G – À L'EXTÉRIEUR DE L'ENTREPRISE

G1. Se déplacer au quotidien

Parce qu'ils sont routiniers et prévisibles, les petits déplacements au quotidien exposent les acteurs économiques à d'importantes vulnérabilités facilitant la perte ou la fuite d'informations sensibles dont les conséquences peuvent s'avérer très préjudiciables à l'entreprise.

TECHNIQUE

➤ Installer un **filtre de confidentialité** sur les écrans des ordinateurs portables, des tablettes et des smartphones à usage professionnel.

COMPORTEMENTAL

➤ Éviter de transporter les données sensibles lors des déplacements quotidiens, notamment entre le domicile et le travail. Prévoir une **solution de chiffrement** (conteneur chiffré ou clé USB sécurisée).

➤ En cas d'utilisation des fonctions Wifi/Bluetooth des appareils nomades dans les transports en commun, garder à l'esprit que toute liaison peut être interceptée (dans ce cas, il est recommandé d'utilisé un **VPN**). Il est vivement conseillé de désactiver les fonctions Wifi/Bluetooth de vos appareils nomades utilisés à des fins professionnelles (smartphones, tablettes, ordinateurs portables) dans les transports en commun et espaces publics (gares, aéroports, salons professionnels, etc.)

➤ Éviter au maximum de parler de sujets professionnels dans les transports (métro, bus, taxis, trains, avions) et les espaces publics partagés (restaurants, cafés, salles d'attente, etc.)

➤ Dans un lieu public, rester discret dans ses lectures professionnelles (rapports, notes en cours, courriels, etc.).

➤ Taper discrètement ses identifiants et mots de passe d'accès à l'ordinateur, ou à sa messagerie.

➤ Privilégier les prises secteurs pour recharger vos appareils nomades plutôt que les prises USB afin d'éviter le risque d'aspiration de vos données (*juice-jacking*)

➤ Ne jamais laisser ses outils de travail (mallette, ordinateurs portables, téléphones, etc.) sans surveillance.

➤ Lors des déplacements en voiture, déposer discrètement ses affaires dans le coffre verrouillé et non sur la banquette arrière ou le siège passager. Lors des stationnements, ne pas laisser d'ordinateurs portables ou de documents contenant des données sensibles dans la voiture, même dans le coffre.

➤ Dans le cas d'une location, éviter les interfaces entre le smartphone et le véhicule afin d'éviter la récupération et le transfert de vos données (sms, contact, photos etc.). En cas d'utilisation du Bluetooth, penser à effacer les données présentes dans le système d'information du véhicule.

Mots clés

Filtre de confidentialité : film de protection qui se place sur un écran et qui restreint la vision des données affichées de part et d'autre de l'axe de vision.

Solution de chiffrement : outil permettant la transformation de données dans le but d'en cacher le contenu.

VPN : le réseau privé virtuel (en anglais *Virtual Private Network*), est un système permettant de créer un lien direct et généralement sécurisé par du chiffrement entre des ordinateurs distants.

Pour aller plus loin

➤ L'Anssi propose des solutions techniques de chiffrement sur son site Internet.