

GUIDE DES BONNES PRATIQUES DU NUMÉRIQUE EN OFFICINE



✓ LES BONS RÉFLEXES AU QUOTIDIEN



Gestionnaire de mots de passe

→ Utilisez des KeePass ou un équivalent : jamais de post-it !



Double authentification (Authenticator)

→ Activez une double authentification sur tous les accès sensibles



Messagerie MSSanté

Jamais utiliser Gmail, Yahoo...
→ pour des données patients : utilisez que MSSanté !



Verrouillage de session à chaque absence

→ Windows + L : verrouillage même pour 2 minutes



Mises à jour régulières

→ Antivirus, LGO, box internet...



Données anonymisées avec l'IA

Aucun nom de patient dans ChatGPT ou outil IA grand public



Sauvegardes 3-2-1-0-1

→ 3 copies
→ 2 supports
→ 1 hors site
→ 1 hors ligne
→ 0 erreur



RECONNAÎTRE UN EMAIL FRAUDULEUX



Ton urgent ou alarmiste

Bon réflexe

Vérifiez l'URL



Expéditeur légèrement modifié

Bon réflexe

Appelez l'organisme



Pièce jointe inattendue

Bon réflexe

Ne l'ouvrez pas



QR code non sollicité (quishing)

Bon réflexe

Ne scannez pas



SE PRÉPARER : QUESTIONS CLÉS

• Avez-vous listé vos systèmes dits « critiques » ?

LGO, messagerie, sauvegardes, TPE... ainsi que leurs alternatives manuelles.

• Qui fait quoi dans les quatre premières heures ?

Désignez un responsable de crise et répartissez les rôles.

• Vos contacts d'urgence sont-ils accessibles hors ligne ?

Prestataire informatique, banque, 17Cyber, CNIL, Ordre des Pharmaciens...

• Avez-vous effectué des sauvegardes ?

Une sauvegarde non testée n'est pas une véritable sauvegarde.



5 ÉTAPES EN CAS DE CYBERATTAQUE

• Isoler la machine infectée

- Débranchez le câble réseau.
- Désactivez le Wi-Fi.
- N'éteignez pas l'ordinateur (afin de préserver les preuves).

• Contacts d'urgence

- 17cyber.gouv.fr : 24h/24h et 7j/7.
- Si virement suspect : appelez votre banque immédiatement.

• Appeler votre prestataire informatique

- Ne réinstallez rien vous-même.
- Conservez les preuves (captures d'écran...) avant toute intervention.

• Déposer plainte

- Auprès de la police ou de la gendarmerie : une cellule cyber est présente dans chaque département.

• En cas de fuite de données, alertez la CNIL.

- Délai légal : 72 heures maximum (cnil.fr).
- Informez également les patients concernés.



URPS Pharmaciens
Centre-Val de Loire



CONTACTS UTILES



NE JAMAIS PAYER LA RANÇON

Payer ne garantit pas la récupération de vos données.



Cela finance les cybercriminels et attire de nouvelles attaques.

17cyber.gouv.fr	Signalement incident (24h/24)
cybermalveillance.gouv.fr	Prestataires référencés, conseils
cnil.fr	Notification fuite données (72h)
signal-spam.fr	Signaler un email frauduleux
ordre.pharmacien.fr	Accompagnement & signalement

RETROUVEZ +
D'INFORMATIONS

