

# Se préparer et réagir à une cyberattaque



## Anticipation

- Exercices pour la continuité d'activité en mode dégradé.
- Préparation à des échanges transversaux.
- Cartographie papier du système de stockage.
- Kits de communication papier pour les situations de crise.



## Formation

- Importance des mots de passe sécurisés.
- Sensibiliser à la technique du phishing.
- Adoption des bonnes pratiques pour minimiser les erreurs humaines.

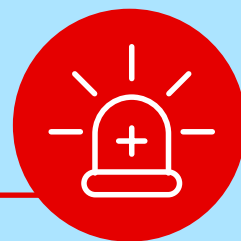


## Pharmacies



## Sécurisation

- Protection des outils numériques (ordinateurs, réseaux, etc).
- Sauvegardes régulières hors réseau.
- Utilisation d'équipements full-web.
- Disposition d'un ordinateur et d'une imprimante hors réseau.
- Mise en place d'un plan de sauvegarde informatique connu de tous.



## Réaction

- Suivi des instructions du service informatique.
- Participation à la cellule de crise.
- Activation immédiate du mode dégradé (retour au papier).
- Préparation pour un retour à la normale sur le long terme.