Business travel - IT security - Best practices

Date: 12.04.2024

Author: JF Dousson

Protecting confidential information when travelling

Information security is also important when travelling, and needs to be prepared in advance.

More and more Swiss companies are falling victim to economic espionage, and the academic world is not spared.

Some countries have legislation enabling them to demand that any traveller arriving at the border disclose their passwords, even if they have not previously committed an offence and are not under suspicion. Others try to gain access to privileged information by accessing equipment left in a hotel room or analysing unencrypted traffic.

These best practices aim to secure the information available to travellers, which is exposed to variable risks depending on its level of confidentiality (intern, confidential, secret), the traveller's area of research, the level of security in the country visited, and local laws and practices. As these factors change regularly, it is not possible to provide a list of the countries concerned.

Before travelling

Medium risk level

Back up all the data stored on the devices you want to take with you on your trip so that you can retrieve it when you return.Do not take the backup with you on your trip, whatever the medium.

Delete any data not required for the trip from the devices you are taking with you. Note that in some cases it is possible to recover deleted files.

Remove email synchronisation and delete mailboxes stored on devices to be taken on trips.

Install the EPFL VPN client.

Activate, if available, the ability to remotely wipe equipment in the event of theft or loss.

Ensure that operating system, applications and anti-virus software are up to date.

Check that the equipment is protected by a password/PIN code when switched on.

Make sure that the equipment does not automatically connect to WiFi when switched on.

High risk level

Leave all commonly used business peripherals (laptop, tablet, smartphone) at the office.

Use an old smartphone that has been reset. Deactivate biometric unlocking and replace it with a PIN code.

Enter only the contacts you need for your trip.

Encrypt sensitive documents needed for the trip on a laptop or tablet reset before the trip, which will only be used to access them.

Activate, if available, the ability to remotely wipe the equipment in the event of theft or loss.

Ensure that operating system, applications and anti-virus software are up to date.

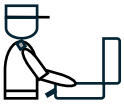
Make sure that the equipment does not automatically connect to WiFi when switched on.

Extreme risk level

Leave all business peripherals (laptop, tablet, smartphone, USB sticks, mobile hard drives) at the office.

Enter only the contacts you need for your trip on a phone that has been reset and updated for the occasion. Do not install any applications that access data in the cloud. Do not connect any mailboxes.

Do not download any sensitive documents.



During the trip

Medium risk level

Before arriving at the airport, switch your smartphone to aeroplane mode.

Access the Internet only via EPFL VPN.

Only access your professional emails from ewa.epfl.ch via the VPN.

Do not download documents on devices taken on trips.

Do not leave equipment unattended. Do not leave equipment in the hotel room, in the hotel room safe or at the hotel reception desk.

Do not recharge peripherals from a USB socket (airport, hotel, taxi, etc.).

If your equipment is searched, ask to be present.

Disable WiFi, Bluetooth and geolocation when not required.

Do not connect any peripherals handed in by a third party, or found, to equipment brought on the trip.

Consider equipment to be compromised if it has been accessed by a third party, even in your presence.

Switch off the smartphone if confidential information needs to be discussed.

Never lend your equipment under any circumstances.

High risk level

Before arriving at the airport, switch off the smartphone and switch it on again a few kilometres from the airport.

If your equipment is searched by the local authorities, ask to be present.

Deactivate WiFi, Bluetooth and geolocation.

Do not leave equipment unattended. Do not leave equipment in the hotel room, in the hotel room safe or at the hotel reception desk.

Do not recharge peripherals from a USB socket (airport, hotel, taxi, etc.).

Do not connect any peripherals given to you by a third party or found with the equipment you have brought with you on your trip.

Consider equipment to be compromised if it has been accessed by a third party, even in your presence.

Switch off the smartphone if confidential information is to be discussed.

Never lend your equipment under any circumstances.

Extreme risk level

Before arriving at the airport, switch off the phone and switch it on again a few kilometres from the airport.

Do not leave the telephone unattended. Do not leave the phone in the hotel room, in the hotel room safe or at the hotel reception desk.

Do not recharge the phone from a USB socket (airport, hotel, taxi, etc.).

If your equipment is searched, ask to be present.

Consider the equipment compromised if it has been accessed by a third party, even in your presence.

Switch off the telephone if confidential information is to be discussed.

Never lend your equipment under any circumstances.

After the trip

Medium risk level

Contact your AdminIT or IT Security if your equipment has been accessed by a third party, even in your presence. DO NOT CONNECT IT TO THE EPFL NETWORK.

High risk level

Reset / have reset equipment taken on a trip. DO NOT CONNECT IT TO THE EPFL NETWORK.

Extreme risk level

Reset / have the phone reset when travelling.

For more information

As mentioned in the introduction, some countries have legislation enabling them to demand that any traveller arriving at the border disclose their passwords, even if they have not previously committed an offence and are not under suspicion. Refusal to disclose passwords can result in the seizure of equipment for a period of several hours to several weeks. It is also possible that the traveller will be refused entry to the country and/or that coercive measures will be taken.

Some countries, such as the USA or Canada, limit their examination in principle to data stored on the device being examined, but it is not excluded that data stored in the cloud and freely accessible from the device may also be examined. They may also ask for travellers' social network identifiers.

The discovery of a hidden encrypted directory may arouse the suspicions of the authorities and will not exempt the traveller from providing the encryption key.

Certain content relating to politics, religion, drugs or pornography is regulated or even banned from entering certain countries. This list is not exhaustive. It is essential to find out before travelling and to check that the peripheral(s) you are taking with you contain nothing of the kind, and that publications on social networks have been filtered accordingly (e.g. a selfie in front of a coffee shop).

More and more Swiss companies are falling victim to economic espionage, and the academic world is not spared. Searching equipment at the border or in a hotel room provides immediate

access to any data of interest to the destination country. It can also be an opportunity to install a backdoor to allow later access to the data, camera or microphone, and then to the EPFL network when the traveller returns and connects his or her equipment.

It should be noted that certain countries and/or certain service providers (transport, seminar organisers, accommodation, etc.) may impose, sometimes in the name of facilitating access, the installation of an application on the traveller's smartphone. This application is likely to require more rights than necessary for the provision of the service, such as position and access to storage, the microphone or the camera, etc.

Nota Bene: Data classified by the Confederation is subject to the Federal Law of 18 December 2020 on the security of information within the Confederation (LSI) and is subject to security measures that take precedence over this document.

For more information