PASSEPORT DE CONSEILS AUX VOYAGEURS

Se déplacer ou partir à l'étranger avec son téléphone, sa tablette ou son ordinateur portable

24 rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 24 93
amsn@gouv.mc

Département de l'Intérieur

1. Préambule.

L'emploi de téléphones connectés (ou ordiphones/smartphones), d'ordinateurs portables et de tablettes facilite et accélère le transport et l'échange de données.

Parmi les informations stockées sur ces supports, 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 majeures 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 lors de nos déplacements quotidien et plus 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 vous aider à assurer le niveau de protection que méritent vos informations sensibles.

2. Lors de vos déplacements, veillez à la sécurité de vos informations !

Des risques et des menaces supplémentaires pèsent 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, dans tous les environnements et à l'étranger le changement d'environnement est accentué par la perte des repères.

Sachez que les cybercafés, les hôtels, les lieux publics, les transports et les bureaux de passage n'offrent aucune garantie de confidentialité.

Dans de nombreux pays étrangers, quel que soit leur régime politique, les centres d'affaires et les réseaux téléphoniques sont surveillés. Dans certains pays, les chambres d'hôtel peuvent être fouillées sans que vous vous en rendiez compte.

Ces menaces ne sont pas inspirées de romans policiers ou d'un film d'espionnage ; mais attestées régulièrement par l'actualité.

Les conseils exposés dans ce passeport vous permettront de vous familiariser avec les menaces identifiées, et de savoir quelles réponses apporter.

3. Avant de partir en déplacement.

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

Si elles n'existent pas, n'hésitez pas à demander conseil à l'AMSN.

3.2. Prenez connaissance de la législation locale.

Les contrôles aux frontières et les règles d'importation ou l'utilisation de la cryptographie sont différents suivant les pays. Renseignez-vous auprès des ambassades, consulats, vos correspondants sur place, ….

3.3. Utilisez de préférence du matériel dédié aux missions (ordinateurs, ordiphones, supports amovibles tels que les disques durs sécurisés et clés USB sécurisées).

Lors des déplacements à l'étranger, ces appareils ne doivent contenir aucune information autre que celles dont vous avez besoin pour votre déplacement ou mission.

A l'étranger : attention aux photos, vidéos, ou œuvres numériques qui pourraient vous placer en difficulté vis-à-vis de la législation ou des mœurs du pays visité.

3.4. Sauvegardez les données que vous emportez et laissez la sauvegarde en lieu sûr.

Vous récupérerez ainsi vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements. Dans le cas où la sauvegarde est compliquée ou impossible, ne stockez pas de données sensibles sur votre matériel.

3.5. Évitez de partir avec des 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 (par exemple avec un client VPN sécurisé mis en place par votre service informatique) ;
- sinon à une boîte de messagerie en ligne (paramétrez impérativement votre messagerie pour utiliser le protocole HTTPS) spécialement créée et dédiée au transfert de données chiffrées. Il faut supprimer les informations de cette boîte après lecture.

3.6. Utilisez un filtre de protection écran pour votre ordinateur.

Cela vous permettra de travailler à vos dossiers pendant vos trajets sans que des curieux puissent lire ou photographier vos documents par-dessus votre épaule.

3.7. Marquez vos appareils d'un signe distinctif (comme une pastille de couleur).

Cela vous permet de 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.

4. Pendant le déplacement.

4.1. Gardez vos appareils, support et fichiers avec vous.

Prenez-les en cabine lors de votre voyage. Ne les laissez jamais dans un bureau, dans un coffre à bagages sans surveillance ou dans la chambre d'hôtel (même dans un coffre).

4.2. Protégez l'accès de vos appareils par des mots de passe forts.

Vous trouverez des recommandations auprès de l'AMSN.

4.3. Ne vous séparez pas de vos équipements.

Si vous devez vous en séparer, conservez avec vous la carte SIM ainsi que la batterie, si possible.

4.4. Utilisez un logiciel de chiffrement pendant le voyage.

Ne communiquez pas d'information confidentielle en clair par téléphone ou tout autre moyen de transmission de la voix (services de voix sur IP comme Skype). L'AMSN peut vous recommander des chiffrements.

4.5. Pensez à effacer l'historique de vos appels et de vos navigations.

Outre l'historique, il faut effacer les données laissées en mémoire cache, les cookies qui ne gèrent pas votre profil, mot de passe d'accès aux sites web et fichiers temporaires. L'AMSN publiera un guide pour faire cette action.

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

Fournissez les mots de passe et clés de chiffrement si vous y êtes contraint par les autorités locales puis alertez votre responsable de sécurité informatique et vos autorités.

4.7. En cas de perte ou de vol d'un équipement ou d'informations, informez immédiatement votre organisme.

Demandez conseil à votre consulat avant toute démarche auprès des autorités locales

4.8. N'utilisez pas les équipements qui vous sont offerts (clés USB, chargeur, accus supplétif). Ils peuvent contenir des logiciels malveillants.

Les clés USB, de par leurs multiples vulnérabilités, sont un vecteur d'infection privilégié par les attaquants.

4.9. Ne connectez pas 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 jetez la après usage.

4.10. Ne rechargez pas vos équipements sur les bornes électriques libre-service.

Certaines de ces bornes peuvent avoir été conçues pour copier les documents à votre insu.

5. Avant votre retour de mission.

5.1. Transférez vos données avant de passer les contrôles de sécurité.

- sur le réseau de votre organisme à l'aide de votre connexion sécurisée ;

- sinon sur une boîte 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.

5.2. Effacez l'historique de vos appels et de vos navigations.

Cela concerne aussi bien vos appareils nomades (tablette, téléphone) que votre ordinateur.

6. Après la mission.

6.1. Changez tous les mots de passe que vous avez utilisés pendant votre voyage.

Ils peuvent avoir été interceptés à votre insu

6.2. Analysez ou faites analyser vos équipements.

Ne connectez pas vos PC à votre réseau avant d'avoir fait ou fait faire par votre service informatique un test anti-virus et anti-espiogiciels. Si cela est possible faites-le aussi pour vos Smartphone sinon évitez de les connecter.

Vous disposez maintenant des bons bagages pour vous déplacer et partir en voyage ou en mission en toute sécurité.

L'AMSN vous souhaite bon déplacement ou bon voyage.

Ce passeport de conseils aux voyageurs a été initialement réalisé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) française,

Son adaptation à la Principauté de Monaco a été réalisée par l'Agence Monégasque de Sécurité Numérique (AMSN).

Agence Monégasque de Sécurité Numérique
Courriel : amsn@gouv.mc - Téléphone : 98 98 24 93