

SÉCURITÉ NUMÉRIQUE

BONNES PRATIQUES À L'USAGE DES PROFESSIONNELS EN DÉPLACEMENT



En 2010, le *Passeport de conseils aux voyageurs* voyait le jour. En matière de sécurité numérique, il attirait l'attention sur l'importance d'être (au moins) aussi prudent en déplacement qu'à son poste de travail. Depuis, les usages ont bien sûr évolué et, avec eux, les enjeux et menaces que draine le développement de nouvelles technologies et pratiques professionnelles.

Pour être au plus près de la réalité de celles et ceux qui sont amenés à se déplacer à deux pas de leur lieu de travail comme à l'étranger, nous avons conçu cette nouvelle version du passeport avec eux : salariés, entrepreneurs, industriels, membres d'ONG, agents de l'État, étudiants, etc. En partageant avec nous leurs expériences, leurs interrogations et leurs besoins, ils nous ont permis d'élaborer un document en prise directe avec les pratiques actuelles. **Merci à tous !**

À travers ces bonnes pratiques à la croisée des enjeux de sécurité numérique et de mobilité chers à l'ANSSI et au ministère de l'Europe et des Affaires étrangères, nous souhaitons rappeler la responsabilité de tous et toutes vis-à-vis des informations que leur confient leurs organisations d'appartenance. Développer cette culture de la sécurité en milieu professionnel, c'est aussi faire naître ou renforcer certains réflexes chez les citoyens, nous en sommes convaincus.

Hélène FARNAUD-DEFROMONT

Directrice générale de l'administration et de la modernisation
Haut Fonctionnaire de sécurité et de défense
Ministère de l'Europe et des Affaires étrangères

Guillaume POUPARD

Directeur général de l'Agence nationale
de la sécurité des systèmes d'information (ANSSI)

LES 9 BONNES PRATIQUES EN UN COUP D'ŒIL

AVANT

1

Évitez le transport de données superflues

2

Informez-vous sur la législation du pays de destination

3

Sauvegardez les données que vous emportez

PENDANT

4

Faites preuve de discrétion

5

Évitez de laisser vos documents et équipements sans surveillance

6

Évitez de vous connecter aux réseaux ou équipements non maîtrisés

7

Informez votre responsable de la sécurité en cas de perte ou de vol

APRÈS

8

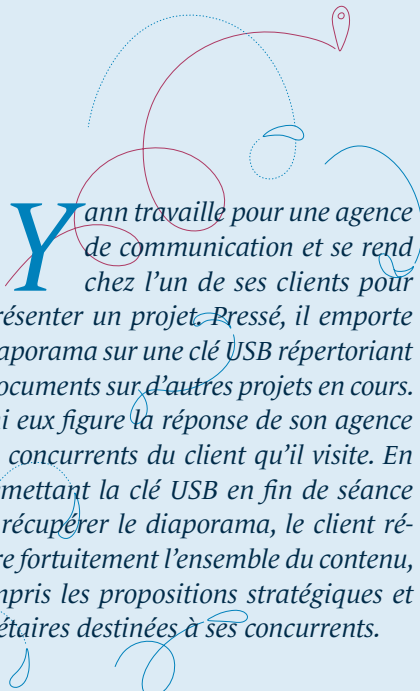
Renouvelez les mots de passe utilisés lors de votre déplacement

9

En cas de doute, faites vérifier vos équipements par votre responsable de la sécurité

The image features a solid dark blue background. The word "AVANT" is written in a bold, white, sans-serif font, oriented vertically in the center-left area. Surrounding the text are several decorative, flowing lines in a light yellow or gold color. Some of these lines are solid, while others are dashed, creating a sense of movement and elegance. The lines swirl and loop around the text and across the frame, with some extending towards the corners. The overall composition is minimalist and modern.

AVANT



Yann travaille pour une agence de communication et se rend chez l'un de ses clients pour lui présenter un projet. Pressé, il emporte un diaporama sur une clé USB répertoriant des documents sur d'autres projets en cours. Parmi eux figure la réponse de son agence à des concurrents du client qu'il visite. En lui remettant la clé USB en fin de séance pour récupérer le diaporama, le client récupère fortuitement l'ensemble du contenu, y compris les propositions stratégiques et budgétaires destinées à ses concurrents.



ÉVITEZ LE TRANSPORT DE DONNÉES SUPERFLUES

- Lors de vos déplacements, réduisez le risque de perte ou de vol de vos données en emportant le strict minimum sur vos équipements nomades.
- Renseignez-vous auprès du responsable de la sécurité de votre organisation sur les solutions sécurisées disponibles (conteneur chiffré, cloud sécurisé, etc.).

Marc, cadre dans une multinationale, se rend à l'étranger pour conclure un important contrat. Pour protéger les ressources utiles à cette transaction, il recourt aux moyens de chiffrement d'usage dans son organisation. Dès son arrivée, Marc est soumis à un contrôle renforcé par les autorités locales. Non renseigné sur la législation du pays vis-à-vis de ces moyens, ses équipements lui sont momentanément saisis et ses mots de passe demandés pour ne pas avoir formulé de demande d'autorisation pour introduire de tels moyens sur le territoire.



INFORMEZ-VOUS SUR LA LÉGISLATION DU PAYS DE DESTINATION

- Renseignez-vous auprès de votre service juridique ou de votre responsable de la sécurité sur la législation du pays de destination vis-à-vis des moyens de chiffrement.
- Adaptez la sécurisation des moyens de communication et de stockage que vous emportez au cadre réglementaire local et aux besoins de votre mission.

Préparez votre voyage avec l'application *Conseils aux Voyageurs* du ministère de l'Europe et des Affaires étrangères :

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

Sofia est à la tête d'une PME qui réalise pour ses clients du mobilier sur-mesure. Désireuse de monter en gamme, elle se rend en voiture chez l'un de ses fournisseurs pour lui présenter sa stratégie et son budget. Alors qu'elle se restaure sur une aire d'autoroute avec son ordinateur portable posé à côté d'elle, celui-ci tombe par terre et se retrouve sérieusement endommagé. En plus du préjudice matériel, Sofia vient ainsi de perdre les documents nécessaires à cet entretien puisqu'elle ne les avait pas préalablement sauvegardés.



SAUVEGARDEZ LES DONNÉES QUE VOUS EMPORTEZ

- La réalisation de sauvegardes garantit la récupération de vos données en cas d'incident (perte, vol, casse, panne, etc.) sur vos équipements.
- Réaliser des sauvegardes régulières sur un support déconnecté de tout réseau fourni par votre organisation constitue un gage de sécurité supplémentaire.



PENDANT



Commerciale dans une entreprise de téléphonie mobile, Anne va annoncer en avant-première les dernières innovations de la marque dans un salon international. Dans le train qui l'emmène vers le lieu de la manifestation, elle peaufine sa présentation sur son ordinateur sans se soucier d'éventuels regards indiscrets. Une personne installée derrière elle va pourtant profiter de ce manque de discrétion et observer le contenu affiché sur son écran. Quelques heures plus tard, l'annonce fuite dans la presse en ligne.



FAITES PREUVE DE DISCRÉTION

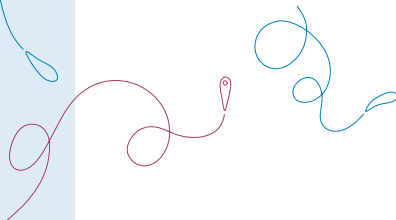
- Évitez autant que possible la consultation de documents sensibles depuis des lieux publics et dotez vos équipements (ordinateur, tablette, téléphone) d'un **filtre de confidentialité**.
- En ligne (photos, commentaires, tweets, etc.) ou dans les lieux publics, évaluez votre communication sur les raisons de votre mission ou votre destination.

Mehdi participe à un groupe de travail qui se réunit à l'extérieur de l'association pour laquelle il travaille. Mis en confiance par la bonne humeur qui règne entre les participants et l'objectif qui les rassemble, Mehdi profite d'un temps de pause et quitte la salle sans verrouiller la session de travail sur son ordinateur. Quelqu'un va profiter de cette courte absence pour se faire passer pour Mehdi en utilisant sa messagerie et en envoyant à ses contacts un mail à l'humour un peu douteux.



ÉVITEZ DE LAISSER VOS DOCUMENTS ET ÉQUIPEMENTS SANS SURVEILLANCE

- Lorsque vous vous absentez, même pendant un temps très court, verrouillez votre session de travail.
- Si vous êtes contraint de vous séparer de vos équipements et souhaitez préserver leur intégrité, des **enveloppes inviolables et câbles antivol** pour ordinateurs portables existent et constituent une parade simple dans la plupart des situations usuelles.



***E**n déplacement professionnel, Guillaume se connecte depuis le réseau de son hôtel pour consulter sa messagerie personnelle sur laquelle il a fait suivre plusieurs messages concernant les affaires en cours. Peu sécurisé, le réseau sur lequel il se connecte est porteur d'une vulnérabilité qui va permettre à un virus d'infecter son ordinateur.*



ÉVITEZ DE VOUS CONNECTER AUX RÉSEAUX OU ÉQUIPEMENTS NON MAÎTRISÉS

- Utilisez les moyens professionnels sécurisés fournis par votre organisation (téléphone, ordinateur, VPN, etc.). Ne les contournez pas par l'usage de moyens personnels (ex. : messagerie personnelle).
- Lorsque c'est possible, évitez de vous connecter aux réseaux non maîtrisés (Wi-Fi d'hôtel, de gare ou de café, bornes de recharge en libre-service, salle de réunion extérieure, etc.) et gardez votre pare-feu actif.
- N'utilisez pas les équipements qui vous sont offerts (clé USB, objet connecté, etc.) sans les avoir fait vérifier par votre responsable sécurité, ils peuvent avoir été piégés.

Myrïam entreprend un voyage d'affaires à l'étranger pour le compte de son entreprise. Lors d'une escale, elle égare dans l'aéroport son téléphone professionnel. Arrivée à destination, elle décide de traiter ce problème à son retour et utilise son téléphone personnel en guise de dépannage. Sauf qu'entre-temps, son téléphone est tombé entre les mains d'un inconnu qui peut désormais consulter à sa guise les données qui s'y trouvent.



INFORMEZ VOTRE RESPONSABLE DE LA SÉCURITÉ EN CAS DE PERTE OU DE VOL

- En cas de disparition de l'un de vos équipements ou de fonctionnement anormal, informez-en sans délai votre responsable de la sécurité.
- Il vous indiquera, selon le contexte, qui contacter sur place voire auprès de qui déposer plainte.
- Il pourra ainsi prendre sans délai les mesures nécessaires pour protéger de connexions malveillantes le patrimoine informationnel de l'organisation.



APRÈS



*P*ar commodité, Julie s'est connectée avec son téléphone personnel au réseau Wi-Fi ouvert proposé par les organisateurs de la conférence à laquelle elle assiste. En accédant au portail de son entreprise sur Internet, ses identifiant et mot de passe ont été interceptés par un attaquant connecté au même réseau Wi-Fi. Dès lors, il devient très facile pour un attaquant de faire étalage de son exploit en organisant la fuite d'informations marquées du logo de l'entreprise.



RENOUVELEZ LES MOTS DE PASSE UTILISÉS LORS DE VOTRE DÉPLACEMENT

- En toutes circonstances et lorsque vos équipements et applications le permettent, préférez l'authentification forte (application mobile, clé USB, carte à puce, etc.).
- Utilisez un mot de passe différent pour chacun de vos comptes et équipements (messageries, réseaux sociaux, poste de travail, téléphone mobile, etc.)
- Renouvelez en priorité les mots de passe utilisés pendant la mission et sur lesquels pèsent un doute.



Avec plusieurs collègues, Pedro assiste à un congrès d'une semaine organisé dans le sud de la France. Au cours de son séjour, il constate l'apparition sur son ordinateur portable de messages d'alerte inhabituels qui semblent ralentir sa navigation. Occupé, il n'y prête qu'une faible attention et n'entreprend rien pour résoudre ce problème. À son retour, il connecte son ordinateur au réseau de son organisation et immédiatement, l'ensemble des équipements reliés à ce même réseau tombe en panne.



FAITES VÉRIFIER VOS ÉQUIPEMENTS PAR VOTRE RESPONSABLE DE LA SÉCURITÉ

À votre retour de mission, confiez vos équipements à votre responsable de la sécurité :

- en cas de saisie de ceux-ci (Police aux frontières, accueil d'une organisation, etc.) durant votre déplacement ;
- Si vous avez des doutes sur l'intégrité de l'un d'eux.

ANNEXES

CONTACTS UTILES

■ Responsable de la sécurité:

Tél.:

E-mail:

■ Service juridique:

Tél.:

E-mail:

■

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

RESSOURCES UTILES

■ L'application *Conseils aux Voyageurs* du ministère de l'Europe et des Affaires étrangères www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/l-offre-de-service-public-en-ligne-du-ministere/

■ Vous êtes un particulier, une entreprise ou une collectivité territoriale et vous pensez être victime d'un acte de cybermalveillance ?

Rendez-vous sur: www.cybermalveillance.gouv.fr.

■ *Guide des bonnes pratiques de l'informatique*, ANSSI-CPME, 2017

www.ssi.gouv.fr/guide-bonnes-pratiques/

■ *Guide d'hygiène informatique*, ANSSI, 2017

www.ssi.gouv.fr/hygiene-informatique/

■ *Recommandations sur le nomadisme numérique*, ANSSI, 2018

www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

BOÎTE À OUTILS

- **Coordonnées du responsable de la sécurité**
- **Clé USB vierge**
- **Batterie USB**
- **Adaptateur**
- **Filtres de confidentialité** : protection que l'on place sur l'écran de ses équipements (ordinateur, téléphone, tablette). Un tel filtre a pour effet d'empêcher quiconque se situerait en dehors du champ de vision « utilisateur » de voir ce qui apparaît à l'écran.
- **Enveloppe inviolable** : enveloppe ou pochette dont les propriétés (adhésif inviolable, numéro unique, etc.) assurent l'intégrité et la traçabilité des documents qu'elle contient. Il est possible de s'en procurer auprès de certaines organisations et employeurs ou dans le commerce.



En partenariat avec
le ministère de l'Europe
et des Affaires étrangères

Version 1.0 – Mai 2019
20190517-1715

.....
Licence Ouverte/Open Licence (Étalab – 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





Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

