Partir en mission à l'étranger avec son téléphone mobile, son assistant personnel ou son ordinateur portable.

PASSEPORT DE CONSEILS AUX VOYAGEURS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Agence Nationale de la Sécurité des Systèmes d'Information

L'emploi de téléphones mobiles, d'ordinateurs portables et d'assistants personnels a favorisé le transport et l'échange de données.

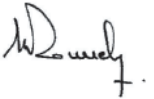
Parmi ces informations, certaines peuvent présenter une sensibilité importante, tant pour nous-mêmes que pour l'administration ou l'entreprise à laquelle nous appartenons. Leur perte, leur saisie ou leur vol peut avoir des conséquences importantes sur nos activités et sur leur pérennité.

Il nous faut donc, dans ce contexte de nomadisme, les protéger face aux risques et aux menaces qui pèsent sur elles, tout particulièrement lors de nos déplacements à l'étranger.

Ce guide présente des règles simples à mettre en œuvre pour réduire les risques et les menaces, ou en limiter l'impact.

Nous espérons qu'il contribuera à aider les voyageurs à assurer le meilleur niveau de protection que méritent leurs informations sensibles.

Patrick PAILLOUX
Directeur général de l'agence nationale de la sécurité des systèmes d'information



François ROUSSELY
Président du club des directeurs de sécurité des entreprises

Lors de vos déplacements à l'étranger, veillez à la sécurité de vos informations !

Des risques et des menaces supplémentaires pèsent en effet sur la sécurité des informations que vous emportez ou que vous échangez, et notamment sur leur confidentialité.

Vos équipements et vos données peuvent attirer des convoitises de toute sorte, et il vous faut rester vigilant, malgré le changement d'environnement et la perte de repères qu'il peut provoquer.

Sachez que les cybercafés, les hôtels, les lieux publics et parfois même les bureaux de passage n'offrent pas de garantie de confidentialité. Dans de nombreux pays étrangers, les centres d'affaires et les réseaux téléphoniques sont surveillés. Dans certains, les chambres d'hôtel peuvent être fouillées.

Pour couvrir l'ensemble de ces menaces potentielles auxquelles vous pouvez être confronté, nous vous invitons à suivre les conseils exposés dans ce passeport.

Avant de partir en mission :

1) Relisez attentivement et respectez les règles de sécurité édictées par votre organisme.

Des recommandations techniques sont disponibles, pour les services informatiques et les utilisateurs avertis, sur le site de l'ANSSI[1].

2) Prenez connaissance de la législation locale.

Des informations sur les contrôles aux frontières et sur l'importation ou l'utilisation de la cryptographie sont disponibles sur le site de l'ANSSI[1].

Par ailleurs, le site du ministère des affaires étrangères et européennes donne des recommandations générales :
www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs_909/

3) Utilisez de préférence du matériel dédié aux missions (ordinateurs, téléphones, supports amovibles, etc.).

Ces appareils ne doivent contenir aucune information[2] autre que celles dont vous avez besoin pour la mission.

[1] www.securite-informatique.gouv.fr/partirenmission/

[2] Y compris des photos, vidéos, ou des œuvres numériques qui pourraient vous placer en difficulté vis-à-vis de la législation ou des mœurs du pays visité.

4) Sauvegardez les données que vous emportez.
Vous récupérerez ainsi vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements.

5) Evitez de partir avec vos données sensibles.
Privilégiez, si possible, la récupération de fichiers chiffrés sur votre lieu de mission en accédant :
- au réseau de votre organisme avec une liaison sécurisée[3] ;
- sinon à une boîte de messagerie en ligne[4] spécialement créée et dédiée au transfert de données chiffrées et en supprimant les informations de cette boite après lecture.

6) Emportez un filtre de protection écran pour votre ordinateur si vous comptez profiter des trajets pour travailler vos dossiers, afin d'éviter que des curieux lisent vos documents par-dessus votre épaule.

7) Mettez un signe distinctif sur vos appareils (comme une pastille de couleur).
Cela vous permet de pouvoir surveiller votre matériel et de vous assurer qu'il n'y a pas eu d'échange, notamment pendant le transport. Pensez à mettre un signe également sur la housse.

[3] Par exemple avec un client VPN mis en place par votre service informatique.
[4] Paramétrez si possible votre messagerie pour utiliser le protocole HTTPS.

Pendant la mission :

1) Gardez vos appareils, support et fichiers avec vous !

Prenez-les en cabine lors de votre voyage. Ne les laissez pas dans un bureau ou dans la chambre d'hôtel (même dans un coffre).

2) Si vous êtes contraint de vous séparer de votre téléphone portable ou de votre PDA, retirez et conservez avec vous la carte SIM ainsi que la batterie.

3) Utilisez un logiciel de chiffrement pendant le voyage.

Ne communiquez pas d'information confidentielle en clair sur votre téléphone mobile ou tout autre moyen de transmission de la voix.

4) Pensez à effacer l'historique de vos appels et de vos navigations (données en mémoire cache, cookies, mot de passe d'accès aux sites web et fichiers temporaires).

5) En cas d'inspection ou de saisie par les autorités, informez votre organisme.

Fournissez les mots de passe et clés de chiffrement, si vous y êtes contraint par les autorités locales.

6) En cas de perte ou de vol d'un équipement ou d'informations, informez immédiatement votre organisme et demandez conseil au consulat avant toute démarche auprès des autorités locales.

7) N'utilisez pas les équipements qui vous sont offerts avant de les avoir fait vérifier par votre service de sécurité. Ils peuvent contenir des logiciels malveillants.

8) Evitez de connecter vos équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance.

Attention aux échanges de documents (par exemple : par clé USB lors de présentations commerciales ou lors de colloques). Emportez une clé destinée à ces échanges et effacez les fichiers, de préférence avec un logiciel d'effacement sécurisé.

Avant votre retour de mission :

1) Transférez vos données

- sur le réseau de votre organisme à l'aide de votre connexion sécurisée ;
- sinon sur une boite de messagerie en ligne dédiée à recevoir vos **fichiers chiffrés** (qui seront supprimés dès votre retour).

Puis effacez les ensuite de votre machine, si possible de façon sécurisée, avec un logiciel prévu à cet effet.

2) Effacez votre historique de vos appels et de vos navigations

Après la mission, tout particulièrement si votre équipement a échappé à votre surveillance :

1) Changez les mots de passe que vous avez utilisés pendant votre voyage.

2) Analysez ou faites analyser vos équipements[5].
Ne connectez pas les appareils à votre réseau avant d'avoir fait au minimum un test anti-virus et anti-espiogiciels.

[5] Une fiche technique, pour les utilisateurs avertis ainsi que les administrateurs systèmes, est disponible sur le portail de la sécurité informatique à l'adresse suivante :
www.securite-informatique.gouv.fr/gp_article636.html

Vous disposez maintenant des bons bagages pour partir en toute sécurité…

Bon voyage

Vous trouverez la dernière version de ce passeport sur le site internet de l'ANSSI :
http://www.securite-informatique.gouv.fr/partirenmission/

Ce passeport de conseils aux voyageurs a été réalisé par l'*agence nationale de la sécurité des systèmes d'information* (ANSSI)

en partenariat avec
- le *club des directeurs de sécurité d'entreprise* (CDSE) ;

et avec le concours des ministères suivants :
- ministère de l'écologie, de l'énergie, du développement durable et de la mer ;
- ministère des affaires étrangères et européennes ;
- ministère de l'économie, de l'industrie et de l'emploi ;
- ministère de l'intérieur, de l'outre-mer et des collectivités territoriales ;
- ministère de l'enseignement supérieur et de la recherche ;
- ministère de la défense ;

et des sociétés et organismes suivants :

AREVA EADS France Telecom

MICHELIN TOTAL Technip CIGREF

Janvier 2010

Agence nationale de la sécurité des systèmes d'information

ANSSI, SGDSN, 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr