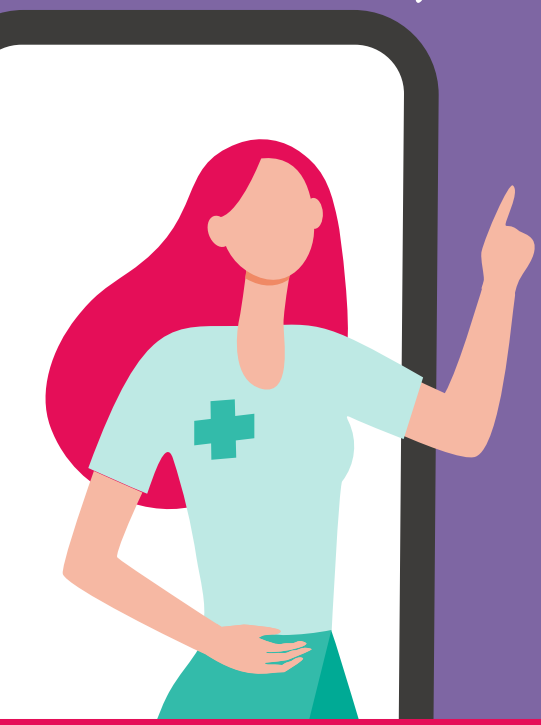
Avec le soutien de

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Le Collectif
Club des groupements d'officines et des partenaires santé

La e-santé en officine, c'est maintenant !



Sécurité numérique

Cybersécurisons l'officine !

Toute pharmacie peut un jour être la cible d'attaques informatiques. Ces attaques exposent à des incidents de sécurité qui peuvent impacter votre activité de façon sévère, voire irréversible. Alors que faire ? Voici **quelques règles d'hygiène informatique de base à adopter** pour protéger votre entreprise.

Concrètement, de quoi parle-t-on ?

Un incident de sécurité, c'est par exemple, le disque dur de votre ordinateur qui tombe en panne, et rend **tout ou partie de vos dossiers patients définitivement inaccessibles**. Ou encore, ces mêmes dossiers peuvent être rendus inexploitables en étant chiffrés par des pirates à l'aide d'un «rançongiciel» qu'ils ont réussi à introduire. Ces pirates vous proposent ensuite de restaurer l'accès à ces données contre une rançon (cette promesse étant tenue après paiement… ou pas).

Quels sont les vecteurs d'attaque les plus courants ?

La messagerie électronique reste la porte d'entrée privilégiée des hackers pour accéder aux données.

L'exploitation de failles non corrigées des outils informatiques qui peuvent être exploitées par les cybercriminels.

À noter

En tant que pharmacien, il est de votre responsabilité d'assurer la sécurité des données de vos patients. Ainsi, il est juridiquement possible de vous attaquer si les données qui vous ont été confiées ont été diffusées. Une cyber-assurance peut rassurer, toutefois il faudra bien analyser les éléments couverts par cette assurance.

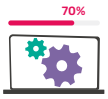
Les bonnes pratiques à adopter

01 Sauvegarder les données

- Ceci permet de **restaurer le système** en cas d'incident.
- **Tester la restauration** pour s'assurer qu'elle fonctionne.
- **Les sauvegardes doivent être déconnectées** dans la mesure du possible afin de les protéger de toute atteinte suite à une cyberattaque (notamment chiffrement par un ransomware).
- En cas d'utilisation d'un **disque dur externe personnel, veiller à ce qu'il soit chiffré**. Idéalement, le support des sauvegardes doit être dupliqué et conservé à deux endroits différents (ex : un à la pharmacie, un autre au domicile)

À noter :
D'autres solutions existent et sont proposées par des professionnels (ex : des solutions de type cloud). Bien veiller à ce que le stockage soit réalisé sur un hébergement certifié HDS (hébergement de données de santé).

02 Mettre à niveau le système et les outils logiciels



- Veiller à la mise à niveau du système et des outils logiciels est au moins **aussi important que tenir son antivirus à jour.**
- **C'est l'ensemble de ces mesures qui assure la sécurité**. Maintenir à jour l'antivirus d'un système d'exploitation obsolète n'est pas suffisant.

03 Utiliser des mots de passe robustes

- Choisir un mot de passe d'au moins **12 caractères**
- Utiliser une combinaison de **minuscules, de majuscules, de chiffres et de caractères spéciaux** (# » !-…)
- Choisir un mot de passe **non prédictible** (Ex : pas de date de naissance)
- S'assurer qu'il est **mémorisable** sans avoir à le noter. Privilégier une approche mnémotechnique pour s'en souvenir.
- Utiliser **un mot de passe unique pour chaque compte**
- Utiliser un **gestionnaire de mots de passe** pour gérer les différents mots de passe (Ex : KeePass Password Safe).

04 Respecter les règles de sécurité pour l'usage des cartes CPx et e-CPS

- Respecter leur caractère **personnel et strictement incessible**
- **Garder secret** le code PIN et le code PUK
- Maintenir la carte **en lieu sûr** lorsqu'elle n'est pas utilisée.

Attention :
- Si vous recevez sur votre téléphone une demande d'authentification e-CPS qui vous paraît suspecte, vous devez refuser l'accès ou ignorer la demande
  Plus d'infos : 0825 85 2000 (0,06 Euros/min + prix d'un appel local).
- Si vous suspectez une utilisation frauduleuse de votre carte CPS ou e-CPS, nous vous invitons à porter plainte et à vous rapprocher de votre caisse d'assurance maladie au **36 08** (service gratuit + prix appel).

05 Séparer les usages professionnels des usages personnels

Par exemple, **ne pas connecter de supports amovibles personnels** sur un équipement professionnel.

06 Utiliser une messagerie sécurisée de santé

Des échanges fiables et sécurisés seront possibles entre les professionnels de santé et leurs patients **via Mon Espace Santé.**

07 Respecter les principes du Règlement Général sur la protection des données (RGPD)

Le RGPD, qu'est-ce que c'est ?

08 Intégrer la sécurité dans les contrats avec les tiers

En savoir plus

09 Sécuriser son WIFI

- **Recommander l'utilisation de protocoles sécurisés** (WPA2 ou WPA3)
- Mettre (ou laisser) **un mot de passe complexe.**
- **Mettre son matériel à jour** (box, routeur wifi..) afin de limiter les risques de failles.

10 Protéger l'accès au poste de travail en cas d'absence

11 Détruire les données qui doivent être supprimées

Votre prestataire informatique est votre interlocuteur clé. N'hésitez pas à le solliciter pour adopter ces bonnes pratiques.

Que faire en cas d'attaques ?

Poste bloqué par un « cryptovirus » qui affiche une demande de rançon, présence d'un programme inconnu qui se lance au démarrage… Si un incident de sécurité informatique est constaté ou suspecté, il est recommandé d'appliquer en premier lieu les mesures suivantes :

1. **Déconnecter le câble réseau ou désactiver le WIFI** sur le poste sur lequel l'incident est suspecté

2. **Maintenir la machine sous tension, ne pas l'arrêter, ni la redémarrer e**t ne plus interagir avec le poste afin de conserver l'information utile pour l'analyse de l'attaque.

3. **Prévenir le fournisseur informatique**

4. **Décrire l'incident de sécurité sur le site cybermalveillance.gouv.fr** et suivre les conseils proposés

www.cybermalveillance.gouv.fr/diagnostic/accueil

« C'était vraiment la galère ! »

« En ouvrant mon officine, j'ai très vite compris… il y avait une demande de rançon. Avec l'équipe, on a eu les bons réflexes : contacter notre service informatique et ne toucher à rien. Mais c'était trop tard ! Tous les postes étaient infestés, malgré l'antivirus. Pendant 2 jours, pas de caisses, plus d'historique, copie des ordonnances… Il a fallu saisir plus de 400 dossiers à la main, et rappeler tous les patients pour les règlements. »

Prune Boudet, pharmacienne titulaire
à Saint-Éloy-les-Mines (Puy-de-Dôme)

« Un petit choc ! »

« Le stress est monté devant le message en anglais indiquant que les fichiers de l'officine étaient cryptés. Mes premiers réflexes : débrancher l'ordinateur et contacter mon informaticien. Il est intervenu du samedi midi au dimanche soir pour restaurer les données dans un autre ordinateur. Cela a pris du temps mais on a pu ouvrir le lundi matin. Cet incident m'a incité à réfléchir à mettre en place des mesures de prévention (doubles sauvegardes, firewall…). J'ai aussi déposé plainte et contacté mon assureur qui venait d'ouvrir un service dédié. Personne n'est à l'abri »

Raphaël Gigliotti, pharmacien titulaire à Nice (Alpes-Maritimes)

Pour vous accompagner utilement, l'Agence du numérique en santé propose :

Le Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

Une checklist des mesures d'hygiène informatique

à mettre en œuvre qui, si elles sont appliquées de façon stricte et régulière, peuvent vous permettre de vous prémunir contre la majorité des attaques.

Télécharger la fiche synthétique

Télécharger le mémento complet

Des questionnaires à faire remplir par votre prestataire de service informatique

afin de vérifier qu'il respecte bien les bonnes pratiques essentielles au vu de votre activité. Il est fortement recommandé que le prestataire s'engage formellement sur l'exactitude de ses réponses en datant et signant les questionnaires renseignés.

Démarches et liens utiles

En cas de violation de données à caractère personnel

Vous pensez être victime d'un acte de cybermalveillance

Signaler un spam (ou courriers indésirables)

Assistance aux victimes de cybermalveillance

Comprendre les menaces et agir