TRAVEL SECURITY

COMMENT SE PROTÉGER ET PROTÉGER SES DONNÉES À L'ÉTRANGER

SECURITY PASSPORT

À QUI CE DOCUMENT EST-IL DESTINÉ ?

Cette brochure contient une série de conseils utiles pour toute personne ou organisation qui souhaite optimiser la sécurité de ses données lors de déplacements à l'étranger.

Les conseils fournis n'offrent cependant pas de garantie absolue. Il reste en effet de la responsabilité de chacun de veiller à sécuriser au mieux ses propres données et celles de son organisation.

RISQUES ACCRUS À L'ÉTRANGER

Voyager à l'étranger est devenu pratique courante, à tel point que **nous oublions souvent les risques auxquels nous nous exposons** : accident, perte de données, vol ou espionnage. Personne n'est à l'abri.

Le voyageur est vulnérable. Il se déplace en emportant des données ou du matériel de son organisation ou de son pays. Pour les criminels, mais aussi les services de renseignement étrangers et d'autres personnes ou organisations, il s'agit là d'une opportunité. Vous intéressez probablement les services de renseignement étrangers plus que vous ne le pensez, notamment pour les connaissances

que vous avez emportées avec vous ou auxquelles vous avez accès par voie numérique.

Ne sous-estimez pas les risques : pertes de réputation ou financières, poursuites ou sanctions, incidents diplomatiques ou politiques, etc. Les conséquences peuvent se révéler (très) lourdes tant pour vous que pour votre organisation.

Ce document vous propose des conseils pour **chacune des trois étapes d'un voyage** : avant le départ, pendant le voyage et au retour.

Les risques ne sont pas identiques dans tous les pays. Les conseils prodigués ne s'appliquent donc pas nécessairement à chacun de vos voyages ou déplacements. Il vous appartient au final d'évaluer correctement les risques potentiels.

COMMENT SE PROTÉGER ?

Choisissez les conseils qui correspondent à vos besoins et au niveau de risque de votre déplacement.

3 NIVEAUX DE RECOMMANDATIONS

BASIC
Protection minimale requise pour tout déplacement.

MEDIUM
Mesures supplémentaires pour une meilleure protection de vos données personnelles et celles de votre organisation.

HIGH
Mesures les plus strictes, valables pour les voyages en dehors de l'Union européenne ou si vous emportez des informations sensibles.

Les recommandations des différents niveaux sont cumulatives.

3 ÉTAPES

AVANT LE DÉPART

Une préparation minutieuse est essentielle pour limiter les risques. Dans quel objectif ? Limiter le nombre de documents et de supports de stockage (ordinateurs portables, smartphones, clés USB, etc.) et sécuriser correctement le matériel. Avant de partir, posez-vous toujours les questions

suivantes :

- En ai-je réellement besoin?
- Quelle est la valeur des informations que j'emporte ?
- Quel est l'impact d'une utilisation inappropriée de ces informations ?
- Quels appareils vais-je emporter et à quelles informations donnent-ils accès ?

PENDANT LE VOYAGE

Pour un voyageur averti, prudence et discrétion sont les maîtres-mots. Agissez avec circonspection face à d'autres personnes et gardez le contrôle permanent sur vos informations.

AU RETOUR

Certaines menaces peuvent persister, y compris à votre retour. Au moindre doute, faites vérifier vos supports de stockage et rapportez tout incident à votre responsable de la sécurité.

AVANT LE DÉPART

1. Informez-vous sur votre destination

Renseignez-vous sur **la situation politique, économique et sociale de votre lieu de destination.** Vous trouverez des informations utiles à ce sujet sur la page « Conseils aux voyageurs » du site web du SPF Affaires étrangères : **https://diplomatie.belgium.be**.

Enregistrez-vous également sur le site travellersonline.diplomatie.be. Le SPF Affaires étrangères pourra ainsi vous informer et vous assister plus facilement. BASIC

Pensez également à **sauvegarder ou à noter sur papier les coordonnées de l'ambassade ou du consulat de Belgique** le plus proche. MEDIUM

Renseignez-vous enfin sur la législation locale et les éventuelles autorisations de voyage. Si vous devez compléter des formulaires de voyage pour des autorités étrangères, **limitez-vous aux informations strictement nécessaires et ne fournissez des détails qu'en cas de demande insistante.** HIGH

2. Préparez vos documents et supports de stockage

Vérifiez les règles de sécurité de votre organisation. N'hésitez surtout pas à contacter le ou les responsables de la sécurité pour bien préparer votre voyage. BASIC

N'emportez que les documents et supports de stockage strictement nécessaires. Gardez à l'esprit le contexte et les objectifs du voyage. Dans certains pays, les services de sécurité sont habilités à demander un accès à votre matériel et/ou à le confisquer. En emportant des documents ou des supports de stockage non indispensables, vous vous exposez à des risques inutiles. BASIC

Faites un **back-up** de vos données, que vous laisserez à la maison. BASIC

Transportez toujours vos documents confidentiels et supports de données dans **votre bagage à main, jamais dans votre valise.** BASIC

Emportez les documents sensibles **sous enveloppes scellées et sécurisées** (sealbags) et prévoyez-en également pour les autres étapes du voyage. MEDIUM

Emportez si possible uniquement des appareils mobiles spécifiquement prévus pour les voyages

et fournis par votre organisation. Ces appareils ne peuvent contenir **que les données strictement nécessaires** au voyage et devront être reformatés à votre retour avant une prochaine utilisation. HIGH

3. Protégez vos appareils mobiles

Suivez les recommandations disponibles sur le site : **www.safeonweb.be/tipswww.safeonweb.be/tips**

Nous attirons votre attention sur les recommandations suivantes :

- Installez les dernières mises à jour du système d'exploitation (OS) et des programmes. Ne téléchargez des programmes ou applications qu'à partir d'app stores officiels. BASIC
- Installez un antivirus sur tous vos appareils mobiles. BASIC
- Vérifiez les paramètres de sécurité et de confidentialité de vos appareils et des comptes qui y sont liés. Protégez au maximum vos données personnelles. BASIC
- Utilisez des modes de verrouillage sécurisés et désactivez l'affichage du contenu des notifications afin d'empêcher toute lecture indésirable par des tiers. BASIC
- Protégez vos mots de passe ! Ne les notez pas, changez-les régulièrement et utilisez si possible l'authentification à deux facteurs (2FA). BASIC
- Installez des applications de messagerie avec chiffrement de bout en bout. BASIC
- Effacez votre historique d'appels et de navigation avant votre départ. MEDIUM

Séparez toujours environnements professionnel et privé pour vos appareils, comptes, numéros de téléphone et adresses e-mail. MEDIUM

Afin de ne laisser aucune trace des réseaux et appareils de votre domicile, utilisez la fonction « Oublier » pour tous les **réseaux et appareils Bluetooth connectés** précédemment. MEDIUM

Prévoyez une connexion sécurisée par **VPN**, notamment pour l'accès à votre messagerie ou au réseau de votre organisation. MEDIUM

Chiffrez les données sensibles sur vos supports de stockage, conformément aux règles de votre organisation. MEDIUM

Remarque : Certains pays interdisent l'utilisation du VPN ou de logiciels de chiffrement. À vérifier avant votre départ.

Limitez au maximum le nombre d'applications sur votre appareil et utilisez si possible un **navigateur web en guise d'alternative** pour éviter que l'application ait accès aux informations de l'appareil. HIGH

4. Réseaux sociaux

Vérifiez vos **paramètres de confidentialité** sur les réseaux sociaux. Protégez au maximum vos données personnelles. BASIC

Contrôlez les **accès pour chaque application** (microphone, appareil photo, contacts, localisation, etc.). Souvent, ceux-ci ne sont pas essentiels pour utiliser l'application. BASIC

Évitez si possible de parler de votre voyage sur les réseaux sociaux. La publication d'informations au sujet de votre programme, des personnes qui vous accompagnent et/ou de votre localisation est également déconseillée. MEDIUM

Faites preuve de vigilance si vous recevez des messages, des demandes de réseaux ou des invitations de tiers. Limitez-vous aux **communications indispensables pour votre voyage**. MEDIUM

PENDANT LE VOYAGE

1. Agissez avec discrétion et prudence

N'affichez pas de logos ni de données d'identité en dehors du lieu de travail. MEDIUM

Ne révélez pas votre localisation au moyen de votre smartphone ou de votre tablette. Désactivez l'**accès à vos données de localisation**. MEDIUM

Protégez-vous des regards indiscrets. Placez à cet effet un **filtre sur votre écran** si vous devez travailler dans un lieu public ou fréquenté. MEDIUM

Évitez les conversations sur des sujets sensibles ou polarisants dans les lieux publics où d'autres personnes pourraient vous écouter. MEDIUM

Désactivez toutes les **connexions non essentielles** (Bluetooth, Wifi, Near Field Communication/NFC) de vos appareils mobiles. **Le « mode avion » n'est pas suffisant** : il ne permet pas toujours de désactiver complètement ces connexions. MEDIUM

N'utilisez **pas d'assistants vocaux**, tels que Siri, Alexa ou Bixby, ni d'autres applications d'IA. HIGH

Si vous devez remettre votre smartphone ou en vous séparer à un endroit, retirez si possible **la carte**

SIM, la carte mémoire et la batterie. HIGH

2. Protégez en permanence vos données et supports de stockage

Ne laissez **jamais vos documents, supports de stockage ou appareils sans surveillance** et n'autorisez en aucun cas l'accès à vos appareils à des tiers. BASIC

Ne chargez pas vos appareils au moyen de dispositifs de recharge offerts et/ou de bornes de recharge USB publiques pour éviter les logiciels malveillants et les vols de données. Si vous n'avez pas d'autre possibilité de recharge, utilisez un câble bloqueur de données pour protéger votre appareil. BASIC

Prévoyez des **systèmes antivol adaptés** et utilisez des mots de passe uniques sur vos appareils pour éviter les échanges. MEDIUM

Ne laissez aucun document sensible dans votre chambre d'hôtel ni dans le coffre-fort, qui pourrait être facilement ouvert par le personnel de l'hôtel à la demande de personnes mal intentionnées. MEDIUM

Évitez d'utiliser des connexions Wifi ou Bluetooth publiques (par ex. dans une voiture de location) ou des codes QR qui ne vous inspirent pas confiance. MEDIUM

Éteignez complètement vos appareils pendant la nuit –

effectuez chaque jour un **cycle d'alimentation** (arrêt complet et rallumage de l'appareil). HIGH

3. Restez critique

Restez critique si vous faites l'objet d'attentions particulièrement marquées ou si votre interlocuteur évoque des références idéologiques, culturelles ou religieuses communes. MEDIUM

Accueillez avec prudence flatteries, confidences et cadeaux (rarement offerts à titre désintéressé). MEDIUM

Ne vous laissez pas déconcerter par des marques de solidarité ou d'amitié. Il pourrait s'agir d'une **tentative de manipulation**. MEDIUM

Faites également preuve de prudence lors d'événements (sociaux) organisés en marge d'une rencontre officielle. MEDIUM


EARTH
EARTH
EARTH
EARTH

AU RETOUR

Effectuez un **cycle d'alimentation** sur vos appareils. BASIC

Rapportez tout incident ou événement suspect par écrit au responsable de la sécurité de votre organisation. BASIC

Si vous avez reçu une **clé USB ou tout autre support de stockage électronique, ne connectez jamais ce matériel** à votre ordinateur sans vérification de sécurité préalable par un opérateur qualifié. BASIC

Au moindre doute, **faites analyser votre ordinateur ou votre smartphone et changez vos mots de passe.** BASIC

Scannez régulièrement vos appareils à la recherche de virus et de logiciels malveillants. BASIC

Interrogez-vous sur l'utilité des relations nouées au cours du voyage. **Restez critique** si l'on vous recontacte après votre voyage : ces demandes, questions ou propositions sont-elles justifiées et pertinentes ? MEDIUM

QUE FAIRE EN CAS D'INCIDENT ?

En cas de perte ou de vol d'un document ou support de stockage, dressez la liste des données concernées. Avertissez immédiatement votre employeur ou le responsable de la sécurité, conformément aux règles de l'organisation. Si nécessaire, adressez-vous à la police locale.

En cas de perte de documents d'identité, contactez l'ambassade ou le consulat de Belgique.

En cas de perte de carte bancaire, appelez Card stop au numéro **078 170 170**. Vous pouvez également bloquer votre carte au moyen de votre application bancaire.

Si vous êtes confronté à d'autres situations suspectes (interrogatoire prolongé lors d'un contrôle aux frontières, photos sans autorisation, remise obligatoire de supports de stockage, etc.), contactez la VSSE : **vsse.be/contact**.

PLUS D'INFOS ?

- www.vsse.be
- www.diplomatie.belgium.be
- www.safeonweb.be

LA VSSE

La VSSE est chargée du suivi des activités d'ingérence et d'espionnage qui représentent une menace pour les intérêts fondamentaux de l'État, y compris de la protection du potentiel économique et scientifique. En cas de voyage à l'étranger, les risques liés à ces menaces sont accrus.

Si vous pensez que vous ou votre organisation êtes victime d'activités d'ingérence ou d'espionnage, ou si vous disposez d'informations potentiellement en lien avec ces menaces, contactez-nous :
www.vsse.be/contact

VSSE

VSSE

.be

Éditeur responsable : Francisca Bostyn
Boulevard du Roi Albert II, 6
1000 Bruxelles