

Chiffrement : protéger les données, du disque aux échanges

Portable volé, disque revendu, email intercepté : le chiffrement rend vos données illisibles pour tout le monde sauf vous.

9 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/chiffrement

Un ordinateur portable disparaît toutes les quelques secondes dans le monde. Sans chiffrement, quiconque le récupère lit tout — le mot de passe de session ne protège que l'ouverture de la session, pas le disque. Chiffrer, c'est garantir qu'une donnée perdue reste une donnée muette. C'est aussi une mesure explicitement citée par le RGPD.

1. Chiffrer les données « au repos »

- Postes et portables : BitLocker (Windows Pro) ou FileVault (Mac), inclus dans le système — il suffit de les activer
- Smartphones : chiffrés par défaut sur les versions récentes d'iOS et Android
- Disques externes et clés USB : chiffrement matériel ou logiciel obligatoire dès qu'ils sortent du bureau
- Serveurs et NAS : chiffrement des volumes contenant des données sensibles
- Point crucial : conserver les clés de récupération en lieu sûr (gestionnaire de mots de passe, coffre) — un disque chiffré dont la clé est perdue est définitivement perdu

2. Chiffrer les données « en transit »

- HTTPS partout : jamais d'identifiant saisi sur une page non sécurisée
- VPN pour tout accès distant aux ressources de l'entreprise
- Messagerie : vérifier que le TLS est actif chez votre fournisseur (standard aujourd'hui)
- Wi-Fi en WPA2/WPA3 — un Wi-Fi ouvert transmet en clair

3. Partager un document sensible

L'email n'est pas un canal sûr pour un document confidentiel : il traîne ensuite dans deux boîtes, des sauvegardes et des transferts. Pour l'occasionnel, une archive chiffrée (7-Zip en AES-256) dont le mot de passe transite par un autre canal (SMS, téléphone) fait l'affaire. Pour un besoin régulier, préférez un espace de partage sécurisé avec liens à expiration et droits par personne — plus simple et plus traçable.

4. La fin de vie du matériel : effacer avant de céder

Vendre, donner ou jeter un ordinateur, un téléphone, un disque ou même une imprimante (elles ont un disque interne) sans effacement sérieux revient à donner vos données avec. La corbeille et le formatage rapide n'effacent rien : les données se récupèrent avec des outils gratuits.

- Si le disque était chiffré : détruire la clé (réinitialisation d'usine sur mobile, rotation de la clé BitLocker)

rend les données définitivement illisibles — c'est l'énorme bonus du chiffrement systématique

- Sinon : effacement sécurisé par un outil dédié, ou destruction physique du support pour les données sensibles
- Tenir un registre des équipements sortants : quoi, quand, comment effacé — le RGPD peut vous demander de le prouver

CAS CONCRET

Des études régulières le confirment : une part significative des disques d'occasion achetés en ligne contiennent encore les données de leur ancien propriétaire — comptabilité, dossiers clients, mots de passe. Le portable de l'entreprise revendu 200 € peut coûter une notification CNIL et un préjudice d'image sans commune mesure.

L'essentiel à retenir

- 01 Activer BitLocker/FileVault sur tous les postes et portables
- 02 Stocker les clés de récupération en lieu sûr et centralisé
- 03 Chiffrer tout support amovible qui sort des locaux
- 04 Imposer VPN et HTTPS pour les accès distants
- 05 Définir un canal sécurisé standard pour les documents sensibles
- 06 Effacer ou détruire les supports avant revente, don ou mise au rebut

Questions fréquentes

Le chiffrement va-t-il ralentir nos ordinateurs ?

Non — les processeurs modernes chiffrent matériellement (AES-NI) : l'impact est imperceptible à l'usage. BitLocker et FileVault tournent d'ailleurs déjà par défaut sur beaucoup de machines récentes sans que personne ne le remarque. Il n'y a plus aucune raison de performance de s'en passer.

BitLocker demande une édition Windows Pro. Et nos postes en Windows Famille ?

Windows Famille propose parfois le « chiffrement de l'appareil » (selon le matériel), mais sans gestion fine. Pour un usage professionnel, la mise à niveau vers Pro se justifie de toute façon (BitLocker, stratégies de sécurité, jonction au domaine) — c'est un coût modeste par rapport au risque du portable perdu non chiffré.

Un ZIP avec mot de passe est-il vraiment sûr ?

Oui à condition d'utiliser le chiffrement AES-256 (celui de 7-Zip, pas l'antique « ZipCrypto ») avec un mot de passe long, transmis par un canal différent du fichier — le mot de passe dans le même email annule tout. Pour un besoin fréquent, un espace de partage sécurisé est plus pratique et plus traçable.

Faut-il chiffrer nos emails ?

Le transport est déjà chiffré (TLS) entre fournisseurs sérieux : vos emails ne circulent pas en clair sur Internet. Le chiffrement de bout en bout (le fournisseur lui-même ne peut pas lire) reste réservé aux échanges très sensibles, car il est contraignant. Dans la plupart des cas, la bonne réponse est : email normal pour l'ordinaire, lien de partage sécurisé pour le confidentiel.

Pour aller plus loin

CNIL — le chiffrement, mesure de sécurité de référence — www.cnil.fr/fr/securite-chiffrer-garantir-lintegrite-ou-signer

ANSSI — Guide d'hygiène informatique — cyber.gouv.fr/publications/guide-dhygiene-informatique

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

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