General Intelligence and
Security Service
*Ministry of the Interior and
Kingdom Relations*

# Travelling abroad

## *Safety risks*

**Are you travelling abroad for professional purposes?**

**Be advised that travel abroad makes you a possible target for espionage. The same applies to long-term employment abroad.**

**Foreign intelligence services are interested in you and in the knowledge you may have.**

**The information in this flyer may help you take precautions to diminish the risks of (cyber-)espionage.**

*The risk of being subject to espionage varies between countries. Depending on your destination it is possible you may receive additional briefings on the specifics of a particular country.*

# Before travelling



## In general

Take no, or as little as possible, confidential information with you. You are responsible for the careful handling of this information. Always ask yourself the following questions before departure:

- Do I really need this?
- What is the value of the information I am carrying (be it on paper, on a data carrier, or otherwise)?
- What would the damage be should the information fall into the wrong hands?
- Which devices should I bring?

When you do bring along confidential information, compile a list of the documents, data carriers and equipment you will be carrying. Should anything be lost or stolen, it will be easy to identify what is missing. Keep this list at your office.

Always transport your confidential documents in your hand-luggage, never in your suitcase. Take note of the applicable regulations for the transport of information classified as state secret.

If there is a Dutch consulate or embassy in the country of your destination, inform them when you are planning to visit a public-sector organisation there.

## Digital

Erase the call history on your mobile phone and delete any received and sent text messages. Only save indispensable contacts to your phone contact list. Consider using a disposable mobile phone, sim card, or temporary email account.

If you travel abroad frequently, it is advisable to acquire devices intended solely for use abroad. Make sure you bring your own chargers, adaptors, cables and car kit.

Only install applications that you actually need. Consult your organisation's security officer for information on trusted applications.

Change your passwords prior to (and again after) your trip.

Use different passwords for all your devices and make sure they are different from your workspace login security passwords.

Beware of people looking over your shoulder or meddling with your equipment. Cover your webcam and use privacy foil or anti-tamper stickers to shield against prying eyes and prevent tampering.

Inquire which security aids are available within your organisation.

## Personal

Be reticent about bringing personal equipment, since your personal devices are just as interesting to foreign intelligence organisations as your professional equipment.

Make sure you use different devices for personal and professional conversations and keep these devices separate from each other as much as possible.

When on a personal trip, try not to bring any devices or information related to your work. Refrain from mentioning that you are going abroad on social media like Twitter or Facebook.

# In transit

## In general

Refrain from presenting yourself as a government official.

Do not enter into confidential talks on the phone or when you are making use of (public) transport such as a rental car, train, or plane.

Keep information and data carriers on your person as much as possible.

Do not tell your conversation partner more than you have to.

Be vigilant when it comes to ‘chance’ encounters with people who take a particular interest in your work or private life, or people attempting to contact you via social media.

Your conduct may put you in a vulnerable position, either immediately or at a later moment. Not just drugs and alcohol, but also

gifts or personal advances may be used to influence you.

Be aware that people may take film and or audio recordings of you in order to pressure you at a later moment; this is also true when using social media or dating apps!

Make sure you can check whether anyone has accessed confidential information. You can use security bags or similar items for this. Do not use hotel safes to store confidential information or data carriers.

## Digital

Switch off all your devices when engaging in a confidential discussion. Remove the battery or place the device between clothes or in a bag in order to muffle the sound. You are more vulnerable to espionage when your equipment is switched on.

Switch off Bluetooth on all your devices. Bluetooth is unsafe and easily exploited for purposes of espionage.

Do not download or update applications while abroad. When required to use local software, use a separate device to do so. Disable automatic updates in the app or play store.

Be wary of unexpected or odd (security) notifications on your phone, laptop or tablet. These notifications may indicate an attack or breach. Make a note of any notifications and other unusual matters and report them to your organisation's security officer upon return.

Never share your password with anyone and do not allow anyone to make use of your equipment.

Refrain from using public Wi-Fi for work purposes.

When working in a mobile setting, never use equipment provided to you by another party. Do not link or connect your devices to those of others (e.g. printers and chargers).

Preferably use an approved VPN connection. Use secure and authorised pen drives. Check with your organisation's security officer for recommendations.

Be cautious when opening emails, text messages, and other electronic messages from unknown parties.

Be careful of spear phishing. Always check whether you are the intended recipient of received messages. When in doubt, first verify the origin of the message with the alleged sender.

Never hand over your equipment. Should you be ordered to do so for security purposes, place them inside a security bag or entrust them to a colleague for safekeeping.



In case of an incident, always inform your organisation's security officer immediately. When in doubt: report!

# After travelling

## In general

Change the password of all devices and (social media and email) accounts brought and used on your trip.

You may be required to hand in your device for analysis or clean-up. It may sometimes even be necessary to destroy the equipment upon your return, as using it will no longer be safe. Your organisation may have guidelines on the matter, often varying for specific travel destinations.

## A secure digital environment

Whether you are travelling or not, always make sure that your digital environment is secure. Some additional tips:

Always ensure that your detection and security software is up to date.

Encrypt sensitive information when storing it on a laptop or (secure) flash drive.

Use security software that only allows specific devices access to your computer.

Use encryption when exchanging sensitive information over public networks and make use of two-factor authentication.

Read more on digital security in the AIVD publication ‘Cyberespionage; Are you aware of the risks?’ on aivd.nl.

*If you have any questions, please contact your organisation’s security officer.*

Safe travels!

General Intelligence and Security Service
aivd.nl

december 2017