Sécurité des déplacements professionnels

Dans l'actualité

Janvier 2024

Voleur de luxe

Arrestation d'un voleur parcourant les hôtels de luxe pendant les grands événements mondiaux pour **s'introduire dans la chambre** de leurs clients, y compris celle des délégations étrangères.

Février 2024

Des plans qui tombent à l'eau

Un fonctionnaire de la Ville de Paris se fait voler dans le train sa sacoche avec son PC et une clé USB qui contiennent de **plans relatifs aux JO de Paris 2024**. L'auteur depuis a été interpellé mais le matériel n'a pas été retrouvé.

Mars 2024

Catastrophe diplomatique

Fuite d'une discussion entre haut-gradés de l'armée de l'air allemande évoquant la possibilité de frapper les infrastructures civiles russes. L'un d'eux aurait utilisé le **WiFi de son hôtel pour se connecter** à la réunion, qui s'est tenue sur Webex (!).

Avant le déplacement

J'emporte le strict minimum !

Cette recommandation s'applique aussi bien au **matériel** qu'aux **données** : évitez ainsi, si possible, d'emporter avec vous des infos ou docs sensibles et de devoir travailler dessus pendant votre trajet.

Je sauvegarde le nécessaire

Sauvegardez les données que vous transportez via les moyens fournis par votre service informatique. La sauvegarde garantit la **récupération** de vos données en cas d'incident (ex: vol ou panne).

Je banalise mes équipements

Evitez d'afficher partout le nom de votre employeur : retirez du matériel **les logos** qui peuvent l'être, ou a minima dissimulez-les lorsque vous vous déplacez (ex : badge, autocollant sur le PC, goodies...).

J'identifie les contacts d'urgence

Pour informer rapidement votre entreprise en cas de vol ou de fonctionnement anormal, il est nécessaire de connaître **à l'avance** les bons contacts chez votre employeur (RSSI, service informatique, etc.).

Pendant le déplacement

Je reste discret !

Dans les transports, pas de discussion sur des sujets sensibles : **les sièges ont des oreilles** ! En particulier dans les trajets menant à des salons, où il n'est pas rare d'avoir un concurrent juste à côté...

Je garde un œil sur mon matériel

Que ce soit pour aller aux toilettes dans le train, à un salon ou au restaurant, ne laissez pas votre matériel sans surveillance. A défaut pensez au moins à **verrouiller votre PC** avant de vous absenter ☺

J'utilise les outils fournis par l'employeur

Evitez d'utiliser du matériel ou des logiciels qui ne sont pas fournis par votre service informatique et potentiellement non-sécurisés (ex: clé USB personnelle, VPN gratuit trouvé sur Internet, etc.).

Je me méfie des Wi-Fi publics

Il est facile pour un attaquant de créer un point d'accès réseau et le diffuser sous un nom inspirant confiance (ex: _SNCF_WIFI_**GRATUIT**). Privilégiez un partage de connexion avec votre téléphone.

Je reste prudent à l'hôtel...

A l'hôtel, deux principaux risques se dégagent :

- **L'intrusion physique** : pensez naturellement à bien verrouiller votre chambre et placer votre matériel dans le coffre-fort si disponible. Astuce : en cas de doute sur la sécurité de votre chambre, n'hésitez pas à les confier à l'accueil.

- **L'interception des communications** : là encore, fuyez les WiFi d'hôtel ! Si vous souhaitez travailler à l'hôtel, utilisez un **VPN** (en général fourni par votre service informatique).

A propos de l'auteur : Nicolas GENET
Consultant en cybersécurité
Contact :