



Pourquoi agir maintenant ?

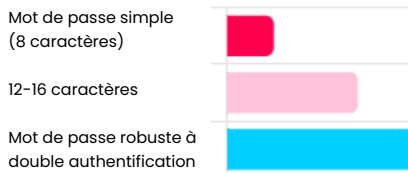
Votre trésorerie et vos données clients sont des cibles. La sécurité est une question de **gestion des risques**.

- ✓ Protégez votre activité
- ✓ Rassurez vos partenaires
- ✓ Assurez votre continuité d'activité

Les 6 piliers de votre sécurité numérique

1. Les mots de passe

Un mot de passe pour identifier. La **double authentification** pour confirmer votre identité grâce à un second moyen de vérification, même si votre mot de passe est compromis.



2. Les mises à jour

Les logiciels ont des failles que les pirates exploitent. Leur maintenance est nécessaire.



Règle d'or : Ne repoussez jamais les mises à jours. Configurez vos ordinateurs et smartphones pour qu'ils se mettent à jour automatiquement.

La technique a ses limites :

L'humain reste **une cible** . Le mail ciblé est une porte d'entrée privilégiée par les pirates. Le réflexe à adopter : Toujours vérifier une demande inhabituelle (Exemple : changement de RIB).

3. Les sauvegardes

Contre le blocage de votre système informatique, la sauvegarde immuable est la solution sans oublier des tests de restauration.

Disque
Utiliser un disque dur externe que vous débranchez impérativement après la copie.

ET

Cloud
Une prestation de sauvegarde externe automatisée et protégée.

4. La gestion des droits

Le principe du "Moindre privilège" : La sécurité commence par des accès limités.

Utilisateur
Pour le travail quotidien (web, email, bureautique). Si un virus infecte ce compte, ses dégats sont limités.

Administrateur
À n'utiliser **que** pour installer un logiciel ou modifier le système. Ne surfez jamais sur internet avec ce compte.

3 Actions Immédiates

1

Activez la **double authentification** sur vos emails professionnels.

2

Activez l'installation de mises à jour automatiques sur tous vos appareils et vérifiez qu'aucune mise à jour n'est en attente

3

Vérifier que vous disposez bien d'une **sauvegarde protégée** contre les attaques d'origine cyber (chez votre prestataire ou sur un disque déconnecté et hors site)

5. La sécurité internet

Activez votre pare-feu sur vos postes de travail et bloquez par défaut les flux entrant. Dès que possible, investissez dans un pare-feu physique.

Pare-feu Pro (Matériel)
Contrôle total des flux & VPN sécurisé

6. Le poste de travail

Antivirus : Les outils gratuits ou par défaut sont souvent insuffisants pour les entreprises. Investissez dans une suite de sécurité gérée (EDR)

Séparation stricte : Pas d'usages personnels (jeu, streaming illégal) sur le matériel pro.

Verrouillage : Touche **Windows + L** ou **Command + L** dès que vous quittez votre chaise, même pour 2 minutes.

Pour aller plus loin : <https://messervices.cyber.gouv.fr/cyberdepart>