VUB Information Security and Privacy

How To - Travel to High-Risk Countries

Managed by
Chief Information Security Officer

Contact(s)
ciso@vub.be

Last update
Dec. 6, 2019

I. Introduction

A "How To" document provides information and/or tips on a specific Information Security and Privacy subject. It does not contain mandatory guidelines; it provides information on how a standard/guideline can be applied.

It's a living document and its quality depends partly on the feedback received from its readers/users. The cover page provides the contact email address to which feedback should be sent.

A "How To" document does not require any formal advice or approval process.

This "How To" document covers travel to high-risk countries; i.e. high-risk from the point of view of Information Security and Privacy.

II. Travel to high-risk countries

II.1. High-Risk Countries

Travellers should consult the travel advice provided by the Belgium Foreign Affairs department[1]. The US travel advisories[2] can also be consulted but bear in mind that such advice is provided for US citizens who may have a different risk profile than EU citizens. Those who hold a different nationality can also consult their home country's travel advice for any specific requirements/warnings linked to their nationality.

A country may be high risk because of physical risks. Colombia, for example, is a high-risk country due to the high crime rate and terrorism. Other countries are high risk because of information security and privacy risks. China, for example, is a high-risk country due to its state-sponsored cyber capability and the willingness to use this for economic, military and political goals.

⚠This document will only cover travel to high-risk countries which potentially pose an information security risk to the VUB and its Travellers.

Countries like China or Russia are examples of high-risk countries with a high information security and privacy risk. It is important to understand that these are not open democracies, and privacy is not protected as it is in the EU. Individuals may be monitored in terms of both their physical movements and all communications. Electronic equipment might be accessed to steal information and/or injected with malware to infect and access the VUB network on the Traveller's return. Access to some websites, including access to some mainstream western social media websites, may be technically blocked in high-risk countries. And those that can be accessed may be monitored. Secure ("https") websites and the use of the VUB virtual private network ("VPN") may also be blocked, because it is more difficult for national authorities to monitor such encrypted traffic.

II.2. Risks

VUB Travellers are certainly a potential target if they are directly engaged in classified or proprietary research in a STEM (science, technology, engineering and mathematics) discipline. Even those VUB Travellers

[1] https://diplomatie.belgium.be/nl/Diensten/Op_reis_in_het_buitenland/reisadviezen (only available in Dutch en French – consult a colleague for translation if required).
[2] https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

not directly engaged in a STEM discipline may be a target as they can be used as an entry-point into the VUB network.

All electronic devices (laptops, tablets, e-book readers, smart phones, mobile phones) can be successfully attacked and compromised via malware or automated attack tools. Security software including antivirus programs, even when kept up to date, may not prevent electronic devices from being compromised.
Electronic devices may be subject to an official review and even full duplication at the border. In some countries, customs officers may temporarily seize your device, and potentially keep a copy of your entire system on entry or exit.

Encryption products can be used for illegal purposes, including terrorist activity, which is why multiple countries regulate the import, export and use of encryption products. In case of doubt, Travellers are therefore required to obtain information on the position of the country visited regarding encryption. China and Russia are high-risk countries that are not in favour of encryption on electronic devices.

The "Wassenaar Arrangement"[3] allows Travellers to freely enter a participating country with an encrypted device under a "personal use exemption" as long as they do not create, enhance, share, sell or otherwise distribute the encryption technology while visiting. Consult their websites to identify participating countries.

II.3. Recommendations

Hope for the best, assume the worst.

- It is not possible to protect a device against all possible attacks, especially when these attacks are state sponsored. It's therefore best to assume that any device taken to a high-risk country will have been compromised in some, potentially undetectable, way.
- Assume that anything you do, particularly over the internet, will be intercepted. Remain vigilant regarding the content you share (via email, data transfer, voice).

II.3.1. Before you travel to a high-risk country

- Obtain information about any special local laws governing the country of destination; these may be totally different from the ones you are accustomed to.

- Limit the number of electronic (data/communication) devices you take with you.

- For those devices that you must take, do not include your own devices used daily.
    - Use a temporary (inexpensive/depreciated) laptop.
    - Use a throw-away prepaid mobile phone, purchased for that trip only.

  Departments with multiple travel to high-risk countries should consider having a travel kit available, containing electronic devices that are required.

- Use a (temporary) laptop equipped with:
    - A webcam cover.
    - A dummy audio-cable (the built-in microphone of the laptop will be disabled by putting a connector in the audio-jack of the laptop, even when no headset or anything similar is connected to that connector).
    - Do not use Office 365 authentication, but a local user account.
      One admin user, only to be used if required, and one standard user, to be used on a day-to-day basis during travel. Use long secure passwords.

[3] https://www.wassenaar.org/

  - Do not install the Office 365 OneDrive functionality. Bear in mind that OneDrive would synchronize all your data with a copy on the laptop.

- Disable all unnecessary network protocols (such as WiFi, Bluetooth or infrared) and location-sharing functionalities. On all your devices.

- Erase your call and browsing history on your devices.

- Ensure that the systems you use are fully patched (have latest security updates).

- Ensure that every device is equipped with antivirus and anti-malware software.

- Consider creating a temporary email (e.g. Gmail) account to be used during this trip only.
  If you need access to data, consider creating a temporary cloud storage account (e.g. Dropbox) to be used during this trip only. You can store data that you may need on that location, but again assume that all the data stored can be compromised once you log in. Data stored in the cloud can be encrypted using tools such as Boxcryptor[4] for additional security.

- Leave all unnecessary door keys, smart cards, one-time password hard tokens, and any similar access control devices at home.

- Have the contact details of the local embassy/representation available in case of emergency.

II.3.2. During travel

- Watch out for shoulder surfing (attacker looking over your shoulder while you enter data such as user-id and password). Always be aware of your surroundings when logging in or inputting data into your device.

- Keep your electronic devices with you at all times. Your hotel safe is not ‘safe’.

- Do not put your system to sleep/into hibernation when you are not actively using it. Instead switch it completely off.

- Avoid using your Office 365 online login.

- If you don’t want to be geographically tracked, or you’re attempting to have a confidential conversation, mobile phone batteries must be removed. Turning off your mobile phone does not suffice.

- Do not attempt to circumvent national censorship (e.g. with Tor or similar products). Such products/processes may be blocked and/or subject to legal proceedings if noticed.

- Make sure you securely discard any data-holding electronic/non-electronic material if it contains confidential data. Physical destruction is the best approach.

[4] Warning: these tools are not centrally supported by VUB DICT. They should only be used If sufficiently understood by the user.

- Avoid using USB-based public battery charging stations, as the USB interface allows the charging station to do more than just provide power (e.g. read your device).

- Do not use public workstations, unless there is no other option. Bear in mind that everything entered, including login credentials, is compromised.

- Do not purchase new hardware while travelling.

- Do not purchase or download any new software while travelling.

- Do not have a malfunctioning electronic device repaired or worked on locally while abroad.

- Do not connect an unknown USB-data holder, CD/DVD/Blue Ray or any other peripheral to your device.

- In case of any incident, including a lost/stolen device, inform the VUB Helpdesk (helpdesk@vub.be) as soon as possible. They will take the required action (if need be block your user-id access until you return).

- Beware of attempts to put you in embarrassing or compromising positions. You may be targeted for possible extortion.

- If arrested, taken into custody, or interrogated, do not make any statements or sign any documents, particularly if they are written in a language you don't know. Ask to have the Belgian Embassy or Consulate (or if you have another nationality, the embassy of your home country) notified of your detention at once.

II.3.3. On return from travel

- Have all electronic equipment completely wiped and re-installed from scratch if possible. Any data that must be kept should be copied via a USB device; the electronic device itself should never be connected to the VUB network.
  (Working with a travel kit makes this easier, as your day-to-day device remains as-is).

- Change any passwords you may have used during your travels. It's advisable to always change your Office 365 password, even when not used during travel.

II.4. Lower-Risk Countries.

Be aware that some security considerations apply for lower-risk countries, such as the US. Customs may have the right to search your laptop, and you may be legally obliged to provide your user-id and password to enter your laptop. Sensitive information on a laptop can thus be at risk.

You must make a risk assessment of the country you are visiting in view of the data you will be carrying. You may apply some of the aforementioned approaches to protect data, even when visiting lower-risk countries.

A. Annex: Sources

Stanford University: https://uit.stanford.edu/security/travel/high-risk-countries-recommendations

University of Rhode Island: https://security.uri.edu/travel/travel-to-china-or-russia/

Princeton University: https://informationsecurity.princeton.edu/intltravel

China Business Review: https://www.chinabusinessreview.com/cybersecurity-best-practices-for-the-traveling-executive-a-qa-with-crumpton-groups-rick-doten/

Harris/Bricken: https://www.chinalawblog.com/2016/01/when-going-to-china-be-paranoid-about-your-data-and-your-privacy.html

Belgium Foreign Affairs: https://diplomatie.belgium.be/nl/Diensten/Op_reis_in_het_buitenland/reisadviezen

US Department of State: https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

The Wassenaar Agreement: https://www.wassenaar.org/

Freshfields Bruckhaus Deringer: https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/china-rules-on-encryption/

