TRAVEL SECURITY

HOW TO PROTECT YOURSELF AND YOUR DATA ABROAD

SECURITY PASSPORT

WHO IS THIS DOCUMENT INTENDED FOR?

This brochure contains a range of useful tips for every person or organisation that wants to improve the security of their data during travels abroad.

The tips offer no absolute guarantee, however. Everyone has the responsibility to make sure that their data or the data of their organisation are as secure as possible.

HEIGHTENED RISK ABROAD

We have become so used to travelling abroad that we **often forget the risks we are exposed to**. Accidents, loss of data, theft or espionage: no one is immune to these risks.

Travellers are vulnerable. They go from place to place while carrying data or materials belonging to their organisation or their country. Criminals, but certainly also foreign intelligence services and other people or organisations, regard this as an opportunity. Foreign intelligence services are probably more interested in you than you realise. They are particularly keen on the knowledge that

you have, that you carry with you or to which you have digital access.

Do not underestimate the risks: reputational damage or financial loss, prosecution or sanctions, diplomatic or political incidents, and so on. The consequences for you and your organisation can be (very) serious.

This document contains advice for **each of the three stages of travel**: before departure, during travel and upon return.

The risks are not the same for every country. The advice is therefore not necessarily applicable to each of your travels or journeys. Ultimately, you must carefully assess the potential risks yourself.

HOW CAN YOU PROTECT YOURSELF?

Choose advice that matches your needs and the risk level of your journey.

3 RECOMMENDATION LEVELS

BASIC

The minimum protection required for each journey.

MEDIUM

Additional measures for better protection of your personal data and the data of your organisation.

HIGH

The strictest measures needed for travel outside the European Union or when carrying sensitive information.

The above recommendation levels are cumulative.

3 STEPS

BEFORE DEPARTURE

Thorough preparation is key in order to minimise the risks. The purpose of the preparation is to limit the number of documents and storage devices (laptops, smartphones, USB flash drives, etc.) and to ensure that they are properly secured. Before departure, always ask yourself the following

questions:

- Do I really need this?
- What is the value of the information that I will be carrying?
- What is the impact of improper use of this information?
- Which devices am I taking with me and to what information do they provide access?

DURING TRAVEL

Caution and discretion are the keywords for well-informed travellers. Do not disclose too much to others and always keep control of your information.

UPON RETURN

Certain threats remain, even after your return. If you have the slightest doubt, have your storage devices checked by your security officer and inform them of every incident.

BEFORE DEPARTURE

1. Find out about your destination

Make sure that you are informed of the **political, economic and social situation of your destination.** Useful information can be found on the 'Travel advice' page on the website of the FPS Foreign Affairs www.diplomatie.belgium.be. Also register on the website **travellersonline.diplomatie.be** so that the FPS Foreign Affairs can keep you informed and support you more easily. BASIC

Do not forget to save or note down on paper the **contact details for the nearest Belgian embassy or consulate.** MEDIUM

Inquire about local legislation and any required travel permits. If foreign authorities require you to fill in travel documents, only provide **the information that is strictly necessary and only provide further details if the authorities insist**.

HIGH

2. Prepare your documents and storage devices

Verify which **security regulations apply in your organisation**. Do not hesitate to contact the security officer(s) to ensure that you are well-prepared for your trip. BASIC

Only **take the documents and storage devices with you that are strictly necessary**. Be aware of the context and the purpose of the trip. In some countries, the security services are authorised to request access to your storage devices and/or to confiscate them. You are therefore taking unnecessary risks by carrying non-essential documents or storage devices. BASIC

Create a **back-up** of your data and leave it at home. BASIC

Always carry your confidential documents and data storage media in **your hand luggage, never in your suitcase**. BASIC

Carry your sensitive documents in **sealed and secured envelopes** (sealbags) and have them ready for the other phases of the trip. MEDIUM

If possible, only bring mobile devices that have been specifically provided for the trip and that have been provided by your organisation. These

devices may **only contain the data that are strictly necessary** for the trip. Upon your return, these devices must be reformatted before they can be used again. HIGH

3. Protect your mobile devices

Follow the recommendations that are available on: **www.safeonweb.be/tips**

We would like to draw your attention to the following recommendations:

- Install the operating system's (OS) **latest updates** and only install programmes or apps through official app stores; BASIC
- Install **antivirus software** on all your mobile devices; BASIC
- Check the **security and privacy settings** on your devices and the accounts that are linked to them. When doing so, protect your personal data as much as possible; BASIC
- Use secure **locking methods** and disable notification content so that nobody can read your messages without your permission; BASIC
- Protect your passwords! Do not write them down, change them regularly and use **Two-Factor Authentication (2FA)** wherever possible; BASIC
- Install **end-to-end encrypted** messaging applications; BASIC
- Delete your **call and browser history** before your departure. MEDIUM

Always **keep your work separated from your private life**, whether it concerns devices, accounts, telephone numbers or e-mail addresses. MEDIUM

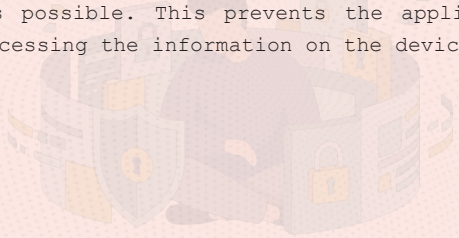
To avoid leaving traces from your home networks and home devices, select 'forget' for all previously **connected networks and Bluetooth devices**. MEDIUM

Set up a connection secured by **VPN**, mainly for access to your messages or to your organisation's network. MEDIUM

Encrypt sensitive data on your storage devices according to your organisation's policies. MEDIUM

Please note: some countries prohibit the use of VPN or encryption software! Be sure to check this before travelling to your destination.

Install as few applications as possible on your device and use a **web browser as an alternative** as much as possible. This prevents the application from accessing the information on the device. HIGH



4. Social networks

Check your **privacy settings** on social media. Keep your personal data private as much as possible. BASIC

Check the **access rights for each application** (access to microphone, camera, contacts, location, etc.). These are often not strictly necessary in order to use the application. BASIC

If possible, avoid talking about your trip on social media. It is also preferable to not post any details online about the programme, the people accompanying you and/or your location. MEDIUM

Do not simply accept messages, networking requests or invitations from third parties. Limit yourself to **the communication that is necessary for the trip**. MEDIUM

DURING TRAVEL

1. Stay discreet and cautious

Do not wear any visible logos or identification outside the workspace. MEDIUM

Do not reveal your location via your smartphone or tablet. Turn off **access to your location data.** MEDIUM

Avoid prying eyes: put a **filter on your screen** when you need to work in a public or busy place. MEDIUM

Do not talk about sensitive or polarising topics in public places where other people can listen in. MEDIUM

Turn off the **non-necessary connections** (Bluetooth, wi-fi, Near Field Communication (NFC)) of your mobile devices. A**irplane mode is not sufficient**: this mode does not always turn off these connections completely. MEDIUM

Do not use voice assistants such as Siri, Alexa or Bixby. Also avoid other AI apps. HIGH

If you need to hand over or leave your smartphone somewhere, remove its **SIM card**, **memory card and battery** - if possible. HIGH

2. Protect your data and storage devices at all times

Never leave your documents, data storage devices or other devices **unattended** and definitely never give third parties access to them. BASIC

Never charge your devices through charging equipment that is offered to you and/or public USB charging points in order to avoid malware or data theft. If there is no other option, use a **data blocker cable** to protect your device. BASIC

Make sure your devices are equipped with **appropriate anti-theft systems** and unique passwords so that they cannot be swapped with others. MEDIUM

Do not leave sensitive documents in your hotel room or in your hotel room safe. It can easily be opened by hotel staff at the request of people with malicious intent. MEDIUM

Do not connect to public wi-fi networks, do not establish public Bluetooth connections (e.g. with a rental vehicle) and avoid using QR codes that you do not trust. MEDIUM

Turn off your devices completely at night - perform a **power cycle** (turning your device on and off completely) every day. HIGH

3. Remain sceptical

Remain sceptical when you receive an unusual amount of attention or when the person you are speaking to refers to shared ideological, cultural or religious references. MEDIUM

Be wary of flattery, unburdenings and gifts (these are seldom without ulterior motives). MEDIUM

Do not be misled by displays of solidarity or friendship. These elements can be signs of **manipulation attempts**. MEDIUM

Also remain careful during (social) events organised on the margins of an official gathering. MEDIUM


EARTH
EARTH
EARTH

UPON RETURN

Upon your return, perform a **power cycle** on your devices. BASIC

Report any incident or suspicious occurrence in writing to the security officer of your organisation. BASIC

If you have received a **USB flash drive or other electronic storage device, never connect it** to your computer without a prior security check by an expert. BASIC

If you have the slightest doubt, **have your computer or smartphone checked and change your passwords.** BASIC

Scan your devices **regularly** for viruses and malware. BASIC

Question the purpose of the relations established during the trip. **Remain sceptical** if you are contacted again after the trip: are the requests, questions or offers justified and relevant? MEDIUM

WHAT TO DO IN THE EVENT OF AN INCIDENT?

If the document or storage device is lost or stolen, compile a list of the data involved. Immediately inform your employer or security officer in accordance with your organisation's policies. Contact the local police if necessary.

If you lose your identity documents, contact the Belgian embassy or consulate.

If your bank card is lost, call Card Stop on **078 170 170**. You can also block your bank card through your bank's application.

If you were confronted with other suspicious situations (lengthy questioning during border checks, unsolicited photographs, mandatory handover of storage devices, etc.), contact us via **vsse.be/contact**.

MORE INFORMATION?

- www.vsse.be
- www.diplomatie.belgium.be
- www.safeonweb.be

THE VSSE

The VSSE is responsible for monitoring cases of interference or espionage that pose a threat to the fundamental values of the state, including the protection of the scientific and economic potential. There is a heightened risk of these threats when travelling abroad.

If you believe that you or your organisation has become the victim of interference or espionage activities, or if you possess information that may be linked to these threats, contact us via **www.vsse.be/contact**

VSSE

VSSE

.be

Responsible editor: Francisca Bostyn
Boulevard du Roi Albert II, 6
1000 Brussels