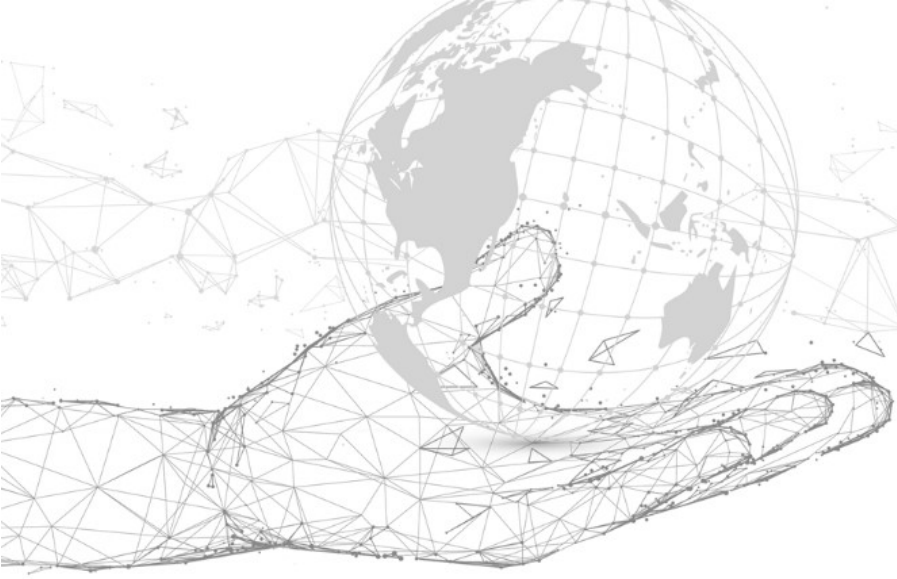

efcse.eu

FRANCE - VADE MECUM : MOBILITÉ ET CYBERSECURITÉ

Guide des bonnes pratiques numériques en déplacement

Auteurs : Olivier de MAISON ROUGE, Vice-President EFCSE, Avocat et Philippe MUELLER FEUGA, Expert
Juin 2018

PREAMBULE

Parce que l'humain doit être placé au cœur des préoccupations et des questions de sécurité numérique dès lors qu'il est souvent son point d'entrée le plus vulnérable,

Parce que les cadres et salariés constituent les forces vives de l'entreprise et le moteur de l'économie réelle,

Parce que l'internationalisation des échanges impose une grande mobilité des acteurs accentuant d'autant les risques pour les données et leurs supports,

Parce que la transformation numérique introduit la flexibilité et la mobilité de ses acteurs, tandis que la chaîne de valeur de gouvernance des données doit être respectée.

La cybersécurité, dans le cadre de la mobilité des acteurs de l'entreprise, est donc une exigence majeure pour la pérennité et la résilience des activités économiques.

C'EST POURQUOI, l'European Federation of CyberSecurity Experts a élaboré ce vade mecum des 10 bonnes attitudes en déplacement à diffuser au sein de chaque structure économique et humaine tournée vers l'ouverture au monde.

AVANT VOTRE DÉPART

1. ANTICIPER SUR L'ENVIRONNEMENT GÉOGRAPHIQUE et le contexte politique : les risques varient selon la région ou le pays de la mission : risques humains (santé) et risques professionnels (sécurité). Chaque secteur géographique doit être considéré comme étant une source de menaces pluridimensionnelles (politiques, économiques, naturels, criminels…) pour des cibles potentielles vulnérables à des degrés divers. Il convient dès lors de se renseigner au préalable, avant tout déplacement sur les risques éventuels auxquels le voyageur est susceptibles d'être confronté et obtenir le cas échéant les autorisations nécessaires.

Une veille auprès des services dédiés s'impose [FRANCE]: Gouvernement français : http://www.gouvernement.fr/risques/preparer-son-voyage-a-l-etranger ANSSI : www.ssi.gouv.fr , Ministère des affaires étrangères, et son site France Diplomatie : www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs

2. SE CONFORMER A LA REGLEMENTATION LOCALE en vigueur : l'effort de sécurité impose de respecter les législations en vigueur du pays d'accueil en matière de données sensibles, données personnelles, chiffrement … Vous devez les connaître en amont afin de ne pas vous faire confisquer vos supports et les données qu'ils contiennent.

Une recension règlementaire doit avoir été réalisée en amont auprès des acteurs cités ci-dessus, outre les Ambassades et consulats.

3. BIEN SELECTIONNER ou TERMINAUX NUMÉRIQUES que vous décidez d'emporter, et limiter LEURS CONTENUS (data) : inutile d'avoir avec vous votre ordinateur habituel contenant l'ensemble des données courantes (fichiers, tableaux, photos, vidéos, …). De préférence, utilisez un matériel configuré par votre DSI[1] ou RSSI[2] et strictement dédié à la mission.

Privilégiez l'utilisation de supports dédiés pour les déplacements (ordinateurs, tablettes), dûment expurgés de données non essentielles à la mission extérieure. Téléchargez à l'arrivée les données nécessaires (cf. « pendant votre déplacement »).

[1] DSI : Directeur du Système d'Information
[22] RSSI : Responsable de la Sécurité du Système d'Information

4. FAIRE UNE SAUVEGARDE préalable des données emportées : une copie sera toujours exploitable à votre retour en cas d'incident intervenu durant votre déplacement (suppression, confiscation, vol, …).

Conservez toujours les données originales sur un autre support qui restera dans vos locaux professionnels.

5. MARQUEZ vos supports : procédez à un marquage de vos supports numériques (ordinateurs, tablettes, smartphones) de manière à les rendre immédiatement identifiables par rapports aux autres. Changez vos mots de passe en les complexifiant.

Personnalisez vos supports numériques pour mieux les distinguer.

PENDANT VOTRE DÉPLACEMENT

1. MASQUEZ vos appareils : évitez les regards fortuits ou appuyés sur vos écrans. En cas d'usage dans les zones publiques (centres d'affaires, transports, …) utilisez les masques appropriés (filtres) pour empêcher à votre voisin de prendre connaissance des informations apparaissant à l'écran.

Utilisez des filtres rendant impossible la lecture pour les tiers.

2. CONSERVEZ vos supports numériques avec vous : gardez les en votre possession en toute occasion. Ne les laissez pas dans votre valise.

En cas de confiscation par les autorités, conservez les supports périphériques : clef USB, carte SIM, carte mémoire, …

3. N'UTILISEZ JAMAIS les supports et périphériques qui vous sont proposés : tout accessoire peut être vérolé (suppression de vos données) ou contenir un cheval de Troie (intrusion) ou un malware.

N'utilisez que vos supports périphériques (USB), dûment identifiés.

4. APPLIQUER les règles essentielles de travail et connexion à distance et/ou en déplacement : éviter l'usage des plateformes de partage et les moyens de connexion publics. Ne transférer que les fichiers utiles. Utilisez les canaux cryptés. recourir au chiffrement des données stratégiques ou sensibles. Ne vous connectez pas aux supports non fiables.

Restez vigilant en permanence sur l'utilisation des outils numériques : connexion, transferts, …

5. A votre retour, AVANT DE VOUS CONNECTER, veillez à INSPECTER vos supports numériques : effacez les historiques, supprimez les cookies, faites analyser vos supports et accessoires, le cas échéant, modifiez les codes d'accès. Soumettez les clés ou autre support remis à votre DSI ou RSSI pour un nettoyage. Eventuellement, faire une note d'évaluation pour votre DSI ou RSSI afin de mettre à jour les informations sur le pays de la mission.

Assurez-vous d'utiliser des supports sains.

Extrait du manifeste de l'EFCSE :

> « *La cyber sécurité n'est certes pas une préoccupation nouvelle. En revanche, la prise en considération des risques numériques appelle à un devoir constant de vigilance et de remise en cause. Elle met en exergue le besoin d'innovation permanente pour les organismes, les institutions et les entreprises concernées par les atteintes à leurs informations essentielles. Il leur appartient de parer chaque jour de nouvelles attaques et de nouveaux modes d'ingénierie, lesquels sont désormais multidimensionnels.*
>
> *Le cyber espace, ouvert au grand public depuis plus de vingt ans désormais, est un monde d'échanges de données – constituant le support originel de ces flux constants – un lieu de communication à l'échelle planétaire et un vaste champ dématérialisé.*
>
> *Mais indépendamment de ces immenses territoires largement ouverts, les menaces sont proportionnelles et affectent toute forteresse, dont aucune n'est imprenable.* »