Voyages professionnels – Sécurité IT – Bonnes pratiques

Date : 12.04.2024

Auteur : JF Dousson

Protéger ses informations confidentielles en voyage

La sécurité de l'information est importante aussi durant les voyages, et se prépare en amont.

De plus en plus d'entreprises suisses sont victimes d'espionnage économique, et le monde académique n'est pas épargné.

Certains pays disposent d'une législation leur permettant d'exiger de tout voyageur se présentant à la frontière la communication de ses mots de passe, même sans infraction préalable ni soupçons. D'autres acteurs tentent d'accéder à des informations privilégiées en accédant au matériel laissé dans une chambre d'hôtel ou analysant le trafic non chiffré.

Les présentes bonnes pratiques visent à sécuriser les informations à disposition des voyageurs qui sont exposées à des risques variables suivant leur niveau de confidentialité (interne, confidentielles, secrètes), le domaine de recherche du voyageur, le niveau sécuritaire du pays visité, et des lois et pratiques locales. Dans la mesure où ces facteurs changent régulièrement, il n'est pas possible de fournir une liste des pays concernés.

Avant le voyage

Niveau de risque moyen

Sauvegarder toutes les données stockées sur les périphériques à emmener en voyage de manière à les retrouver au retour du voyage. Ne pas emporter la sauvegarde en voyage, quel que soit le support envisagé.

Supprimer les données inutiles au voyage des périphériques à emmener en voyage. Attention, il est possible dans certains cas de récupérer des fichiers effacés.

Supprimer la synchronisation des emails et effacer les boites aux lettres stockées sur les périphériques à emmener en voyage.

Installer le client VPN de l'EPFL.

Activer, si disponible, la possibilité d'effacer à distance le matériel en cas de vol ou de perte.

S'assurer que le système d'exploitation, les applications et l'anti-virus sont à jour.

Vérifier que le matériel est protégé par un mot de passe / PIN code à l'allumage.

S’assurer que le matériel ne se connectera pas automatique au WiFi à l’allumage.

Niveau de risque élevé

Laisser tous les périphériques professionnels utilisés habituellement (laptop, tablette, smartphone) au bureau.

Utiliser un ancien smartphone réinitialisé. Désactiver le déverrouillage biométrique et le remplacer par un PIN code.

Saisir uniquement les contacts indispensables au voyage.

Chiffrer les documents sensibles nécessaires au voyage sur un laptop ou une tablette réinitialisée avant le voyage qui ne sera utilisé que pour y accéder.

Activer, si disponible, la possibilité d’effacer à distance le matériel en cas de vol ou de perte.

S’assurer que le système d’exploitation, les applications et l’anti-virus sont à jour.

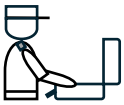
S’assurer que le matériel ne se connectera pas automatique au WiFi à l’allumage.

Niveau de risque extrême

Laisser tous les périphériques professionnels (laptop, tablette, smartphone, clefs USB, disques durs mobiles) au bureau.

Saisir uniquement les contacts indispensables au voyage sur un téléphone réinitialisé et mis à jour pour l’occasion. N’installer aucune application permettant d’accéder à des données dans le cloud. Ne connecter aucune boite aux lettres.

Ne télécharger aucun document sensible.



Pendant le voyage

Niveau de risque moyen

Avant d’arriver à l’aéroport, mettre le smartphone sur mode avion.

N’accéder à Internet qu’au-travers du VPN de l’EPFL.

N’accéder à vos emails professionnels qu’à partir de ewa.epfl.ch via le VPN.

Ne pas télécharger de documents sur les périphériques emmenés en voyage.

Ne pas laisser le matériel sans surveillance. Ne pas laisser le matériel dans la chambre d’hôtel, ni dans le coffre-fort de la chambre d’hôtel, ni à la réception de l’hôtel.

Ne pas recharger les périphériques depuis une prise USB (aéroport, hôtel, taxi...).

En cas de fouille du matériel, demander à y assister.

Désactiver le WiFi, Bluetooth et la géolocalisation lorsqu'ils ne sont pas nécessaires.

Ne connecter aucun périphérique remis par un tiers, ou trouvé, au matériel apporté en voyage.

Considérer le matériel comme compromis s'il a été accédé par un tiers, même en votre présence.

Eteindre le smartphone si des éléments confidentiels doivent être abordés lors de discussions.

Ne prêter son matériel sous aucun prétexte.

Niveau de risque élevé

Avant d'arriver à l'aéroport, éteindre le smartphone et le rallumer à quelques kilomètres de l'aéroport.

En cas de fouille du matériel par les autorités locales, demander à y assister.

Désactiver le WiFi, Bluetooth et la géolocalisation.

Ne pas laisser le matériel sans surveillance. Ne pas laisser le matériel dans la chambre d'hôtel, ni dans le coffre-fort de la chambre d'hôtel, ni à la réception de l'hôtel.

Ne pas recharger les périphériques depuis une prise USB (aéroport, hôtel, taxi...).

Ne connecter aucun périphérique remis par un tiers ou trouvé au matériel apporté en voyage.

Considérer le matériel comme compromis s'il a été accédé par un tiers, même en votre présence.

Eteindre le smartphone si des éléments confidentiels doivent être abordés lors de discussions.

Ne prêter son matériel sous aucun prétexte.

Niveau de risque extrême

Avant d'arriver à l'aéroport, éteindre le téléphone et le rallumer à quelques kilomètres de l'aéroport.

Ne pas laisser le téléphone sans surveillance. Ne pas laisser le téléphone dans la chambre d'hôtel, ni dans le coffre-fort de la chambre d'hôtel, ni à la réception de l'hôtel.

Ne pas recharger le téléphone depuis une prise USB (aéroport, hôtel, taxi...).

En cas de fouille du matériel, demander à y assister.

Considérer le matériel comme compromis s'il a été accédé par un tiers, même en votre présence.

Eteindre le téléphone si des éléments confidentiels doivent être abordés lors de discussions.

Ne prêter son matériel sous aucun prétexte.

Après le voyage

Niveau de risque moyen

Contacter votre AdminIT ou la Sécurité IT si votre matériel a été accédé par un tiers, même en votre présence. NE PAS LE CONNECTER AU RESEAU DE l'EPFL.

Niveau de risque élevé

Réinitialiser / faire réinitialiser le matériel emporté en voyage. NE PAS LE CONNECTER AU RESEAU DE l'EPFL.

Niveau de risque extrême

Réinitialiser / faire réinitialiser le téléphone emporté en voyage.

Pour aller plus loin

Comme indiqué en introduction, certains pays disposent d'une législation leur permettant d'exiger de tout voyageur se présentant à la frontière la communication de ses mots de passe, même sans infraction préalable ni soupçons. Le refus de transmission de ses mots de passe peut entrainer la saisie du matériel pour une durée de quelques heures à plusieurs semaines. Il est aussi possible que l'entrée dans le pays soit refusée au voyageur et/ou que des mesures de contrainte soient exercées.

Certains pays, comme les USA ou le Canada limitent en principe leur examen aux données stockées sur le périphérique examiné, mais il n'est pas exclu que des données stockées dans le cloud et accessibles librement depuis le périphérique soient examinées aussi. Ils peuvent aussi demander les identifiants des réseaux sociaux des voyageurs.

La découverte d'un répertoire chiffré dissimulé peut éveiller les soupçons des autorités et ne dispensera pas le voyageur d'en donner la clef de chiffrement.

Certains contenus liés à la politique, à la religion, aux drogues ou à la pornographie sont règlementés, voire interdits pour entrer dans certains pays. Cette liste n'est pas exhaustive. Il est indispensable de se renseigner avant le voyage et de vérifier que le/les périphériques

emportés ne contiennent rien de tel, et que les publications sur les réseaux sociaux ont été filtrées en conséquence (p. ex. selfie devant un coffee shop).

De plus en plus d'entreprises suisses sont victimes d'espionnage économique, et le monde académique n'est pas épargné. La fouille du matériel à la frontière ou dans une chambre d'hôtel permet d'accéder immédiatement à d'éventuelles données intéressantes pour le pays de destination. Elle peut aussi être l'occasion d'installer une porte dérobée pour permettre l'accès ultérieur aux données, à la caméra ou au microphone, puis au réseau de l'EPFL au retour du voyageur lorsqu'il y connectera son matériel.

Il est à relever que certains pays et/ou certains prestataires de services (transport, organisateurs de séminaires, hébergement…) peuvent imposer, parfois au nom d'une facilitation d'accès, l'installation d'une application sur le smartphone du voyageur. Ladite application est susceptible de requérir plus de droits que nécessaire pour la fourniture du service, comme la position et l'accès au stockage, au micro ou à la caméra…

Nota Bene : Les données classifiées par la Confédération sont soumises à la Loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (LSI) et font l'objet de mesures de sécurité qui prévalent sur le présent document.

Plus d'informations