A+ A-

Entreprises : comment protéger vos données sensibles lors de vos déplacements à l'étranger ?

Par **Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous>** , le 16/03/2022 - **Sécurité numérique**

Vos salariés se déplacent à l'étranger dans le cadre de leurs activités professionnelles ? Attention aux données sensibles sur leurs ordinateurs, tablettes et smartphones ! L'Agence nationale de la sécurité des systèmes d'information (ANSSI) met à disposition un livret des bonnes pratiques pour aider les entreprises et leurs salariés à protéger leurs données sensibles lorsqu'ils sont à l'étranger.

Dans l'ordinateur, tablette ou smartphone, vos salariés transportent peut-être des données confidentielles sur votre entreprise. Ces données sont vulnérables et pourraient être facilement dérobées ou dupliquées. Voici nos 10 conseils (liste non exhaustive) à appliquer et à relayer à vos salariés lors des voyages à l'étranger.

Que faire avant de partir en mission à l'étranger ?

Évitez de transporter des données superflues et sensibles

Il est préférable que les appareils (ordinateurs, tablettes, smartphones, disques durs, clés USB) utilisés pendant le voyage soient des **appareils dédiés à la mission**, qui **ne contiennent pas d'autres fichiers confidentiels**.

L'ANSSI préconise même de ne **rien stocker sur ces appareils** et de plutôt privilégier la récupération de fichiers chiffrés sur le lieu de mission via deux options :

- l'accès au réseau de l'organisme avec une liaison sécurisée
- la création d'une boîte de messagerie en ligne spécialement créée et dédiée au transfert de données chiffrées. Notez que les informations de cette boîte devront être supprimées après lecture.

Renseignez-vous sur la législation locale

Il serait dommageable que les appareils emportées (ordinateurs, tablettes, smartphones, disques durs, clés USB) soient bloqués et/ou vérifiés par les autorités locales lors des contrôles aux frontières.

C'est pourquoi il est conseillé de se **renseigner sur la législation locale applicable** concernant les contrôles aux frontières du matériel informatique et sur l'importation ou l'utilisation de la cryptographie.

Vous pouvez consulter ces informations en vous rendant sur le site de l'**ANSSI < https://www.ssi.gouv.fr/>** .

Sauvegardez les données que vous emportez

En cas de perte, de vol ou de saisie de vos équipements, vos données seront définitivement perdues.

C'est pourquoi il est conseillé de les **sauvegarder avant le voyage**, et de les conserver dans un lieu sécurisé pour les récupérer en cas de problème.

Créez un mot de passe fort et chiffrez vos données

Afin de bien protéger vos données sur votre appareil, **créez un mot de passe fort et sécurisé**.

Que faire pendant la mission à l'étranger ?

Surveillez vos équipements

Il s'agit d'un conseil de bon sens, mais **surveillez attentivement vos appareils** et gardez-les près de vous afin d'éviter un vol.

N'utilisez pas des appareils qui vous ont été offerts

N'utilisez pas les appareils qui vous ont été offerts (tablette, ordinateur, clé USB, etc.) : ils peuvent contenir des logiciels malveillants.

Pour les mêmes raisons, **ne connectez pas vos appareils sur des postes informatiques dont vous n'êtes pas sûr**. L'accès à internet dans les cybercafés, les hôtels ou les lieux publics ne garantit aucune confidentialité. Donc soyez vigilant lorsque vous vous connectez.

De même ne rechargez pas vos équipements dans les bornes électriques libre-service. Ce type de borne peut copier vos données.

En cas de perte ou de vol de vos équipements, informez votre responsable sécurité

En cas de perte, vol ou saisie par les autorités d'un équipement, **informez immédiatement le responsable de la sécurité informatique** de votre entreprise.

De même, vous pouvez vous rapprocher du **consulat français < https://www.diplomatie.gouv.fr/fr/le-ministere-et-son-reseau/annuaires-du-ministere-de-l-europe-et-des-affaires-etrangeres/ambassades-et-consulats-francais-a-l-etranger/>** avant d'entamer toute démarche auprès des autorités locales

Que faire après la mission à l'étranger ?

Modifiez les mots de passe

Comme indiqué plus haut dans cet article, il est conseillé de changer les mots de passe avant la mission.

Pensez à les modifier de nouveau à votre à votre retour en France, car ils pourraient avoir été interceptés à votre insu.

Faites analyser vos équipements

À ce titre, l'ANSSI conseille de ne connecter aucun appareil au réseau de l'entreprise **avant d'avoir fait ou fait faire au minimum un test anti-virus et anti logiciel-espion**.

Ces contenus peuvent aussi vous intéresser

Entreprises : quelles règles de cybersécurité appliquer ?
Sécurité de vos données : quelles sont les méthodes de piratage les plus courantes ?
Comment lutter contre les spams ?
Cinq conseils pour se prémunir contre les « rançongiciels » (ransomware)
Entreprises : faites attention aux tentatives d'escroqueries !

En savoir plus sur les bonnes pratiques pour les

déplacements à l'étranger

Bonnes pratiques à l'usage des professionnels en déplacement < https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/> *sur le site de l'ANSSI*

Partir à l'étranger avec son téléphone, sa tablette ou son ordinateur portable < https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf?v=1647428178> [PDF ; 1,64 Mo] *sur le site de l'ANSSI*

Thématiques : **Sécurité numérique**