FICHE D'INFORMATION 01

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Service de renseignement de l'État

VOYAGER EN SÉCURITÉ

BONNES PRATIQUES POUR PROTÉGER VOS DONNÉES LORS DE DÉPLACEMENTS PROFESSIONNELS À L'ÉTRANGER

EDITEUR : SERVICE DE RENSEIGNEMENT DE L'ÉTAT (SRE)

WEB : SRE.GOUVERNEMENT.LU

JUIN 2026

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Service de renseignement de l'État

SOMMAIRE

Dans le cadre de sa mission d'anticipation et de prévention des menaces liées à l'espionnage, le SRE souhaite offrir aux représentants des services publics et des entreprises privées des conseils pratiques pour protéger leurs données et informations sensibles lors de déplacements professionnels à l'étranger.
En effet, dans le cadre d'activités d'espionnage, des acteurs étrangers mettent en œuvre des moyens de plus en plus divers pour accéder à des informations qui ne sont pas accessibles au public.

LA SÉCURITÉ DES VOYAGES D'AFFAIRES. QUI EST CONCERNÉ ?

Dans le cadre d'un déplacement professionnel à l'étranger, une personne représentant un organisme étatique, une institution ou organisation internationale, une entreprise ou un centre de recherche, peut être amenée à transporter des informations stratégiques et sensibles. La perte ou le vol de ces informations pourrait, le cas échéant, causer des dommages considérables pour le secteur public, privé ou académique/scientifique.
Afin de limiter les risques d'un accès non autorisé à vos données, le SRE met à votre disposition quelques bonnes pratiques, **AVANT, PENDANT** et **APRÈS** un voyage d'affaires en dehors du Luxembourg.

BONNES PRATIQUES POUR PROTÉGER LES DONNÉES SENSIBLES

Vous trouverez ci-dessous une sélection de recommandations élémentaires qui peuvent être complétées selon les besoins spécifiques de l'organisation que vous représentez et le niveau de risque du pays dans lequel vous vous déplacez. Il est recommandé de vous concerter avec le ou la responsable de la sécurité de votre entreprise ou organisation pour décider des mesures de sécurité à mettre en œuvre.

AVANT DE PARTIR

INFORMEZ-VOUS SUR LE PAYS DE DESTINATION

- Consultez les conseils aux voyageurs sur le site web du ministère des Affaires étrangères et européennes, de la Défense, de la Coopération et du Commerce extérieur.
- Informez-vous sur d'éventuelles autorisations de voyage. Si vous devez remplir un formulaire pour les services d'immigration, ne fournissez que les informations strictement nécessaires. Certains pays demandent des détails sur la nature de votre emploi. Les données fournies sur ces formulaires peuvent aider à déterminer l'intérêt que représente la personne en déplacement en tant que cible potentielle d'un intérêt en renseignement. Ayez conscience des informations personnelles qui sont disponibles sur Internet, p.ex. profil LinkedIn ou site web de votre entreprise.
- Adaptez la sécurisation des moyens de communication et de stockage de données que vous emportez en fonction de la réglementation locale. Dans certains pays, les services de contrôle aux frontières peuvent demander vos mots de passe et identifiants pour accéder à vos appareils numériques et peuvent même retenir ces derniers.
- Sauvegardez les coordonnées de contact de l'ambassade ou du consulat luxembourgeois le plus proche.

LIMITEZ LE TRANSPORT DE DONNÉES NON NÉCESSAIRES

- Emportez le strict minimum d'informations et d'appareils électroniques avec vous.
  Avant votre départ, posez-vous les questions suivantes :
  - Est-ce vraiment nécessaire d'emporter cet objet ou cette information ?
  - Quelle est la valeur des informations que je transporte (sur papier, données numériques, ou autre) ?
  - Quels seraient les dommages encourus en cas de perte ou de vol de ces données ?
  - Quels appareils dois-je absolument prendre avec moi ?
    Si possible, emportez uniquement des appareils électroniques professionnels dédiés à la mission (smartphones, tablettes, laptops, disques durs, clés USB, etc.), qui ne contiennent pas de documents, de courriels ou de coordonnées de contact non nécessaires pour le voyage. À votre retour, il est recommandé de réinitialiser les appareils emportés.
    Les mêmes recommandations s'appliquent pour les appareils électroniques personnels (smartphone, montre intelligente, etc.).

PROTÉGEZ VOS DONNÉES ET APPAREILS

- Si vous devez apporter des documents confidentiels sur papier, mettez-les dans des enveloppes scellées et sécurisées.
  Transportez toujours vos documents confidentiels dans votre bagage à main.
  Informez-vous auprès de l'officier de sécurité de votre établissement ou de votre entreprise sur les réglementations concernant le transport d'informations classifiées.

- Avant votre départ, assurez-vous de protéger vos appareils mobiles en suivant ces étapes :

- Installez les dernières mises à jour, y compris celles des applications, au Luxembourg. N'installez pas de mises à jour à l'étranger.
- Installez un programme antivirus (recommandé par votre employeur) sur tous vos appareils et vérifiez que tous les paramètres de sécurité sont activés.
- Mettez en place des mécanismes de verrouillage sécurisés et utilisez des mots de passe et des codes PIN robustes.
- Effacez l'historique de votre navigateur et de vos appels.

- Utilisez une connexion sécurisée via un virtual private network (VPN), en particulier lorsque vous accédez à votre environnement de travail ou gérez vos services de messagerie.

- Consultez le ou la responsable de la sécurité de votre organisation pour connaître les solutions sécurisées disponibles, telles que les conteneurs chiffrés ou le cryptage des données. Assurez-vous également de respecter les éventuelles règles de sécurité de votre employeur.
  Notez que dans certains pays l'utilisation d'un VPN ou le cryptage de données sont interdits.

LIMITEZ LA PUBLICATION D'INFORMATIONS PERSONNELLES EN LIGNE

- Vérifiez les paramètres de confidentialité sur les réseaux sociaux et sur votre smartphone.

- Évitez de partager des informations sur votre voyage sur les réseaux sociaux, comme votre itinéraire, des détails sur votre programme, ou votre lieu de séjour.

PENDANT LE VOYAGE

ÉVITEZ DE LAISSER VOS DONNÉES ET APPAREILS SANS SURVEILLANCE

- Évitez de laisser vos documents et appareils dans des endroits accessibles à d'autres personnes.
- Utilisez si possible des systèmes antivols.
- Ne laissez pas de données sensibles dans votre chambre d'hôtel, y inclus dans le coffre-fort.
- Si vous devez vous séparer de vos données, appareils ou autres supports, utilisez des enveloppes scellées pour préserver leur intégrité et pour constater toute tentative d'accès.

RESTEZ DISCRET ET VIGILANT

- Placez un filtre de confidentialité pour écran si vous devez travailler dans des lieux publics.
- Évitez les conversations sur des sujets sensibles dans des lieux publics fréquentés et les transports en commun.
- Évitez d'exposer votre identité ou le logo de votre organisation en dehors du cadre professionnel.
- Restez critique si vous faites l'objet d'une attention soutenue de votre interlocuteur.
- Accueillez avec prudence des cadeaux ou flatteries.

ÉVITEZ DES CONNEXIONS NON SÉCURISÉES

- Désactivez la géolocalisation sur votre smartphone et votre tablette.
- Désactivez toutes les connexions de vos appareils que vous n'utilisez pas (Bluetooth, Wi-Fi, etc.).

- Évitez à tout moment de vous connecter à des points d'accès Wi-Fi publics. Si vous devez vous connecter à Internet, utilisez si possible le point d'accès mobile de votre téléphone professionnel.
- Ne chargez pas vos appareils via des points de charge USB. Ils peuvent être exploités pour pirater votre matériel ou voler des données. Utilisez toujours votre propre chargeur et chargez via une prise électrique classique.
- N'utilisez pas les équipements qui vous sont offerts, tels que des clés USB, des batteries externes ou des objets connectés via Bluetooth.

APRÈS LE VOYAGE

RENOUVELEZ VOS MOTS DE PASSE

- Au moindre doute, changez vos mots de passe et les codes de connexion que vous avez utilisés pendant votre voyage.

FAITES VÉRIFIER VOS ÉQUIPEMENTS

- En cas d'incident suspect, faites analyser vos appareils pour détecter d'éventuelles failles de sécurité.
- Si vous avez reçu en cadeau une clé USB ou tout autre dispositif qui se connecte à votre ordinateur ou à votre téléphone portable, ne l'utilisez pas avant de l'avoir soumis à un contrôle de sécurité approfondi.

MÉFIEZ-VOUS DE PRISES DE CONTACT

- Méfiez-vous des prises de contact après le voyage. Les questions, les offres, les messages, sont-ils justifiés ?
- Signalez toute rencontre ou tout incident suspect au service de sécurité de votre organisation.

QUE FAIRE SI VOUS CONSTATEZ UNE ACTIVITÉ SUSPECTE ?

N'hésitez pas à signaler toute rencontre ou tout événement suspect au service de sécurité de votre entreprise.
En cas de vol ou de perte d'informations, informez immédiatement le ou la responsable de la sécurité de votre ministère ou entreprise.

Liens utiles :

- Le site internet du ministère des Affaires étrangères et européennes, de la Défense, de la Coopération et du Commerce extérieur offre des informations sur les sujets suivants :
  - Perte ou vol de documents d'identité
  - Représentations consulaires du Grand-Duché de Luxembourg à l'étranger
  - Assistance consulaire, etc.

LE SRE – ANTICIPATION ET PRÉVENTION DE MENACES EN LIEN AVEC L'ESPIONNAGE

Le Service de renseignement de l'État (SRE) a pour mission de prévenir et d'anticiper des activités qui menacent les intérêts fondamentaux du Grand-Duché de Luxembourg, y compris la protection de son potentiel scientifique et technique, de ses intérêts économiques ou de ses relations internationales.

Certains États ont recours à des activités d'espionnage pour recueillir des renseignements qui servent leurs intérêts politiques ou économiques. **Si vous pensez que vous ou votre organisation avez été la cible d'activités d'espionnage, ou si vous détenez des informations qui pourraient être utiles dans le cadre de l'anticipation et la prévention des menaces liées**

à l'espionnage, vous pouvez remplir le formulaire de contact en ligne ou contacter le SRE par e-mail (info@me.etat.lu).

Veuillez indiquer dans votre message :

- vos nom(s) et prénom(s) ;
- votre employeur ou l'organisation que vous représentez, le cas échéant ;
- votre message (veuillez préciser la situation que vous voulez signaler ou les renseignements que vous souhaitez obtenir) ;
- un numéro de téléphone pour permettre au SRE de vous contacter, si vous le souhaitez.

Toute information fournie est traitée de manière strictement confidentielle.