

Les bonnes pratiques



Pour **protéger votre ordinateur et les données de votre cabinet**, bannissez les **clés USB et disques durs externes personnels** qui peuvent être endommagés et causer la perte de vos données.



Verrouillez **votre session** dès que vous quittez votre poste, même pour une petite pause café !



Choisissez un **mot de passe robuste** de 12 caractères mêlant majuscules, minuscules, chiffres et caractères spéciaux.



Évitez d'utiliser les mêmes **mots de passe** pour vos activités professionnelles et personnelles. **Variez les mots de passe** pour chaque service, logiciel ou application.

Utilisez un coffre-fort numérique pour générer et stocker vos mots de passe en toute sécurité.



Lors de vos déplacements, évitez de vous connecter à des **réseaux Wi-Fi publics non sécurisés**.

Ces réseaux sont souvent exposés aux **attaques malveillantes**, pouvant conduire à une **violation de vos données**.



Les ressources du cabinet peuvent être utilisées à des fins personnelles, tant que cela reste raisonnable.

Pour garantir la **confidentialité des données personnelles**, pensez à les classer dans des dossiers nommés "Personnel".