

Sécuriser le télétravail

VPN, poste dédié, Wi-Fi domestique : les règles pour travailler à distance sans exposer l'entreprise.

10 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/teletravail

En télétravail, le périmètre de sécurité de l'entreprise s'étend jusqu'au salon de chaque collaborateur. Sans cadre, chaque connexion domestique devient une porte d'entrée potentielle vers vos données.

1. Le poste de travail

- Un équipement professionnel dédié, fourni et géré par l'entreprise — pas l'ordinateur familial
- Disque chiffré (BitLocker, FileVault) : un portable volé ne doit rien révéler
- Session verrouillée dès qu'on s'éloigne, y compris à la maison
- Antivirus/EDR à jour et mises à jour automatiques activées
- Comptes séparés si le partage du poste est inévitable

2. La connexion

- Un VPN d'entreprise pour accéder aux ressources internes
- Wi-Fi domestique en WPA2/WPA3 avec un mot de passe robuste (pas celui d'origine de la box)
- Éviter les Wi-Fi publics ; préférer le partage de connexion 4G/5G du téléphone
- Double authentification sur tous les accès distants

3. Les usages

- Pas de transfert de documents professionnels vers des emails ou clouds personnels
- Attention aux oreilles et écrans indiscrets en espace partagé (train, café)
- Une procédure claire de signalement en cas de perte ou vol de matériel

4. Encadrer : la charte télétravail

Les règles techniques ne tiennent que si elles sont écrites, expliquées et signées. Une page suffit, annexée à la charte informatique :

- Équipement : usage professionnel du matériel fourni, interdiction d'y installer des logiciels personnels
- Connexion : VPN obligatoire pour les ressources internes, Wi-Fi publics interdits ou encadrés
- Données : aucun transfert vers des comptes ou clouds personnels, impression à domicile limitée aux documents non sensibles
- Incidents : qui prévenir, dans quel délai, en cas de perte, vol ou comportement anormal du poste
- Famille : le poste professionnel ne sert ni aux devoirs ni aux jeux — la moitié des infections domestiques passent par là

BON À SAVOIR

Le BYOD (travailler sur son ordinateur personnel) semble économique mais coûte cher en risque : machine non maîtrisée, antivirus incertain, données professionnelles mêlées à la vie privée. Si vous ne pouvez pas l'éviter, exigez au minimum un antivirus à jour, le chiffrement du disque, une session dédiée au travail et un accès uniquement via VPN et navigateur — sans synchronisation locale des fichiers.

L'essentiel à retenir

- 01 Fournir un poste professionnel dédié à chaque télétravailleur
 - 02 Chiffrer les disques de tous les portables
 - 03 Déployer un VPN avec double authentification
 - 04 Exiger un Wi-Fi domestique sécurisé (WPA2/WPA3, mot de passe changé)
 - 05 Rédiger une charte télétravail simple et la faire signer
 - 06 Définir la procédure en cas de perte ou de vol d'équipement
-

Questions fréquentes

Un VPN gratuit trouvé sur Internet fait-il l'affaire ?

Non — c'est même souvent pire que rien : les VPN gratuits grand public monétisent fréquemment vos données de navigation, et ils ne donnent de toute façon pas accès à votre réseau d'entreprise. Ce qu'il faut est un VPN d'entreprise (intégré à votre pare-feu, ou une solution dédiée) configuré par votre prestataire, avec double authentification.

Le collaborateur peut-il travailler depuis un café ou en voyage ?

Oui, avec trois précautions : partage de connexion 4G/5G du téléphone plutôt que le Wi-Fi public, filtre de confidentialité sur l'écran dans les lieux publics, et appareil jamais laissé sans surveillance. Pour les déplacements à l'étranger sensibles, l'ANSSI recommande même un équipement dédié vidé des données non nécessaires.

Comment sécuriser la visioconférence ?

Utilisez l'outil validé par l'entreprise (pas celui que propose l'interlocuteur du jour), activez les salles d'attente pour les réunions sensibles, ne partagez les liens qu'aux participants, et méfiez-vous des invitations de réunion inattendues par email — c'est devenu un vecteur de phishing courant.

L'employeur peut-il surveiller le poste en télétravail ?

La supervision de sécurité (antivirus, mises à jour, alertes) est légitime et nécessaire. La surveillance de l'activité du salarié, elle, est strictement encadrée par le droit du travail et le RGPD : proportionnée, transparente et déclarée. Les logiciels d'espionnage de productivité exposent l'employeur à des sanctions CNIL.

Pour aller plus loin

Cybermalveillance.gouv.fr — sécuriser le télétravail — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-teletravail

ANSSI — recommandations sur le nomadisme numérique — cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique

CNIL — télétravail et protection des données — www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail

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