban or rural trip? State of the roads? 4x4 necessary?
* Desirability of vehicle for car-jacking
* High profile or low profile

**Road worthiness checks carried out before using a vehicle should include:**

* Tyres
* Seatbelts
* Fuel
* Brakes
* Oil level
* Steering
* Loading

**5. What to Have**

The following items (location dependant) should be kept in the vehicle at all times.

**Equipment:**

* Communication equipment and key telephone numbers
* Additional fuel & oil
* Water
* Maps
* GPS
* Spare parts for car
* Spare wheel (x2) and jack
* Basic tools
* Fluorescent warning triangle
* Tow rope
* First aid kit
* Torch

**Documents:**

* Permission to travel, if required
* Visas
* Car documents
* Driver’s licence & insurance
* Personal ID
* Organisational ID if possible
* Medical vaccination certificates

**General items:**

* Food
* Water
* Cold/ hot weather clothing
* Blankets/ shade structure

**6. Accidents**

Traffic accidents can be minimized by implementing defensive driver training and other precautions, but they can never be avoided entirely. When an accident is mishandled, it can quickly change from an unfortunate occurrence into a security risk. In extreme situations, it can trigger violence or threats of retribution.

The following procedures are useful when involved in an accident.

* Quickly discern the attitudes and actions of people around the accident site to ensure that you are not at risk by staying.
* Do not leave the site unless your safety is jeopardized and then only to drive to the nearest police or military post.
* Make site safe and visible to other traffic.
* Provide care and assistance as appropriate.
* As appropriate, contact local authorities immediately and cooperate as required.
* Contact the your office as soon as practical.
* If feasible, take pictures of the scene and record the names and contact information of witnesses, responding authorities, and those involved.
* When approaching an accident involving other vehicles consider safety and security, taking care not to become involved in a second accident while responding.

Vehicle accidents are the main cause of injury and fatality among NGO staff. Avoiding excessive speed, following applicable traffic laws, and wearing seat belts minimize the chances of injury.

Offices should implement a transportation policy that ensures vehicles are maintained in a state of operational readiness; journeys are planned; and vehicle users are prepared to respond to a range of possible incidents. An accident report format should be placed in the logbook of each vehicle.

**7. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Checkpoints lesson*
* *Preparation lesson*

*FURTHER READING*

* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)
* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)

***Vehicle Basic Checklist***

* ***WEAR A SEATBELT***
* ***Park in well lit, busy places***
* ***Close windows and lock doors on leaving***
* ***Have keys in hand returning to vehicle***
* ***Lock doors on entry***
* ***Open windows no more than 5cm***
* ***Do not speed***
* ***Observe local driving regulations***
* ***Avoid driving at night/alone***
* ***Avoid letting fuel tank fall below half full***
* ***Keep spare key in office***
* ***Don’t carry unauthorized passengers unless threatened***
* ***Meet incoming staff on arrival***
* ***Vary regular journey times/routes***
* ***Have alternate routes planned***
* ***Avoid criminal areas and chokepoints***
* ***Consult with other agencies***
* ***Notify team of travel plans***
* ***Mark vehicles appropriately***
* ***Avoid transporting sensitive items through volatile areas***

***Journey considerations***

* ***Recent incidents***
* ***Weather***
* ***Length***
* ***Communications***
* ***Checkpoints/ other dangerous points***
* ***Safe ‘waypoints’***
* ***Refuelling stops***
* ***Food stops***
* ***Plan in case of breakdown***
* ***Appropriate vehicle type***
* ***Ethnicity of driver if dangerous area***

***Checks***

* ***Tyres***
* ***Seatbelts***
* ***Fuel***
* ***Brakes***
* ***Oil***
* ***Steering***
* ***Loading***

***Keep in vehicle***

* ***Communication equipment and key telephone numbers***
* ***Additional fuel & oil***
* ***Water***
* ***Maps***
* ***GPS***
* ***Spare parts for car***
* ***Spare wheel (x2) and jack***
* ***Basic tools***
* ***Fluorescent warning triangle***
* ***Tow rope***
* ***First aid kit***
* ***Torch***
* ***Permission to travel, if required***
* ***Visas***
* ***Car documents***
* ***Driver’s licence & insurance***
* ***Personal ID***
* ***Organisational ID if possible***
* ***Medical vaccination certificates***
* ***Food***
* ***Water***
* ***Cold/ hot weather clothing***
* ***Blankets/ shade structure***

***In case of accident***

* ***Ascertain risk of staying***
* ***Do not leave site unless at risk***
* ***If at risk, drive to nearest police/military post***
* ***Make site safe and visible to others***
* ***Provide assistance as appropriate***
* ***Contact and cooperate with authorities***
* ***Contact your office***
* ***Take pictures of scene and details of those involved***
* ***Complete accident report form in log book if applicable***

**CHECKPOINTS**

*BASIC*

**1. Assessment**

Many checkpoints have a legitimate purpose, for example to prevent weapons from entering an area. Some checkpoints, however, are designed to harass people or as a cover for ambush, theft or violence. It is important to recognise the difference between a legal, sanctioned checkpoint and one designed for the gain of the checkpoint personnel.

You first need to rapidly assess the nature of the checkpoint.

* Where it is located?
* Who is manning it?
* What does their mood appear to be?
* Are there any signs of trouble?

Checkpoints at crossroads, bridges, mountain passes and town entrances and exits are to be expected, and are likely to have been set up for the general monitoring of all passers-by. Checkpoints in the middle of a forest or on a mountain road away from habitation may exist for a more ominous purpose. Checkpoints manned by regular army and police forces may be less problematic than ones manned by irregulars.

If you suspect that there is a risk of violence or other serious problems, turn round and drive steadily away, if it is safe to do so.

Before approaching or leaving a checkpoint, inform base by radio. Do so in a discreet way, far enough from the checkpoint to avoid them seeing that you are using the radio

**2. On Approach**

* Slow down
* Turn radios down low or off
* Keep valuables out of sight
* Roll window down low enough for civil conversation, but difficult to put hand inside car
* During day, remove sunglasses
* After dark, turn light inside the cabin on and headlights off
* Be ready with your ID documents
* Have one person who is prepared to talk on behalf the group: Agree where you have come from/ Where you are going/ Who you work for
* Keep a reasonable distance between vehicles
* Be sure you understand the signals given by checkpoint personnel (e.g. are they waving me on or into the side of the road?). Stop if unsure.

**3. At Checkpoint**

You should know the accepted etiquette for passing through a checkpoint in your area. It is always important to stay calm and clearly demonstrate that you are not a threat.

* Stop a few meters from the barrier
* Keep engine running unless told otherwise
* Remain in the vehicle unless asked to get out
* If asked to get out release seatbelt slowly so it does not look like you are reaching for a gun
* Avoid any sudden movements in the car – if moving announce what you are doing before you do it, and move slowly
* Do not laugh or giggle
* Keep hands visible
* If vehicle is searched, comply
* Be friendly, co-operative and alert. Treat the soldiers or police with respect. They have a boring job to do, and are likely to give you an easier time if you show an interest in them. If appropriate, chat a little, perhaps about their family.
* If they ask you to do things that are inappropriate, be polite but firm in refusing, and use gentle humour if appropriate.
* NB. A soldier asking for money is a negotiation. A solider pointing his gun at you and demanding money is armed robbery. If threatened with a weapon, comply calmly with their instructions.
* If anything stolen, politely ask for it back (use your judgement; if the situation is threatening it may be best to accept the loss). If there is the possibility of violence at a checkpoint report the incident to a more senior officer once your journey is complete.
* If at all possible, refuse lifts to armed or uniformed personnel. Be prepared to be turned back if your organizational policy forbids it.
* Avoid looking back
* Once the checkpoint has been cleared and you are out of view report back in to base that you are continuing on your route.

**4. What now?**

**Swipe right for this lesson’s checklist**

*RELATED LESSONS/TOOLS*

* *Preparation lesson*
* *Arrest lesson*

*FURTHER READING*

* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)

***Checkpoint Basic Checklist***

* ***Assess nature of checkpoint***
* ***Slow down***
* ***Turn off radios***
* ***Roll down windows***
* ***Remove sunglasses/turn off headlights & turn on interior light***
* ***Get travel documents ready***
* ***Nominate spokesperson***
* ***Keep distance between vehicles/ barrier***
* ***Keep engine running***
* ***Remain in vehicle***
* ***Keep hands visible***
* ***Avoid sudden movements***
* ***Comply with vehicle search***
* ***Be friendly, co-operative & alert***
* ***Firmly but politely refuse inappropriate requests***
* ***If threatened with a weapon, calmly comply***
* ***Refuse lifts to personnel if possible***
* ***Don’t look back***
* ***Once out of sight, report back to your base***

**KIDNAPPING**

*BASIC*

**1. Why do People Kidnap?**

The best defence against kidnapping is having and practising a high-quality, well-managed security management plan, which is based on a thorough understanding of the general context and risks, and on the context and threat of kidnapping specific to your location. Understanding who carries out kidnappings, and why, will help shape your avoidance and survival strategies.

The main reasons for kidnappings are:

* To hold for ransom
* To cause a political effect
* To achieve publicity
* To be used as human shields

The main actors that carry out kidnappings are:

* Criminals
* Political extremists
* Terrorists
* Militia groups
* Regimes that use terror

Factors which may encourage kidnapping:

* The state’s ability to provide protection from the crime, and prosecute those who engage in such activity
* A lack of political, legal or military response will encourage more actors to become involved
* Media coverage of successful kidnap attempts
* High financial rewards from kidnapping

**2. The Phases of a Kidnapping**

1. **Surveillance**
2. **Capture**
3. **Transport (This could happen several times)**
4. **Confinement**
5. **Release/ Termination**

This Beginner lesson concentrates on the first 2 phases: how to AVOID kidnap by reducing the incentives and opportunities for kidnap and making it more complex for prospective kidnappers.

For advice on survival techniques in the event of being kidnapped go to the **Advanced lesson**, and for advice on what to do if a colleague has been kidnapped go to the **Expert lesson**.

**3. Reduce promoting factors**

* **Stay low profile**

Don’t use big expensive cars; avoid ‘no-go’ areas in town; don’t display assets etc.

* **Build key relationships**

Build relationships with key actorswho may be of use in the prevention of kidnapping. In environments where a host is responsible for the wellbeing of their guests, it might be a good idea to obtain local protection. Likewise, asking respected elders to join a site visit may offer a form of protection. Only good knowledge of the context will determine whether this tactic will reduce the risk.

* **Be aware of how work is received**

If the political or conflict situation is putting your work at a heightened risk be prepared to suspend the programme if necessary and leave the country for a period of time if appropriate. (See **Evacuation lesson** for more advice on this)

* **Have a public policy of no ransom**

**4. Reduce Opportunity**

* **Be cautious**

Don’t make yourself an easy target. This will mean different things depending on the local context but may include avoiding walking to the shops on foot or driving alone at night. See the **Vehicle lesson** for detailed security advice for vehicles. At times of heightened risk you should restrict movements to minimum necessary.

* **Avoid predictability**

50% of abductions take place while the victim is in their car. The majority take place in the early morning, within 400 meters of home or office, due to a predictable pattern of behaviour. Roadblocks or car accidents may be staged to create a scene where abductors then have a pretext to operate quickly, disguised as officials. Avoid predictability when moving between residences and offices, as well as in off-hours activities, such as taking children to school and going shopping. It may be difficult but try to vary travel times and routes.

* **Reduce visibility**

This might mean staff travelling in a trusted taxi rather than an easily identifiable agency vehicle. If there is a suspicion that radio communications may be overheard, staff should not be identified when travelling. Information about movement plans, routes and travel times should be encoded.

* **Ensure good site security for homes and offices**

Site protection and strict rules governing the identification of strangers and limits on access complicates the situation for potential kidnappers.

**5. Practice counter-surveillance**

In simple terms this means ‘watch to see if someone is watching you’. A successful kidnapping normally needs planning, and the perpetrators will be watching the residence, office and movements of their identified target for some time before making their move. They may try to find out more about the residence by presenting themselves as servicemen, or checking the locks of doors and windows while staff are away. They may follow a target in a car to establish routines and identify the ideal point at which to strike. Practicing counter-surveillance may also make you aware of an imminent attack.

* Be observant and watch for anything unusual
* Note if someone starts asking numerous unexpected questions or takes an unexpected interest in you are or the work that you do.
* Situational awareness is vital
* Know the “choke points” on your route
* Multiple sightings of the same person, vehicle, or activity may confirm you’re being watched.
* If you are suspicious that you are being followed you can speed up, slow down, make three right turns, stall at a green light and continue just as the lights change back to red, take a one way street, or make a dead stop. Check if any cars following are doing the same thing.

Practicing counter-surveillance effectively requires constant attention and knowledge about the local environment, including who belongs in the locality and who does not. See the **Counter-surveillance lesson** for more detailed advice.

**5. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Advanced lesson for advice on survival techniques if you are kidnapped.**

**Go to the Expert lesson for advice on what to do if a staff member is kidnapped.**

*RELATED LESSONS/TOOLS*

* *Evacuation lesson*
* *Vehicle lesson*
* *Counter-surveillance lesson*

*FURTHER READING*

* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)
* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)
* [*Protection International: New Protection Manual for Human Rights Defenders (3rd Ed.)*](http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/)
* [*EISF Abduction Advice Note*](https://www.eisf.eu/wp-content/uploads/2014/09/0541-MO-2010-Advice-Note-Abduction-Kidnapping.doc)

***Kidnapping Basic Checklist***

* ***Understand local kidnapping threat***
* ***Reduce promoting factors***
  + ***Stay low profile***
  + ***Build key relationships***
  + ***Be aware of how work is received***
  + ***Have public policy of no ransom***
* ***Reduce opportunity***
  + ***Be cautious***
  + ***Avoid predictability***
  + ***Reduce visibility***
  + ***Ensure good site security***
* ***Practice counter-surveillance***
  + ***Be observant***
  + ***Note unusual interest***
  + ***Maintain situational awareness***
  + ***Know choke points on route***
  + ***Look out for multiple sightings***
  + ***Practice counter-surveillance techniques and watch for response***

*ADVANCED*

**1. Kidnap Stages**

Your main goal if you have been kidnapped is to survive and regain freedom.

How you behave during a kidnapping can increase or reduce the likelihood of survival and regaining freedom. You therefore have some control over the outcome of a kidnapping.

There are five key phases of a kidnap/hostage situation:

1. **Surveillance**
2. **Capture**
3. **Transport (This could happen several times)**
4. **Confinement**
5. **Release/ Termination**

Prevention measures for stages one and two are dealt with in the **Beginner** **lesson**. This lesson will outline survival strategies for capture, transport, confinement and release.

**2. Capture**

The first 15 - 45 minutes are the most dangerous moments in the event; the abductors will be under stress, they are probably armed and most likely to use weapons if resistance is shown. Your objective is to survive, hence:

* Be calm and cooperative, speak only when spoken to, listen carefully and attentively, avoid sudden moves. Do not behave aggressively or try to be a hero: accept the situation.
* If in a group, try not to be separated. Appoint one person to speak for the group, selected on the basis of ability rather than formal rank.
* Do not attempt to escape and or to physically resist.
* Do not make eye contact it may be mistaken for aggression.
* Recognise that fear and shock are normal reactions.

**3. Transport**

* You may be drugged, blindfolded, restrained and beaten. Do not resist, the main purpose is to make you more submissive.
* If being transported, use the time to compose yourself. Keep your mind active.

**4. Confinement**

* Anticipate periods of isolation and other methods of intimidation and prepare for a long wait. Do not believe everything you are told. Try to persuade your abductors to contact your colleagues or the authorities, find reasons why this would benefit them.
* Try to build a relationship of respect whilst keeping your dignity, do not beg or plead; be cooperative and obey demands without being servile or aggressive; do not discuss politics, keep to mutual subjects such as family and children; encourage your abductors to view you as a person.
* Try to retain personal belongings such as clothes, identification, watch and books unless forced to hand them over; ask for practical things such as toiletries, medicines, or time to exercise; avoid an exchange of clothes with abductors - it may hinder your identification in a rescue attempt.
* Be aware of body language and non-verbal communication styles; do not threaten to testify against abductors; if concealing their identity, do not indicate that you recognise them.
* Eat and drink water even if you have no appetite or it is unpalatable; maintain a routine of rest and activity; try to exercise daily and to keep track of time; maintain personal hygiene and maintain your values.
* Try to remember positive and pleasant memories, meditation techniques or other ways to connect to your personality; mentally reconstruct books or movies; think positively; do not despair; do not allow yourself to be convinced that you have been abandoned – your colleagues and family will be working on your release.
* Keep a low profile, avoid appearing to study your abductors, although, to the extent possible, make mental notes about mannerisms, behaviour, speech, clothes, ranks, etc, in order to understand their profile, attitude and intentions; it may help in establishing possibilities for communication, the potential risks and may help the authorities after your release.
* Agree to talk on the radio, phone or video: say only what you are asked to, do not try to send signals or messages; if asked to sign notes, or write a confession, do so if not doing so will endanger your, or others, well being. You may be asked for specific details of your personal life and/or family, be aware this may be part of ongoing negotiations regarding your release (known as proof of life). Never get directly involved in the negotiations for your release. This will only complicate matters.

**5. Termination/Release**

This will come through release, rescue or escape (as a last resort only).

* If released; obey all instructions from your abductors.
* If rescue is attempted by force lie on the floor, put hands over your head, do not try to identify yourself until appropriate to do so.
* Escape should only be considered if you are sure it will succeed, or if it is imperative in order to *save your life*, otherwise it may create more danger. If in a group it may endanger the lives of others and may frustrate rescue activities. If you are caught you are likely to be held in harsher conditions than before.

**6. Aftermath**

* Regardless of the method of freedom, expect to be immediately and thoroughly debriefed. Cooperate with the authorities, giving as much detail as possible.
* You will not immediately get all the quietness and privacy you may want. Being kidnapped is a huge psychological ordeal: expect to feel its impact for months and perhaps even years to come, but feel confident that, with the right help, you can recover and get on with your life. See the **Dealing with Stress lesson** for more help on this.

**7. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on how to avoid kidnapping.**

**Go to the Expert lesson for advice on what to do if a staff member is kidnapped.**

*RELATED LESSONS/TOOLS*

* *Travel Prep lesson*

*FURTHER READING*

* [*EISF Abduction Advice Note*](https://www.eisf.eu/wp-content/uploads/2014/09/0541-MO-2010-Advice-Note-Abduction-Kidnapping.doc)
* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)
* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*Protection International: New Protection Manual for Human Rights Defenders (3rd Ed.)*](http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/)

***Kidnapping Advanced Checklist***

***Capture***

* ***Be calm & cooperative***
* ***Try not to be separated***
* ***Do not attempt escape***
* ***Do not make eye contact***
* ***Accept that fear and shock are normal***

***Transport***

* ***Do not resist efforts to make you more submissive***
* ***Use time to compose yourself & mentally prepare***

***Confinement***

* ***Anticipate isolation***
* ***Do not believe everything you’re told***
* ***Advocate for contact***
* ***Build relationship of respect***
* ***Try to retain personal belongings***
* ***Be aware of body language***
* ***Do not threaten abductors***
* ***Eat and drink even if you don’t want to***
* ***Exercise daily***
* ***Maintain hygiene***
* ***Keep track of time***
* ***Maintain personal values***
* ***Meditate***
* ***Reconstruct positive memories or stories***
* ***Keep a low profile***
* ***Watch behaviour for indicators of intentions***
* ***Agree to demands if not doing so will endanger you or others***

***Release***

* ***Obey all instructions***
* ***If force is used, lie on floor with hands over your head***
* ***Escape should ONLY be considered if necessary to save your life***
* ***Cooperate with authorities***
* ***Manage your mental health***

*EXPERT*

**1. In Case of Kidnapping**

Dealing with the kidnapping of a member of staff is a very sensitive and complex task. This lesson provides only the basic outline for recommended actions.

**If one of your staff is kidnapped we highly recommend reading the detailed advice given in the ‘*Further Reading’* links at the end of this lesson.**

**2. First Steps**

If kidnap occurs, the organisation should immediately set up a crisis management team, in HQ if possible. It should be made clear at once which manager has responsibility for managing the incident. That manager should then consider the following actions, depending on the circumstances and his or her assessment of the best course of action:

* Inform the local police and other appropriate authorities
* Inform all relevant parties of the name and contact details of the incident manager. Request that no action be taken in relation to the incident without prior agreement with him or her.
* The incident manager should delegate responsibilities to colleagues as appropriate: e.g.:
* Contacting Next of Kin. This should be a top priority. Failure to do this quickly can damage the relationship of trust with the staff member’s family, particularly if they first hear the news through the media. This could then make the management of the crisis much more difficult.
* Answering enquiries from the press
* Keeping contact with all relevant staff and other agencies
* Providing 24-hour communications and logging all messages and events
* Marking maps
* Ensuring that the crisis management team has sufficient food, water and rest

**3. Make a Plan**

* Make a plan. Will you negotiate directly with the kidnappers, if that is possible? Or will you appoint an intermediary? (A trusted intermediary is often thought preferable, to give time for decision-makers to consider their responses to any messages from the kidnappers.)
* Decide whether to call in specialist advice, either from the police or from a reputable company specialising in hostage negotiations. It may help if contact has been made with such a company before any kidnap occurs. If you are not sure that you have the necessary expertise to handle a kidnapping, specialist advice from a reputable company is strongly recommended.
* Allocate the necessary resources – human, financial and other – to ensure that your plan has the best possible chance of success.

**4. Carry out Plan**

* Carry out your plan.
* While you will naturally desire to conclude the incident safely and as quickly as possible, kidnap negotiations can sometimes last months or even years. Prepare the crisis management team for this, while encouraging them to remain optimistic. Keep morale high: enough food and rest are helpful, but possibly the greatest aid to morale is to manage the incident well, keeping everyone fully informed, and taking the best available advice.
* Ensure strict confidentiality from the onset of the crisis. Information should be shared only on a need to know basis. This may require the usual management chain to be bypassed, e.g. if someone is part of the crisis management team, he or she should be exempted from reporting to his or her superior on the crisis.
* Ransom should not be paid. All humanitarian organisations should have a clearly stated policy that ransom will not be paid in case of kidnap, since to do so encourages more kidnapping.
* Throughout the crisis, significant events and decisions should be recorded, and lessons learned wherever possible.

**6. Aftermath**

* Attend to the needs of the victim, including making arrangements for them to speak to their loved ones and for their physical reunion.
* Arrange for the authorities to meet and interview the victim.
* Manage the press; organise a short press conference with the victim and/ or their family, and retain control over press contacts.
* Arrange for a debriefing with the organisation.
* Arrange time off, with full insurance coverage and no loss of income.
* Arrange for professional and appropriate counseling and long-term support mechanisms.
* Specific preparations need to be made in case of a negative outcome.
* Once a kidnap incident is resolved, conduct an after-action review, to see what lessons can be learned.

**6. What now?**

**Swipe right for this lesson’s checklist**

**Go to the Beginner lesson for advice on how to avoid kidnapping.**

**Go to the Advanced lesson for advice on survival techniques if you are kidnapped.**

*RELATED LESSONS/TOOLS*

* *Travel Prep lesson*

*FURTHER READING*

* [*Good Practice Review Number 8: Operational security management in violent environments (Revised Ed.)*](http://www.odihpn.org/download/gpr_8_revised2pdf)
* [*CARE International: Safety & Security Handbook*](http://ngolearning.org/courses/availablecourses/CARE%20Safety%20Course/Shared%20Documents/English_CARE_International_Safety_and_Security_Handbook.pdf)
* [*EISF Abduction Advice Note*](https://www.eisf.eu/wp-content/uploads/2014/09/0541-MO-2010-Advice-Note-Abduction-Kidnapping.doc)
* [*Protection International: New Protection Manual for Human Rights Defenders (3rd Ed.)*](http://protectioninternational.org/publication/new-protection-manual-for-human-rights-defenders-3rd-edition/)
* [*ECHO Generic Security Guide for Humanitarian Organisations*](https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fecho%2Ffiles%2Fevaluation%2Fwatsan2005%2Fannex_files%2FECHO%2FECHO12%20-%20echo_generic_security_guide_en.doc&ei=kLxAVc6LOILuUP2SgbAE&usg=AFQjCNEXEOcbLeV24f3WolHmDwLq7KJzlQ&sig2=hbnI7wfdrGIHS7mmikBRWA)

***Kidnapping Expert Checklist***

* ***Read detailed advice manuals***
* ***Set up crisis management team***
* ***Inform authorities***
* ***Inform all of incident manager***
* ***Contact next of kin***
* ***Answer enquiries from press***
* ***Keep contact with relevant staff & agencies***
* ***Provide 24 communication channels***
* ***Log decisions and events***
* ***Ensure wellbeing of crisis management team***
* ***Make a negotiation plan***
* ***Consider specialist advice***
* ***Allocate all resources needed***
* ***Carry out plan***
* ***Keep morale high***
* ***Ensure confidentiality***
* ***Avoid payment of ransom***
* ***Attend to needs of victim***
* ***Arrange meeting with authorities***
* ***Manage the press***
* ***Arrange debrief with organisation***
* ***Arrange time off***
* ***Arrange professional counseling***
* ***Prepare for possibility of negative outcome***
* ***Conduct a review***