Aide-mémoire : Consignes de sécurité pour les voyageurs

Au cours d'un déplacement, les utilisateurs peuvent transporter diverses plateformes informatiques et appareils dont la compromission ou le vol pourrait faire du tort à l'École. Ce document contient des conseils visant à se prémunir contre les menaces cybernétiques qui peuvent toucher les employés, enseignants et étudiants de l'École en voyage à l'étranger ou au pays.

MISE EN GARDE

Dans certains pays, les centres d'affaires et les réseaux téléphoniques des hôtels sont surveillés et, à certains endroits, les chambres d'hôtel peuvent même être fouillées. En règle générale, on ne doit s'attendre à aucun respect de la vie privée dans les bureaux, les hôtels, les cafés Internet ou tout autre endroit public.

Avant le départ en voyage

Un voyage à l'étranger cyber-sécurisé nécessite une bonne préparation. Dans cette optique, il est recommandé de :

- Faire une sauvegarde du contenu de votre ordinateur et téléphone portable. Si vous sauvegardez régulièrement vos données sur les partages de l'École (lecteurs U, P, Sharepoint, Teams et OneDrive), vous n'avez pas à vous inquiéter, vos données sont prises en copie régulièrement par les services informatiques de l'École et sont accessibles de l'externe via une connexion sécurisée. Si vous utilisez des équipements personnels, assurez-vous de sauvegarder vos données sur un espace de stockage sûr et sécurisé.
- Tenez compte des répercussions de la perte ou du vol des informations stockées sur l'appareil de voyage sur votre organisation. Supprimez les données inutiles au voyage, faites-en une copie de sauvegarde sur les serveurs de l'École.
- Modifier les mots de passe et les codes d'accès de vos appareils en utilisant une combinaison forte, mais facile à retenir.
- Activez un économiseur d'écran sur vos téléphones portable, qui contient un nom et un point de contact en cas de perte de l'appareil. Évitez de mentionner le nom de l'École.
- Désactivez le protocole Bluetooth sur votre appareil mobile si vous n'en avez pas besoin.
- Assurez-vous d'avoir le client VPN installé ſur votre ordinateur pour établir des connexions sécurisées avec le réseau de l'École. Tous les ordinateurs portables fournis par l'École sont équipés de ce logiciel par défaut.

Pendant le voyage

- Conservez l'appareil avec vous en tout temps. Ne laissez pas l'appareil avec vos bagages en consigne et évitez les casiers de sûreté des wagons de train, des aéroports et des hôtels.
- Prenez garde aux personnes dans votre environnement immédiat qui pourraient voir votre écran ou votre clavier, surtout dans les aires publiques (par exemple, protégez les mots de passe contre les regards indiscrets) et mettez fin à la connexion lorsque vous avez terminé votre session de travail.
- Videz la corbeille et les dossiers « récents » après chaque utilisation. Nettoyez le navigateur après chaque utilisation : effacez les fichiers d'historique, la mémoire cache, les témoins, les adresses URL et les fichiers Internet temporaires.

WIFI

- Parfois, des points d'accès gratuits à Internet sont établis à des fins malveillantes et sont nommés intentionnellement de manière à donner l'impression de points d'accès de confiance. Par exemple, un hôtel peut avoir établi le point d'accès « HotelABC Internet ». Un auteur de menace peut établir à proximité de cet hôtel un point d'accès malveillant appelé « SecureHotelABC Internet ». La puissance du signal de ce dernier peut être supérieure à celle de l'hôtel. L'utilisateur croira alors qu'il s'agit de la connexion à choisir de préférence. Le voyageur devrait donc vérifier auprès de l'établissement d'hébergement ou l'organisateur de la conférence le nom du point d'accès légitime.
- Faites particulièrement attention aux réseaux Wifi publics. S'il est très tentant de s'y connecter lorsque le réseau 4G est faible ou défaillant, cette démarche est très risquée, car ce sont des cibles faciles pour les pirates informatiques. Pour éviter toute menace, mieux vaut ne pas utiliser les réseaux wifi en libre accès (à l'aéroport, dans les gares, à l'hôtel…). Même si ce n'est que pour aller sur les réseaux sociaux. Si vous devez vous connecter au bureau, utilisez toujours une connexion VPN.

Ordinateurs publics

- Ne jamais utiliser un ordinateur public (dans une exposition ou conférence par exemple) pour vous connecter à votre session professionnelle ou pour faire des transactions financières, car ce type d'appareil est fortement exposé aux menaces cybercriminelles. Des pirates informatiques peuvent y avoir installé un **enregistreur de frappe** (keylogger) ou autres logiciels malveillants et ainsi voler vos identifiants, code d'accès et mots de passe. N'utiliser les ordinateurs publics que pour trouver des renseignements touristiques.

Stations de chargement

- Les aéroports et autres structures d'accueil proposent aujourd'hui des **stations de recharge pour équipements informatiques en libre accès**. Si cela peut être très pratique et d'un grand secours, leur usage peut également être risqué. Apporter avec vous votre propre chargeur ou une **batterie de secours**, et éviter de vous connecter à toute station de recharge qu'un voyageur ou conférencier vous propose.
- Éviter également de connecter à votre téléphone ou ordinateur portatif des appareils USB et des supports de stockage obtenus auprès de sources inconnues.

Méfiez-vous des réseaux sociaux

- La prudence est nécessaire dans toutes les communications publiques, notamment celles que vous faites sur les réseaux sociaux. Évitez de publier des informations sur la destination, le but et la durée de votre voyage.
- Si vous avez vraiment envie de poster des photos de voyage, modifiez au préalable **la confidentialité de vos publications** et limitez-la aux personnes en qui vous avez vraiment confiance (familles et amis proches par exemple). Évitez surtout de faire des partages en **mode public**.

Incidents de sécurité

- Signalez sans délai les incidents suspects au soutien technique de la DTI à l'adresse soutien.ti@hec.ca.

Au retour du voyage, soyez à l'affût de toute activité suspecte au niveau de votre ordinateur ou téléphone portable. Signalez toute anomalie immédiatement au soutien technique de la DTI.

Liens utiles

https://cyber.gc.ca/sites/default/files/publications/ITSAP.00.001-fr.pdf

https://cyber.gc.ca/sites/default/files/publications/itsap70015-fr.pdf

https://cyber.gc.ca/sites/default/files/2021-04/ITSAP00011-utilisation-technologie-bluetooth.pdf

HEC MONTRÉAL

3000, chemin de la Côte-Sainte-Catherine
Montréal (Québec) H3T 2A7 CANADA
Téléphone : 514 340-6000

SDG-24461 – HEC-SI-21-1201