TRAVEL ADVICE BOOKLET

Going abroad with your telephone, tablet or laptop computer

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI

This travel advice booklet was initially produced by the Agence nationale de la sécurité des systèmes d'information (ANSSI),

in partnership with the Club des directeurs de sécurité d'entreprise (CDSE),

and with the help of the following ministries:

- the Ministry of Ecology, Energy, Sustainable development and the Sea;
- the Ministry of Foreign and European affairs;
- the Ministry of the Economy, Industry and Employment;
- the Ministry of the Interior, French overseas territories and Regional authorities;
- the Ministry of Research and Higher education;
- the Ministry of Defence,

and the following companies and organisations:

Areva, EADS, France Télécom, Michelin, Total, Technip and Cigref.

It was updated by ANSSI.

The use of connected telephones (or smartphones), laptop computers and tablets facilitates and accelerates the transport and exchange of data.

Amongst the information stored on these terminals, some may be highly sensitive, both for ourselves and for the administration or company to which we belong. Their loss, seizure or theft may have major consequences for our activities and their viability.

When roaming, we must therefore protect them from the risks and threats to which they are subject, particularly when travelling abroad.

This guide presents simple rules to be implemented, to reduce the risks and threats or limit their impact. We hope that it will contribute to helping travellers ensure the level of protection that their sensitive information deserves.

When travelling abroad, keep your information safe!

There are additional risks and threats to the security of the information that you carry or exchange, and particularly to its confidentiality.

Your equipment and data may arouse all sorts of envy and you must remain vigilant, in spite of the change of environment and the disorientation that this can cause.

Be aware that cyber cafes, hotels, public places and temporary offices provide no guarantee of confidentiality. In numerous foreign countries, whatever their political regime, business centres and telephone networks are monitored. In certain countries, hotel rooms may be searched without you noticing it.

These threats are not inspired by detective novels or spy films ; these things actually occur regularly.

The advice given in this booklet will let you familiarise yourself with the threats that are identified and know what to do.

Before leaving on your assignment

[1]

Carefully re-read and comply with the security rules laid down by your organisation.

Technical recommendations are available, for IT services and users, on the ANSSI's site [1]

1) *www.ssi.gouv.fr/en/*

[2]

Find out about the local legislation.

Information on border controls and the import and use of cryptography are available on the ANSSI's site [2].

Also, the site run by the Ministry of Foreign and European affairs gives general recommendations :
www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/

2) www.ssi.gouv.fr/en/

[3]

Preferably use equipment dedicated to assignments *(computers, smartphones and removable media such as hard disks and USB drives).*

These terminals should contain no information [3] other than what you need for the assignment.

3) *Including photos, videos or digital works that could get you into difficulties with the legislation or customs of the country visited.*

[4]

Backup the data that you are taking and leave the backup in a secure place.

You can therefore recover your information on your return in case of loss or theft or if your equipment is seized.

[5]

Avoid leaving with sensitive data.

If possible, prefer the recovery of encrypted files at the place of your assignment by accessing :

> your organisation's network via a secure link [4];

> or an online email box [5] specially created and dedicated to the transfer of encrypted data. The information in this box must be deleted when it is read.

---

4) *For example, with a VPN client put in place by your IT service.*

5) *It is imperative to configure your email to use the HTTPS protocol.*

[6]

Use a protective screen filter for your computer.

This will let you work on your files during your journeys without your documents being read or photographed over your shoulder by the curious.

[7]

Mark your terminals with a distinctive sign (such as a coloured dot).

This lets you monitor your equipment and make sure that there has been no swap, particularly during transport. Remember to also put a sign on the cover.

During the assignment

[1]

Keep your terminals, media and files with you.

Take them in the cabin during your journey. Never leave them in an office or in a hotel room (even in a safe).

[2]

Protect access to your terminals using strong passwords.

You will find recommendations on the ANSSI's site [6].

6) *http://www.ssi.gouv.fr/mots-de-passe*

[3]

Do not get separated from your equipment.

If you must do so, keep the SIM card with you and, if possible, the battery.

[4]

Use encryption software during the journey.

Do not communicate confidential information unencrypted by telephone or any other means of voice transmission (VoIP services such as Skype).

[5]

Remember to delete the history of your calls and your web browsing.

In addition to the history, you must delete the data left in the cache memory, cookies, passwords for access to websites and temporary files.

[6]

In case of inspection or seizure by the authorities, immediately inform your organisation.

Supply the passwords and encryption keys if you are required to do so by the local authorities, then alert your Information Systems department.

[7]

In case your equipment or information is lost or stolen, immediately inform your organisation.

Request advice from the consulate before any approach to the local authorities.

[8]

Do not use equipment that is given to you (USB drives). They may contain malicious software.

USB drives, due to their numerous vulnerabilities, are a preferred means of infection by attackers.

[9]

Do not connect your equipment to workstations or computer peripherals that are not trusted.

Beware of exchanges of documents (for example : by USB drive during marketing presentations or conferences). Take a USB drive intended for these exchanges and dispose of it after use.

[10]

Do not recharge your equipment on self-service electrical terminals.

Some of these terminals may have been designed to copy documents without your knowledge.

Before your return from your assignment

[1]

Transfer your data

> to your organisation's network using your secured connection ;
> otherwise use an online email box dedicated to receiving **encrypted files** (which will be deleted as soon as you return). Then delete them from your machine, if possible in a secure manner with software provided for this purpose.

[2]

Delete the history of your calls and your web browsing.

This concerns both your roaming terminals (tablet and telephone) and your computer.

After the assignment

[1]

Change all the passwords that you used during your journey.

They may have been intercepted without your knowledge.

[2]

Analyse your equipment or have it analysed.

Do not connect the terminals to your network before at least having an anti-virus and anti-spyware test performed.

You now have some good advice so that you can leave in complete safety…

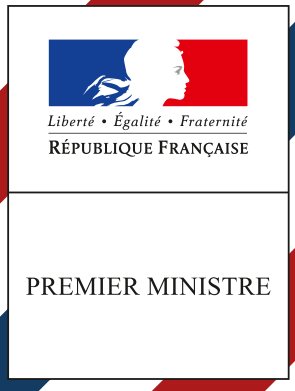
Enjoy your journey

You will find the latest version of this booklet on the ANSSI's Internet site :
www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs

Version 2.0 – Août 2014 / 20141020-1651

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75 700 PARIS 07 SP
www.ssi.gouv.fr / communication@ssi.gouv.fr


Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE