



LE RISQUE CYBER A L'HÔPITAL

Un clic peut tout changer ! – Le guide des bons réflexes cyber

POURQUOI UN HÔPITAL EST-IL UNE CIBLE PRIVILÉGIÉE ?

Les établissements de santé figurent parmi les cibles les plus attaquées en France.

Plusieurs raisons expliquent cet intérêt des cybercriminels :



LES DONNÉES MÉDICALES
ONT UNE TRÈS FORTE VALEUR MARCHANDE.



UN HÔPITAL
NE PEUT PAS INTERROMPRE
SON ACTIVITÉ LONGTEMPS.



LES CONSÉQUENCES HUMAINES
D'UNE PANNE INFORMATIQUE POUSSENT
PARFOIS LES VICTIMES À CÉDER RAPIDEMENT
AUX EXIGENCES DES PIRATES.



LES ÉQUIPEMENTS MÉDICAUX
SONT NOMBREUX, PARFOIS ANCIENS
ET DIFFICILES À METTRE À JOUR.



**LES HÔPITAUX SONT AU CŒUR
DES ATTENTIONS DES CYBERCRIMINELS**



UNE CYBERATTAQUE N'EST DONC PLUS UNE HYPOTHÈSE
MAIS **UN RISQUE MAJEUR** QUI DOIT ÊTRE INTÉGRÉ
AU MÊME NIVEAU QU'UN INCENDIE, UNE PANNE ÉLECTRIQUE
OU UNE CATASTROPHE SANITAIRE.

LES PRINCIPAUX RISQUES CYBER

Comprendre les menaces pour mieux se protéger



1 LE PHISHING (HAMEÇONNAGE)

C'est aujourd'hui la première porte d'entrée des pirates.

EXEMPLE

Vous recevez un mail :

"Votre mot de passe expire aujourd'hui. Cliquez ici pour le renouveler."

Ou encore :

"Vous avez reçu une facture."

En cliquant sur le lien ou en ouvrant la pièce jointe, le logiciel malveillant s'installe.

CONSÉQUENCES

- vol du mot de passe
- prise de contrôle de la messagerie
- infection de tout le réseau
- vol de données médicales

2 LE RANSOMWARE (RANÇONGICIEL)

C'est le scénario le plus redouté.

EXEMPLE

Un ransomware est un logiciel malveillant qui bloque l'accès à vos fichiers et demande une rançon pour les débloquer.

Exemple :

Le ransomware "WannaCry" a chiffré les fichiers de milliers d'établissements dans le monde en 2017, paralysant de nombreux services.

CONSÉQUENCES

- impossibilité d'accéder aux dossiers patients
- retour au papier
- déprogrammation d'interventions
- transfert de patients
- fermeture de services

3 LE VOL DE DONNÉES

Les pirates cherchent à récupérer :

- identité des patients
- comptes-rendus médicaux
- résultats biologiques
- données RH
- informations bancaires
- identifiants

Ces données sont revendues ou utilisées pour des fraudes.



4 LE PIRATAGE DES COMPTES

Un mot de passe faible ou réutilisé permet à un pirate de se connecter comme un utilisateur légitime.

Il peut alors :

- consulter des dossiers patients
- envoyer des mails frauduleux
- supprimer des fichiers
- installer des virus



5 LES CLÉS USB INFECTÉES

Une simple clé USB peut contenir un logiciel malveillant.

Une fois branchée :

- le virus se diffuse automatiquement ;
- il peut contaminer tout le réseau.



6 LES OBJETS CONNECTÉS

Aujourd'hui un établissement possède :

- pompes à perfusion
- ECG
- échographes
- imprimantes
- télévisions connectées
- automates
- caméras



LA CYBERSÉCURITÉ EST L'AFFAIRE DE TOUS.
CHAQUE GESTE COMPTE POUR PROTÉGER NOS PATIENTS,
ET NOS RÉSIDENTS, NOS DONNÉES ET NOTRE ÉTABLISSEMENT.



LES CONSÉQUENCES POUR UN ÉTABLISSEMENT

⚠ UNE CYBERATTAQUE PEUT PROVOQUER :



IMPACT SUR LES SOINS



impossibilité d'accéder au DPI



erreurs médicamenteuses



retard de prise en charge



reports d'intervention



perte de traçabilité



IMPACT ORGANISATIONNEL



retour au papier



surcharge de travail



perte de temps



saturation du standard



perturbation des admissions



IMPACT FINANCIER



coût de restauration
informatique



interruption d'activité



perte de recettes



pénalités éventuelles



IMPACT JURIDIQUE



Violation :

- RGPD
- secret médical
- obligations de sécurité



IMPACT SUR L'IMAGE

Une cyberattaque entraîne souvent :



médiatisation



perte de confiance



inquiétude des familles



atteinte à la réputation



PROTÉGER NOS SYSTÈMES,
C'EST PROTÉGER NOS PATIENTS, NOS RESIDENTS
NOTRE ÉTABLISSEMENT ET NOTRE AVENIR.

LES CONDUITES À TENIR



EN CAS DE MAIL SUSPECT

TOUJOURS :

- ✓ vérifier l'expéditeur
- ✓ lire attentivement l'adresse mail
- ✓ vérifier les fautes d'orthographe
- ✓ se méfier des demandes urgentes
- ✓ contacter l'expéditeur par téléphone si besoin
- ✓ signaler au service informatique



SI UN ORDINATEUR SEMBLE INFECTÉ

FAIRE IMMÉDIATEMENT :

-  débrancher le câble réseau si possible
-  couper le Wi-Fi
-  laisser l'ordinateur allumé (sauf consigne contraire du service informatique)
-  prévenir immédiatement le service informatique
-  prévenir son encadrement ou le référent DPI.



NE PAS ATTENDRE.
UNE MINUTE PEUT SUFFIRE
À CONTAMINER TOUT LE RÉSEAU.



EN CAS DE PERTE D'UN ORDINATEUR

INFORMER IMMÉDIATEMENT :

-  le responsable informatique
-  le DPO si nécessaire
-  la direction



EN CAS DE PERTE D'UN TÉLÉPHONE PROFESSIONNEL

MÊME RÉACTION QU'EN CAS DE PERTE D'UN ORDINATEUR, PRÉVENIR :

-  le responsable informatique
-  le DPO si nécessaire
-  la direction



**LA RÉACTIVITÉ ET LA VIGILANCE DE CHACUN
SONT NOTRE MEILLEURE PROTECTION.**



LES CHOSES À NE JAMAIS FAIRE



ADOPTONS LES BONS RÉFLEXES,
PROTÉGEONS NOS DONNÉES
ET NOS PATIENTS

❌ 1. CLIQUER SUR UN LIEN SANS VÉRIFIER

Même si le mail semble provenir :

- de la Direction
- de Microsoft
- de l'ARS
- de la CPAM
- d'un laboratoire
- d'un fournisseur

Toujours vérifier.



❌ 2. OUVRIR UNE PIÈCE JOINTE INATTENDUE

Exemples :

- facture
- devis
- CV
- bon de livraison
- PDF inconnu

Même si l'expéditeur paraît connu.



❌ 3. BRANCHER UNE CLÉ USB PERSONNELLE

Jamais.

Même pour :

- une photo
- un document Word
- un CV
- une présentation



❌ 4. INSTALLER UN LOGICIEL

Même gratuit.
Même connu.

Toute installation doit
être validée par le
service informatique.



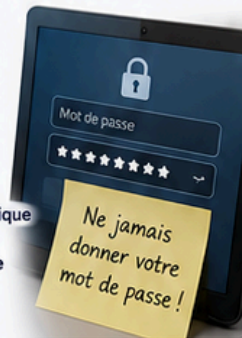
❌ 5. DONNER SON MOT DE PASSE

Jamais.

Même :

- à un collègue
- au cadre
- à un médecin
- au service informatique

Le support informatique
ne demandera jamais
votre mot de passe.



❌ 6. ÉCRIRE SON MOT DE PASSE SUR UN POST-IT

Erreur encore très fréquente.

Également interdit :

- sous le clavier
- dans un tiroir
- sur l'écran



❌ 7. UTILISER LE MÊME MOT DE PASSE PARTOUT

Si votre mot de passe est
compromis sur un site
personnel, il pourra être
testé sur les applications
professionnelles.



❌ 8. QUITTER SON POSTE SANS VERROUILLER LA SESSION

Toujours utiliser :



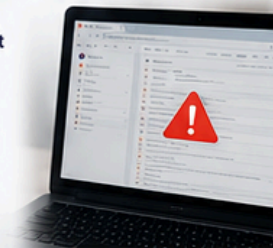
Quelques secondes
suffisent pour consulter
un dossier patient ou envoyer
un mail frauduleux sous
votre identité.



❌ 9. UTILISER SA MESSAGERIE PROFESSIONNELLE À DES FINS PERSONNELLES

Cela augmente fortement
le risque :

- de phishing ;
- de spam ;
- d'infection.



❌ 10. ENVOYER DES DONNÉES MÉDICALES NON SÉCURISÉES

Jamais :

- via Gmail
- via Outlook personnel
- via WhatsApp
- via Messenger
- par SMS

Toujours utiliser les outils
sécurisés de l'établissement.



❌ 11. CONTOURNER LES RÈGLES DE SÉCURITÉ

Exemples :

- désactiver l'antivirus ;
- prêter son badge ;
- partager un compte utilisateur ;
- utiliser un compte générique sans autorisation ;
- laisser une session ouverte.



LA SÉCURITÉ NUMÉRIQUE EST **L'AFFAIRE DE TOUS.**
UN BON RÉFLEXE AUJOURD'HUI, C'EST ÉVITER UNE CRISE DEMAIN.





LES MOTS DE PASSE : PREMIÈRE BARRIÈRE CONTRE LES CYBERATTQUES

Le mot de passe constitue la **première ligne de défense** du système d'information hospitalier. Un mot de passe faible ou réutilisé peut permettre à un cybercriminel d'accéder aux applications métiers, aux dossiers patients, à la messagerie professionnelle ou aux données administratives. Il est donc **essentiel** que chaque professionnel adopte de bonnes pratiques.



LES RÈGLES À RESPECTER



CHOISIR UN MOT DE PASSE COMPLEXE,
composé d'au moins **12 caractères**, associant :

- des lettres majuscules ;
- des lettres minuscules ;
- des chiffres ;
- des caractères spéciaux (ex. : !, ?, @, #, %, &, *).



*Ma maison
bleue ! 2026*

PRIVILÉGIER UNE PHRASE DE PASSE,
plus facile à mémoriser et plus difficile à deviner, par
exemple en combinant plusieurs mots sans lien entre eux,
des chiffres et des caractères spéciaux.



**UTILISER UN MOT DE PASSE DIFFÉRENT
POUR CHAQUE APPLICATION.**

Un mot de passe utilisé à la fois pour un compte personnel
(messagerie, réseaux sociaux, sites marchands) et pour un compte
professionnel expose l'établissement à un risque important en cas de fuite de données.



NE JAMAIS COMMUNIQUER SON MOT DE PASSE,
y compris à un collègue, à un supérieur hiérarchique ou
au service informatique. Les équipes informatiques n'ont
jamais besoin de connaître votre mot de passe.



NE JAMAIS ENREGISTRER SON MOT DE PASSE
sur un papier, un Post-it ou dans un fichier non sécurisé.



À RETENIR

Un mot de passe robuste, unique et bien protégé
est l'un des moyens les plus efficaces pour protéger
les données de santé et exercer notre mission
en toute sécurité.



**UN BON MOT DE PASSE,
C'EST LA SÉCURITÉ DE TOUS !**





CHANGER RÉGULIÈREMENT SON MOT DE PASSE

Le changement du mot de passe doit être réalisé **chaque fois que l'établissement le demande**, conformément à sa politique de sécurité.

Il est également impératif de le **modifier immédiatement** dans les situations suivantes :



vous pensez qu'il a été divulgué ou compromis ;



vous avez cliqué sur un lien suspect ou saisi vos identifiants sur un site douteux ;



vous constatez une activité inhabituelle sur votre compte ;



le service informatique vous informe d'un incident de sécurité.



Lors d'un changement, ne réutilisez jamais un ancien mot de passe

et évitez les variantes trop simples (par exemple Motdepasse2026! puis Motdepasse2027!), facilement détectables par les outils utilisés par les cybercriminels.



LES ERREURS

À NE JAMAIS COMMETTRE



✗ Utiliser des informations personnelles

(nom, prénom, date de naissance, prénom d'un enfant, nom de l'établissement).

Nom : DUPONT
Prénom : Jean
Né le : 12/05/1985



✗ Choisir un mot de passe trop simple

comme Azerty123, Password, Bienvenue2026 ou 123456.

Azerty123 *****



✗ Réutiliser le même mot de passe

sur plusieurs applications professionnelles ou personnelles.



✗ Valider automatiquement l'enregistrement des mots de passe dans un navigateur partagé.

Enregistrer le mot de passe ?

Enregistrer

Jamais



Un mot de passe robuste et bien géré, c'est la sécurité de vos données et de vos patients.



LES 10 RÉFLEXES

— À RETENIR —

Ensemble, protégeons notre système d'information et les données de santé



1

Je réfléchis avant de cliquer.



2

Je protège mon mot de passe.



3

Je verrouille mon poste.



4

Je ne branche jamais de clé USB inconnue.



5

Je ne partage jamais mon compte.



6

Je vérifie les expéditeurs.



7

Je signale immédiatement tout comportement anormal.



8

Je protège les données des patients.



9

Je respecte les procédures informatiques.



10

En cas de doute, je contacte le service informatique.



LA CYBERSÉCURITÉ,
l'affaire de tous !

Agissons chaque jour pour la sécurité de notre établissement et la protection des données de santé.



UNE QUESTION ? UN DOUTE ?
Contactez le service informatique

La vigilance de chacun
est notre meilleure protection.



8