

DIGITAL SECURITY BEST PRACTICES FOR BUSINESS TRAVELLERS



In 2010, the "*Advice to travellers*" passport was published, drawing attention to the importance, in terms of digital security, of being (at least) as careful when travelling as when at your workstation. Since that time, in step with changing uses, the issues and threats posed by the development of new technologies and business practices have also evolved.

To best reflect the reality of all business travellers – whether this entails merely going round the corner from your office or heading abroad – we have designed this new version of the passport together with you: employees, entrepreneurs, manufacturers, NGO members, State officials and students among others. By sharing your experiences, queries and needs with us, you have helped us to produce a document that is fully in tune with today's practices. **Thank you to all of you!**

Through these best practices, which jointly address digital security and mobility – two key concerns for ANSSI, the National Cybersecurity Agency of France, and the Ministry for Europe and Foreign Affairs – we are seeking to remind all of you of your responsibility regarding the information your organisations entrust you with. We firmly believe that nurturing this security culture in the workplace also involves instilling or stepping up certain reflexes in citizens.

Hélène FARNAUD-DEFROMONT

Director-General for Administration and Modernisation
Senior Security and Defence Official
Ministry for Europe and Foreign Affairs

Guillaume POUPARD

Director-General of ANSSI, the National
Cybersecurity Agency of France

THE 9 BEST PRACTICES

BEFORE

DURING

AFTER

1

Don't transport
irrelevant data

2

Do find out about the
legislation of the country
you're going to

4

Do exercise
discretion

5

Don't leave your documents
and devices unattended

8

Do change the passwords
used during your trip

9

If in doubt, do have your
devices checked by
your security officer

AT A GLANCE

3

Do make backups of
any data you transport

6

Don't log on to unsecured
networks or devices

7

Do tell your security officer
in the event of loss or theft

BEFORE

Yann works for a PR agency and visits one of his clients to present a proposal. In a hurry, he takes a slideshow on a USB memory stick which also contains documents on other proposals in progress. One of these outlines his agency's response to the competitors of the client he's visiting. At the end of the presentation, Yann gives the USB memory stick to the client so that he can get a copy of the slideshow, and the client inadvertently copies across all of the contents – including the strategic and budgetary proposals meant for his competitors.



DON'T TRANSPORT IRRELEVANT DATA

- When you're travelling, minimise the risk of data loss or theft by storing only what data you strictly need on your mobile devices.
- Find out from your organisation's security officer what secure solutions are available (encrypted container, secure cloud, etc.).

Marc, an executive working for a multinational, is heading abroad to secure a major contract. To protect the resources he needs for this deal, he uses his organisation's usual encryption methods. On his arrival, Marc has to go through a heightened security check with the local authorities. Because he hadn't found out about the country's legislation regarding such methods, his devices are temporarily confiscated and he is ordered to disclose his passwords on the grounds that he hadn't applied for authorisation to bring such methods on to the territory.



DO FIND OUT ABOUT THE LEGISLATION OF THE COUNTRY YOU'RE GOING TO

- Find out from your legal department or security officer about the legislation of the country you're going to regarding encryption methods.
- Adapt the level of security covering the communication and storage devices you travel with to the local regulatory context and requirements of your assignment.

Plan your trip using the "Advice to Travellers" application of the Ministry for Europe and Foreign Affairs:

<https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatique-numerique/l-offre-de-service-public-en-ligne-du-ministere/>

Sofia runs an SME that makes bespoke furniture for its customers. Eager to go more up-market, she drives to one of her suppliers to present her strategy and budget. While she's taking a break at a motorway services station, her laptop, which was perched beside her, falls and gets seriously damaged on hitting the ground. On top of the tangible loss, Sofia also loses the documents she needs for this meeting as she didn't make a backup of them before the trip.



DO MAKE BACKUPS OF ANY DATA YOU TRANSPORT

- ▶ Backing up your data means you'll be able to recover it if an incident occurs (loss, theft, breakage, failure, etc.) on your devices.
- ▶ Making regular backups on a device, that is not connected to any network, supplied by your organisation, is an additional security measure.

DURING





10



Anne, a sales rep for a mobile phone company, is heading to an international exhibition to premier the brand's latest innovations. On the train to the exhibition venue, she adds the finishing touches to her presentation on her laptop without taking enough precautions against prying eyes. Someone sitting behind her decides to benefit from this lack of discretion and snoops at the content displayed on her screen. A few hours later, the announcement is leaked to the online press.



DO EXERCISE DISCRETION

- Where possible, don't consult sensitive documents in public spaces and do equip your devices (laptop, tablet, telephone) with a privacy filter.
- Online (photos, comments, tweets, etc.) or in public spaces, do assess your communications in light of the reasons for your assignment and your destination.

Mehdi is taking part in a working group that is meeting outside the association he works for. Emboldened by the sense of camaraderie between the participants and their common purpose, Mehdi decides to take a quick break and leaves the room without locking the user session on his laptop. Someone seizes on this brief absence to pass themselves off as Mehdi and uses his email account to send a hoax message to his contacts that not everyone might find funny.



DON'T LEAVE YOUR DOCUMENTS AND DEVICES UNATTENDED

- Whenever you leave your workstation, however briefly, always lock your user session.
- If you have no choice but to part with your devices and you want to secure them, security envelopes and anti-theft cables for laptops exist and provide a simple protection mechanism in most standard situations.

While away on business, Guillaume uses his hotel's network to check his personal email account as he had forwarded several messages to it about his current work projects. The network he logs on to is not very secure, and a vulnerability within it allows a virus to infect his computer.





DON'T LOG ON TO UNSECURED NETWORKS OR DEVICES

- Do use the secure corporate devices supplied by your organisation (telephone, laptop, VPN, etc.). Don't bypass them by using personal means (e.g.: personal email account).
- As far as possible don't log on to unsecured networks (hotel, train station or café Wi-Fi, free charging stations, external meeting rooms, etc.) and do keep your firewall enabled.
- Don't use devices you are given while on your trip (USB memory stick, connected device, etc.) without having had them checked by your security officer: they may have been bugged.

Myriam's company is sending her abroad on business. During a stopover, she loses her work mobile at the airport. On arriving at her destination, she decides to put off dealing with the problem until she gets back, and uses her personal mobile to tide her over. Only, in the meantime, a stranger finds her work mobile and can now consult the data it contains at his leisure.



DO TELL YOUR SECURITY OFFICER IN THE EVENT OF LOSS OR THEFT

- If one of your devices should go missing or start playing up, do notify your security officer immediately.
- S/he will advise you, depending on the context, about who to contact at your location or even which authority to report the loss to.
- In this way, s/he will immediately be able to take the necessary steps for protecting the organisation's cyber assets from malicious logins.

AFTER



For convenience's sake, Julie uses her personal mobile to log on to the open Wi-Fi network supplied by the organisers of the conference she's attending. While accessing her company's online portal, her login and password are intercepted by an adversary logged onto the same Wi-Fi network. Now the adversary can easily show off his exploit by orchestrating leaked information marked with the company's logo.



DO CHANGE THE PASSWORDS USED DURING YOUR TRIP

- In all circumstances and whenever your devices and applications allow, do opt for strong authentication (mobile app, USB memory stick, smart card, etc.).
- Do use a different password for each of your accounts and devices (email account, social media, workstation, mobile phone, etc.)
- Do give priority to changing the passwords used during the assignment if there's any doubt.

Pedro is going with some colleagues to a week-long congress organised in the south of France. During the trip, he notices unusual warning messages pop up on his laptop which seem to be slowing his browser down. But with so much on, Pedro only pays passing attention to them and does nothing to sort the problem out. When he gets back, he connects his laptop to his organisation's network, and all of the devices connected to the same network suddenly crash.



DO HAVE YOUR DEVICES CHECKED BY YOUR SECURITY OFFICER

On getting back from your assignment, give your devices to your security officer for checking:

- ▶ in the event of confiscation during your trip (by Border Police or an organisation's reception, etc.);
- ▶ if you have any doubts over the integrity of one of them.

APPENDICES

USEFUL CONTACTS

► **Security officer:**

Tel.:

E-mail:

► **Legal department:**

Tel.:

E-mail:

.....

.....

.....

.....

.....

.....

.....

USEFUL RESOURCES

- The "*Advice to Travellers*" application of the Ministry for Europe and Foreign Affairs —
www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatique-numerique/l-offre-de-service-public-en-ligne-du-ministere/
- Are you an individual, a business or a local authority and you think you've been targeted by cyber malicious activities?
Go to: www.cybermalveillance.gouv.fr.
- *IT Best Practice Guide*, ANSSI-CPME, 2017
www.ssi.gouv.fr/guide-bonnes-pratiques/
- *Guideline for a healthy information system in 42 measures*, ANSSI, 2017
www.ssi.gouv.fr/hygiene-informatique/
- *Recommendations on digital mobility*, ANSSI, 2018
www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

TOOL BOX

- **Security officer's contact details**
- **Clean USB memory stick**
- **USB portable charger**
- **Adapter**
- **Privacy filters:** protection that can be placed on device screens (laptop, mobile, tablet). These filters stop anyone not sitting directly in front of the screen (so trying to sneak a peek from the sides or top) from seeing what's on it.
- **Security envelope:** envelope or pouch with features (tamper-evident adhesive seal, unique numbering, etc.) which ensure the integrity and traceability of the documents enclosed. These can be obtained from certain organisations and employers or from specialist retailers.



In partnership with the Ministry
for Europe and Foreign Affairs

Version 1.0 – July 2019
ANSSI-GP-065-EN

Licence Ouverte/Open Licence (Etalab – V1)

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



