SYNTHESE DES BONNES PRATIQUES

1. Se connecter systématiquement au VPN

Sans VPN, toutes les données qui circulent entre l'entreprise et vous restent accessibles au hacker qui peut les récupérer.

2. Choisissez des mots de passe uniques pour chaque compte.

Des générateurs de mots de passe existent pour vous créer des mots de passe robustes, et des gestionnaires peuvent vous aider à les stocker. Evitez les post-it !



3. Pensez à séparer les usages pro/perso

Plus vous mélangez le pro/perso, plus c'est facile pour le hacker de passer de l'un à l'autre : lire vos mails pro sur votre smartphone perso, imprimer un document sur votre imprimante perso…

4. Prenez garde aux vols !

Le vol de matériel constitue également un risque important, en particulier pendant vos trajets domicile – travail.

5. Protéger le mot de passe de votre box WIFI

Pour que la connexion à votre box personnelle reste fiable et sécurisée, attribuez-lui un mot de passe assez robuste.

© Dæsign - Ces contenus sont protégés par le droit d'auteur. Leur reproduction est interdite sans l'accord préalable de Dæsign. La reproduction sur un support papier demeure autorisée aux conditions suivantes : usage non commercial, respect de l'intégrité des documents reproduits (ni modifications, ni altérations), citation claire et lisible du copyright Dæsign.