
TRAVEL SECURITY

COMMENT PROTÉGER SES DONNÉES
LORS DE DÉPLACEMENTS À L'ÉTRANGER



PASSEPORT



SECURITÉ

COMMENT SE PROTÉGER ?

Choisissez des conseils qui répondent à vos besoins et au niveau de risque de votre déplacement.

3 NIVEAUX DE RECOMMANDATIONS

BASIC

La protection minimale requise pour tout déplacement.

MEDIUM

Des mesures supplémentaires pour une meilleure protection de vos informations personnelles et des données de votre organisation.

HIGH

Les mesures les plus strictes lorsque vous voyagez en dehors de l'Union européenne ou que vous transportez des informations sensibles.

LES RECOMMANDATIONS DES DIFFÉRENTS NIVEAUX SONT CUMULATIVES



3 ÉTAPES

1>AVANT :

La préparation est une étape essentielle pour **limiter son exposition aux menaces**. Objectif : limiter et sécuriser ses documents et supports.

2>PENDANT :

Prudence et discrétion sont les maîtres mots d'un voyageur averti. Ne soyez pas un livre ouvert pour les autres et **gardez le contrôle permanent** sur vos informations.

3>APRÈS :

Certaines menaces persistent après le retour. Au moindre doute, faites **vérifier vos supports et rappez tout incident**.

AVANT DE PARTIR

INFORMEZ-VOUS SUR VOTRE DESTINATION

→ Renseignez-vous sur la situation politique, économique et sociale de la zone de destination. Vous trouverez des informations utiles sur la page « Voyager à l'étranger » du site web du SPF Affaires étrangères. **MEDIUM**

www.diplomatie.belgium.be



→ Pensez également à **sauvegarder les coordonnées de l'ambassade** ou du consulat belge de référence. **MEDIUM**

→ Renseignez-vous sur **la législation locale** et les éventuelles autorisations de voyage. Si vous devez remplir des formulaires d'informations pour des services d'immigration étrangers, **ne fournissez que les informations strictement nécessaires.** **HIGH**

AVANT DE PARTIR

2

PRÉPAREZ VOS DOCUMENTS ET SUPPORTS

→ Informez-vous sur **les règles de sécurité de votre organisation**. N'hésitez pas à contacter votre conseiller en sécurité pour préparer votre voyage. **BASIC**

→ **Emportez uniquement les documents et supports mobiles strictement nécessaires au voyage**. Pour ce faire, il est nécessaire de vous informer précisément sur le contexte et les objectifs du voyage. Emporter des documents ou supports non indispensables vous fait courir un risque inutile. **BASIC**



→ Faites **un backup de vos données** et ne l'emportez pas avec vous. **BASIC**

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

→ Si possible, emportez uniquement des appareils mobiles dédiés aux voyages fournis par votre organisation. Ces appareils ne doivent contenir que **les données strictement nécessaires**. Ils seront dûment formatés au retour avant leur prochaine utilisation. **HIGH**

AVANT DE PARTIR

3 PROTÉGEZ VOS APPAREILS MOBILES

Suivez les recommandations disponibles sur : www.safeonweb.be

Nous attirons votre attention sur les **conseils suivants** :



Installez les dernières **mises à jour** de l'OS et des applications. **BASIC**



Installez un **anti-virus** sur tous vos appareils mobiles. **BASIC**



Vérifiez les **paramètres de sécurité et de confidentialité** des appareils et des comptes utilisateurs qui y sont liés. **BASIC**



Utilisez des **modes de verrouillage sécurisés**. **BASIC**



Protégez **vos codes et mots de passe**. **BASIC**



Effacez **l'historique** de navigation et des appels. **MEDIUM**

→ **Prévoyez un mode de connexion sécurisé par VPN**, particulièrement pour l'accès à votre messagerie ou au réseau de votre organisation. **MEDIUM**

→ **Chiffrez les données sensibles** sur vos supports selon les règles en vigueur au sein de votre organisation. **Important : certains pays interdisent l'utilisation du VPN ou de logiciels de chiffrement.** **MEDIUM**



AVANT DE PARTIR

RÉSEAUX SOCIAUX

→ Vérifiez vos paramètres de confidentialité sur les réseaux sociaux. Il est recommandé de limiter autant que possible l'exposition de vos données personnelles en dehors de votre cercle de confiance. **BASIC**

→ Si possible, évitez de communiquer sur les réseaux sociaux au sujet de votre voyage. Il est déconseillé de publier des détails sur le programme, les personnes qui vous accompagnent et votre localisation. **MEDIUM**



→ Soyez attentif aux messages, recommandations de relations ou invitations à l'approche de votre voyage. **N'acceptez d'interagir qu'avec des personnes dont vous jugez la relation pertinente.** **MEDIUM**



DURANT LE VOYAGE

1 RESTEZ DISCRET ET PRUDENT

- Évitez d'afficher des logos ou votre identité en dehors des lieux de travail (en rue, à l'hôtel ou dans des établissements horeca). **MEDIUM**
- Évitez d'être géolocalisé par votre smartphone ou tablette. **MEDIUM**
- Évitez les regards indiscrets. Placez un filtre pour écran si vous devez travailler dans un lieu public ou fréquenté. **MEDIUM**
- Évitez les conversations sur des sujets sensibles dans des taxis ou des lieux fréquentés. **MEDIUM**
- Si vous devez vous séparer de votre smartphone, retirez la carte SIM, la carte mémoire et la batterie (si possible). **HIGH**

2 PROTÉGEZ VOS DONNÉES ET SUPPORTS EN PERMANENCE

- Évitez de laisser vos documents, supports et outils de travail sans surveillance, ne permettez pas leur accès à une tierce personne. **BASIC**
- Prévoyez des systèmes antivols adaptés et apposez des signes distinctifs sur vos appareils pour éviter les échanges. **MEDIUM**
- Ne laissez aucun document sensible dans votre chambre d'hôtel ni dans le coffre-fort, qui peut être facilement ouvert par le personnel de l'hôtel à la demande d'une personne malveillante. **MEDIUM**
- Verrouillez toutes les connexions non indispensables de vos appareils mobiles (bluetooth, wifi, NFC). **MEDIUM**
- Évitez de vous connecter à des points d'accès wifi publics. **HIGH**
- Ne chargez pas vos appareils sur les stations de charge USB publiques pour éviter tout malware ou vol de données. **HIGH**

DURANT LE VOYAGE

RESTEZ CRITIQUE

- Restez critique si vous faites l'objet d'une attention appuyée ou si votre interlocuteur fait appel à **des références idéologiques, culturelles ou religieuses communes.** **MEDIUM**
- Accueillez avec prudence les **flatteries, confidences et cadeaux** (rarement désintéressés). **MEDIUM**
- **Ne vous laissez pas abuser** par un sentiment de proximité ou d'amitié. **MEDIUM**

Ces éléments peuvent être des indicateurs d'**une tentative de manipulation.**



AU RETOUR

- 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 un autre support électronique**, ne le branchez jamais sur votre ordinateur sans une vérification de sécurité par un opérateur qualifié. **BASIC**
- Au moindre doute, **faites analyser votre ordinateur ou smartphone** et changez les mots de passe utilisés durant votre séjour. **MEDIUM**
- Questionnez la pertinence des relations établies. **Restez critique** à l'égard des reprises de contact consécutives à la mission : les demandes, questions ou offres sont-elles justifiées et pertinentes ? **MEDIUM**





.be

Éditeur responsable : Jaak Raes
Boulevard du Roi Albert II, 6
1000 Bruxelles - D/2019/7951/FR/1204