

Déplacements professionnels : protéger données et matériel en voyage

Train, hôtel, salon, étranger : le kit de survie numérique du collaborateur en déplacement.

7 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/securite-deplacements

En déplacement, tout change : le matériel sort du bureau, les écrans s'ouvrent dans les trains, les documents se présentent chez des tiers, et à l'étranger certaines frontières s'intéressent de près aux appareils. La sécurité en mobilité n'est pas de la paranoïa — c'est un petit ensemble d'habitudes qui évitent les incidents les plus fréquents : le vol, l'indiscrétion et la perte.

1. Avant de partir

- Le strict nécessaire : un portable chiffré (BitLocker/FileVault) et à jour, les seuls documents utiles au déplacement — le disque qui contient « tout » n'a rien à faire en voyage
- Sauvegarde complète avant le départ : le matériel perdu ou cassé ne doit emporter aucun travail
- Localisation et effacement à distance vérifiés sur portable ET téléphone
- Les accès prêts : VPN testé, MFA fonctionnelle sans dépendre d'un seul appareil (codes de secours accessibles)
- Pour les destinations sensibles : suivre les recommandations dédiées de l'ANSSI — appareil de prêt vidé, données minimales, briefing spécifique

2. Dans les transports et lieux publics

- Le filtre de confidentialité sur l'écran : à moins de 30 €, il rend la lecture latérale impossible — l'indiscrétion du voisin de TGV est LE grand classique
- Les conversations sensibles attendent : le wagon entier profite de votre point client au téléphone — noms, montants, différends compris
- Le matériel reste sur vous : jamais de portable dans la valise en soute ni de sacoche « juste deux minutes » sans surveillance
- Verrouillage systématique à chaque pause (Windows+L devient un réflexe), même « pour aller au wagon-bar »
- Connexions : la règle du Wi-Fi public s'applique en permanence

CAS CONCRET

L'expérience du filtre de confidentialité en TGV : sans lui, votre proposition commerciale — tarifs, marges, nom du client — se lit depuis deux sièges autour, et il se trouve que le monde professionnel est petit. Beaucoup d'histoires d'affaires perdues commencent par « quelqu'un a vu/entendu dans le train ». C'est l'accessoire au meilleur ratio discrétion/prix du marché.

3. À l'hôtel et chez les tiers

- Le coffre de la chambre pour le matériel qu'on ne prend pas — imparfait, mais dissuasif pour le vol d'opportunité
- Jamais de session ouverte sur l'ordinateur « en libre service » de l'hôtel ou du client pour vos comptes : ces machines sont hors de tout contrôle
- En présentation chez un client : un support dédié (la clé ou le dossier de LA présentation), pas votre session complète avec les emails qui surgissent
- Impressions et documents papier : ce qui se distribue se compte, ce qui se jette se déchire

4. Incidents en déplacement : réagir vite

- Vol ou perte : la procédure standard s'applique depuis n'importe où — verrouiller/effacer à distance, prévenir le référent, opposition opérateur, plainte locale
- Appareil saisi ou manipulé hors de votre vue (contrôle, réparation imprévue) : considérer l'appareil comme compromis — mots de passe changés au retour, poste vérifié avant reconnexion au réseau
- Le doute suffit : un comportement anormal après un déplacement se signale — c'est exactement le scénario où l'analyse préventive vaut le coup

L'essentiel à retenir

- 01 Partir léger : appareils chiffrés, données minimales, sauvegarde faite
- 02 Équiper les nomades de filtres de confidentialité
- 03 Verrouiller à chaque pause, ne jamais laisser le matériel sans surveillance
- 04 Appliquer la règle 4G/VPN pour toutes les connexions
- 05 Connaître la procédure perte/vol et l'appliquer sans délai
- 06 Considérer comme compromis tout appareil manipulé hors de vue

Questions fréquentes

Qu'est-ce qui change pour un déplacement à l'étranger ?

Selon la destination : certains pays pratiquent l'inspection des appareils aux frontières, la surveillance des réseaux, voire des intrusions ciblées sur les voyageurs d'affaires. Pour les destinations et secteurs sensibles, l'ANSSI publie un guide dédié (passeport de conseils aux voyageurs) : appareils de prêt épurés, pas de données sensibles locales, vigilance renforcée. Pour l'UE et destinations comparables, les règles standards de ce guide suffisent.

Puis-je utiliser l'ordinateur du business center de l'hôtel pour imprimer ?

Pour imprimer un document non sensible envoyé via un lien à usage unique, à la rigueur. Jamais pour vous connecter à vos comptes : ces machines partagées peuvent enregistrer les frappes. L'alternative moderne : l'impression depuis votre téléphone, ou la réception de vos documents à l'accueil.

Le responsable, c'est le voyageur ou l'entreprise ?

Les deux : l'entreprise fournit le cadre (matériel chiffré, filtres, VPN, procédure incident, briefing pour les destinations sensibles), le voyageur applique les gestes. Une demi-page « déplacement » dans la charte, remise avec le portable, aligne tout le monde.

Pour aller plus loin

ANSSI — passeport de conseils aux voyageurs — cyber.gouv.fr/publications/passeport-de-conseils-aux-voyageurs

Cybermalveillance.gouv.fr — la sécurité en déplacement — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr