Check List

LA CYBERSÉCURITÉ POUR L'OFFICINE

01 **Surveiller l'âge du hardware**

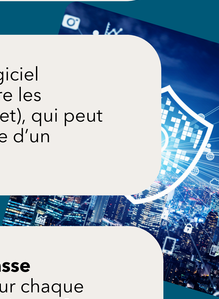
Un ordinateur obsolète risque de ne plus permettre l'installation des mises à jour de sécurité.

Indice : si le démarrage et l'arrêt du PC prennent du temps, qu'il "rame" et/ou que les erreurs sont fréquentes (écran bleu ou noir), il est sans doute temps de le renouveler.

02 **Effectuer dès que possible** les mises à jour des systèmes d'exploitation et des logiciels utilisés.

03 **Utiliser un antivirus,** complété de préférence par un anti-spam et une solution anti-hameçonnage pour sécuriser les messageries.

04 **Effectuer régulièrement des sauvegardes** (pouvant être locales ou externes) des données essentielles à l'activité de l'officine, ainsi que des tests de restauration. L'ANSSI conseille 3 copies de sauvegarde, sur 2 supports différents dont 1 hors ligne.



05 **Activer un pare-feu** (logiciel protégeant surtout contre les attaques venant d'Internet), qui peut être configuré avec l'aide d'un prestataire.

06 **Utiliser des mots de passe robustes :** différents pour chaque service, comptant au minimum 9 caractères pour les services peu critiques et 15 caractères pour les services critiques, et comportant des capitales, des minuscules, des chiffres et des caractères spéciaux.

07 **Sensibiliser l'équipe officinale aux risques cyber** et aux bonnes pratiques de sécurité, par une communication régulière et une charte des usages numériques remise aux nouveaux arrivants.

L'astuce supplémentaire !

Pour une sécurisation optimale, il est aussi possible de :

• Souscrire à un **contrat d'EDR** (« Endpoint Detection and Response »), un peu l'équivalent du gardiennage pour le périmètre informatique : cet antivirus de nouvelle génération, monitoré à distance par un prestataire, permet de détecter et bloquer les rançongiciels.

• Souscrire à des **clauses d'assurance spécifiques** contre les risques numériques.