

Sécurisez l'accès à vos appareils

Ne laissez pas vos ordinateurs, tablettes, clés USB, disques durs externes ou smartphones sans surveillance et n'oubliez pas de verrouiller vos appareils en quittant votre siège !

Ne divulguez pas vos mots de passe

Pas de pense-bête apposé sur votre ordinateur pour vous souvenir de vos mots de passe ! Votre voisin de siège pourrait en être friand.

Évitez les regards en coin

Utilisez un filtre d'écran ou réduisez la luminosité afin de limiter la visibilité de votre écran pour les autres passagers.

Choisissez des mots de passe solides

Pour votre compte Mon identifiant SNCF, choisissez un mot de passe en béton et différent de vos autres comptes en ligne.

En manque d'inspiration ? Pour générer des mots de passe efficaces et les conserver de manière sécurisée, vous pouvez utiliser un gestionnaire de mots de passe.

Ne donnez pas tout de suite vos données !

Méfiez-vous des messages inattendus et alarmants se revendiquant d'organismes officiels (banque, administration, SNCF...), il peut s'agir d'une tentative d'hameçonnage. N'envoyez jamais vos informations personnelles avant d'avoir vérifié l'origine du message, par exemple en allant sur le site officiel depuis votre navigateur au lieu de cliquer sur un lien présent dans le message reçu.

Protégez vos données en ligne

- Gardez en tête que certains réseaux Wi-Fi, notamment publics, ne sont pas aussi sécurisés qu'au bureau ou à la maison ; vérifiez toujours que le site est bien sécurisé (affichage d'un petit cadenas ou de la mention « https »).
- Ne pré-enregistrez pas vos informations en ligne dans votre navigateur.
 - Et pour vos achats en ligne, retrouvez les conseils de la CNIL.

HISTOIRE VRAIE

Un passager critiquait ouvertement son employeur dans une conversation privée avec un collègue sur un réseau social.

Manque de chance : son voisin de siège et son supérieur étaient de bons amis. Protéger son écran, c'est aussi protéger sa vie privée.

Retrouvez plus de conseils sur [cnil.fr](https://www.cnil.fr)