

CYBERSÉCURITÉ

Quelques règles clés à respecter



Dans le cadre de votre activité, vous vous appuyez sur les outils informatiques (ordinateurs, messageries, tablettes, smartphones, etc.). Ces usages vous exposent à des incidents de sécurité qui peuvent impacter votre activité de façon sévère, voire irréversible. Vous êtes par ailleurs tenu de mettre en œuvre des mesures garantissant la sécurité des données sensibles que vous manipulez et ne disposez parfois pour cela que de moyens techniques limités et de peu de temps disponible.

Bonnes pratiques •

- Inventoriez votre parc informatique
- Sauvegardez vos données régulièrement
- Protégez vos accès avec des mots de passe solides
- Utilisez un antivirus
- Appliquez les mises à jour de sécurité sur tous vos appareils, et ce, dès qu'elles vous sont proposées
- Sensibilisez vos collaborateurs

Si vous souhaitez approfondir le sujet, l'Agence du Numérique en Santé (ANS) met à disposition des professionnels de santé un certain nombre d'outils permettant de se prémunir contre les risques de cyberattaque.

Elle propose notamment un **Mémento de sécurité informatique** pour les professionnels de santé en exercice libéral.

Dans ce document, l'ANS propose une checklist pour les libéraux des principes et mesures d'hygiène informatique à mettre en œuvre. Pour les 12 grands principes listés, un certain nombre d'actions sont détaillées.

Télécharger le [Kit Communication Cybersécurité pour le Secteur Santé](#)

Pour aller plus loin : [CNIL-Guide de la sécurité des données personnelles](#) [ANSSI-Guide TPE/PME](#)