



10 recommandations pour renforcer la sécurité numérique



1 Sécurisez vos mots de passe :

- ne le partagez pas, ne l'affichez pas
- spécifique et unique :
1 compte = 1 mot de passe
- 12 caractères minimum mélangeant majuscules, minuscules, chiffres et caractères spéciaux.



2 Privilégiez un gestionnaire de mots de passe ou un trousseau d'accès sécurisés stockés de préférence en local, pour conserver vos mots de passe en sécurité.



3 N'enregistrez pas vos mots de passe dans un ordinateur partagé. Déconnectez-vous en partant afin que vos mots de passe et vos sessions ne soient pas eux aussi partagés (ex. : dans un hôtel, une salle de classe, etc.).



4 Ne connectez jamais à votre ordinateur un support amovible (clé USB, etc.) dont vous ne connaissez pas l'origine.



5 Ne téléchargez pas ou n'installez pas de logiciel non autorisé ou vérifié. Seul le téléchargement depuis des sources fiables (site de l'éditeur, ou via les services académiques par exemple) est autorisé sur vos matériels.



6 Utilisez un anti-virus à jour et ne le désactivez jamais. Un anti-virus permet de détecter une grande partie des menaces s'il est bien à jour. Ne désactivez jamais un anti-virus ; les logiciels malveillants invitent à le désactiver pour pouvoir s'installer.



7 Surveillez vos équipements. Verrouillez systématiquement votre session de travail et déconnectez-vous des services auxquels vous avez eu accès depuis des ordinateurs partagés.



8 Méfiez-vous des messages inattendus. Par exemple, ceux qui viennent d'un interlocuteur inhabituel. Au moindre doute, ne les ouvrez pas, ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe : ces messages peuvent vous piéger pour dérober des informations confidentielles ou installer un virus.



9 Séparez vos usages privés et professionnels. Par exemple, n'utilisez pas votre adresse de messagerie professionnelle pour des usages personnels. N'utilisez pas non plus des services grand public de la sphère privée pour traiter des données professionnelles.



10 Appliquez les mises à jour de sécurité sur tous vos appareils dès qu'elles vous sont proposées. Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour vous voler vos données et mots de passe.