Sécurité de l'information lors de voyages internationaux

Mise à jour : avril 2025

UNIVERSITÉ LAVAL

Table des matières

Introduction

Ce guide est à l'intention de tous les membres de la communauté universitaire.

Lorsque vous voyagez à l'extérieur du Canada, que ce soit pour des raisons personnelles, professionnelles ou liées aux études, vous vous exposez à des risques accrus en matière de sécurité de l'information.

Dans certains pays, des fouilles électroniques peuvent être imposées, des restrictions sur l'importation temporaire de tout appareil contenant des technologies de chiffrement peuvent s'appliquer, et les communications sur les réseaux peuvent être plus facilement interceptées.

Ce guide propose des pratiques recommandées pour protéger vos appareils mobiles et les données institutionnelles lors de vos déplacements à l'étranger.

Avant le voyage

❑ Vérifier les lois du pays de destination

- Dans plusieurs pays, les agents frontaliers peuvent inspecter les appareils électroniques. Vous pouvez refuser de fournir vos mots de passe; cela peut toutefois entraîner des délais, une saisie temporaire de l'appareil ou d'autres conséquences selon le pays.
- Le Canada est signataire de l'*Arrangement de Wassenaar*, qui prévoit une exemption permettant de voyager temporairement avec un appareil chiffré pour usage personnel, pourvu qu'aucune technologie de chiffrement ne soit installée, modifiée ou diffusée durant le séjour.
    - Cette exemption n'est toutefois pas universellement reconnue. Certains pays exigent une autorisation préalable ou une licence d'importation pour les appareils chiffrés.
- Plusieurs pays interdisent ou réglementent l'importation de dispositifs contenant des technologies de chiffrement. Informez-vous avant votre départ.

❑ Évaluer la nécessité d'emporter un appareil

- Privilégiez l'accès à distance aux services institutionnels au transport local de fichiers.
- Dans certaines situations sensibles ou lors de déplacements vers des destinations à risque élevé, privilégiez l'utilisation d'un appareil temporaire contenant uniquement l'information minimale requise.

❑ Sécuriser les données

- Supprimez de vos appareils toute donnée confidentielle ou sensible (notamment les dossiers internes, les informations personnelles et les courriels).
- Assurez-vous que les sauvegardes de vos fichiers associés à l'Université sont à jour et stockées sur des plateformes de l'Université.
- Utilisez des mots de passe robustes et uniques.
- En fonction du pays de destination, consultez votre centre de services en TI afin d'évaluer la possibilité d'activer le chiffrement complet des données présentes sur votre appareil.
- Activez l'authentification multifactorielle sur tous vos comptes.

❑ Désinstaller les applications non essentielles

- Retirez les applications non nécessaires, notamment celles reliées aux réseaux sociaux ou aux services personnels.
- Déconnectez-vous des comptes associés à l'Université lorsque leur accès n'est pas requis pendant le voyage.

Pendant le voyage

❑ Protéger physiquement vos appareils

- Gardez vos appareils avec vous en tout temps, y compris dans les lieux publics ou partagés.
- Évitez de les prêter, de les entreposer dans des lieux non sécurisés ou de les laisser branchés sans surveillance.
    - Les coffres-forts des hôtels ne sont pas considérés comme des lieux sécurisés.

❑ Se connecter de manière sécurisée

- Connectez-vous uniquement à des réseaux Wi-Fi fiables. Lorsque possible, privilégiez les réseaux cellulaires.
- Activez le VPN de l'Université Laval (vpncampus.ulaval.ca) pour tout accès aux services internes.
- N'accédez jamais aux systèmes de l'Université par l'entremise de connexions publiques non protégées.

❑ Réduire les expositions involontaires

- Désactivez les connexions automatiques aux réseaux Wi-Fi publics ou inconnus.
- Coupez les fonctions Bluetooth et Wi-Fi lorsque vous ne les utilisez pas. Notamment, en utilisant la fonctionnalité « Mode Avion ».
- N'utilisez pas de bornes publiques USB de recharge.
- Évitez de balayer tout code QR dont la provenance n'est pas vérifiée.

Au retour

❑ Réinitialiser vos identifiants d'accès

- Modifiez les mots de passe de vos comptes associés à l'Université, surtout si vous avez utilisé un appareil personnel, fait l'objet d'une fouille ou si un doute subsiste quant à la sécurité de vos connexions.

❑ En cas de doutes, faire analyser vos appareils

- Si vous avez le moindre soupçon de compromission, de manipulation ou d'inspection non sollicitée, faites vérifier l'appareil par votre centre de services en TI.

❑ Éliminer les données superflues après le séjour

- Supprimez les documents ou fichiers temporaires téléchargés pendant le séjour.
- Ne conservez que les données réellement nécessaires à la suite de vos activités professionnelles ou d'études.

❑ Rester vigilant(e)

- De nombreuses personnes rapportent une augmentation des tentatives d'hameçonnage ciblé et de fraude après un voyage.

Appui et soutien

Votre centre de services en TI peut vous conseiller avant, pendant et après un déplacement à l'étranger.

L'équipe du Centre de cyberdéfense de l'Université Laval peut pour sa part vous soutenir en cas d'incident de sécurité de l'information lors d'un déplacement à l'étranger. Pour communiquer avec le Centre de cyberdéfense : cyberdefense@ulaval.ca

En savoir plus

Informations et ressources supplémentaires mises à la disposition des voyageuses et voyageurs par le Gouvernement du Canada :

- Cybersécurité au cours des déplacements : recommandations en matière de sécurité - Voyage.gc.ca
- Dispositifs mobiles et voyages d'affaires (ITSAP.00.087) - Centre canadien pour la cybersécurité
- À L'étranger – Directives de sécurité sur les voyages - Canada.ca