



# CYBER RÉFLEXES

## inéa

De bons gestes à adopter

# GRADEs

# inéa

Sant& Numérique  
Hauts-de-France



# 1 MOT DE PASSE SOLIDE ET DIFFÉRENT POUR CHAQUE COMPTE

## BONNES PRATIQUES

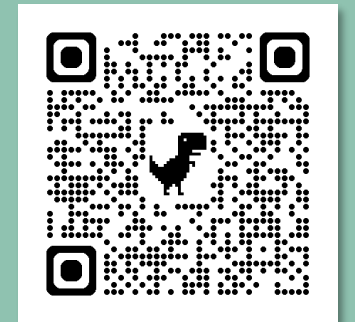
Utilisez des mots de passe d'**au moins 12 caractères**, incluant majuscules, chiffres, caractères spéciaux.

**Évitez les informations personnelles** : date de naissance, prénom, nom, etc.

Changez-les **régulièrement**, ou utilisez un gestionnaire de mots de passe sécurisé.

*Un mot de passe robuste est votre première ligne de défense. Utilisé sur plusieurs services, il devient une vulnérabilité. Variez-les, renforcez-les.*

Testez le module de création de mot de passe de la CNIL !



# 2 USAGES SÉPARÉS

## BONNES PRATIQUES

**N'utilisez pas** vos adresses ou outils personnels pour des activités professionnelles (et inversement).

**Ne connectez pas** de périphériques personnels (USB, comptes cloud) aux équipements de votre organisation.

Soyez **vigilant** sur les paramètres de confidentialité lors de vos usages numériques personnels.

*La séparation claire entre vos usages professionnels et personnels est essentielle pour limiter les risques de fuites de données ou d'intrusion dans votre environnement de travail.*



# 3

FOIS RIEN !

VERROUILLER SA SESSION

BONNES PRATIQUES

Utilisez les raccourcis clavier :

Windows + L

OU

Ctrl + Alt + Suppr puis  
Verrouiller

Activez le **verrouillage automatique** après  
inactivité (paramètres de sécurité)

*Verrouiller votre session évite les accès non autorisés à vos outils, fichiers et données. Un réflexe simple qui protège immédiatement votre environnement numérique, même pour quelques minutes d'absence.*



# 4 TASTROPHE ! PRUDENCE AVEC LES EMAILS ET LES LIENS

## BONNES PRATIQUES

**Ne cliquez jamais sur un lien sans vérification préalable**

**Ne transmettez jamais vos identifiants par email. En cas de doute, passez par le site officiel en tapant l'adresse manuellement**

**Utilisez une messagerie professionnelle dotée d'un filtre anti-hameçonnage**

*Les attaques par phishing se présentent sous forme de courriels, SMS ou appels imitant des organismes de confiance pour vous inciter à cliquer sur des liens frauduleux ou transmettre des données sensibles.*

*Objectif : obtenir vos identifiants, propager un virus ou accéder à des données confidentielles.*





# CYBER RÉFLEXES

inéa

De bons gestes à adopter



**inéa**  
Sant& Numérique  
Hauts-de-France

# 1 MOT DE PASSE SOLIDE ET DIFFÉRENT POUR CHAQUE COMPTE

Au moins 12 caractères incluant majuscules, chiffres, caractères spéciaux.

Évitez les informations personnelles et changez vos mots de passe régulièrement, ou utilisez un gestionnaire de mots de passe sécurisé.



# 2 USAGES SÉPARÉS

N'utilisez pas vos adresses mail ou outils personnels pour des activités professionnelles (et inversement). Ne connectez pas de périphériques personnels (USB, compte cloud) aux équipements de votre organisation.



# 3 FOIS RIEN ! VERROUILLER SA SESSION

Activez le verrouillage automatique de votre session de travail après inactivité (paramètres de sécurité).



# CYBER RÉFLEXES

De bons gestes à adopter

# 4 TASTROPHE ! PRUDENCE AVEC LES EMAILS ET LES LIENS



Ne cliquez jamais sur un lien sans vérification préalable.

Ne transmettez jamais vos identifiants par email. En cas de doute, passez par le site officiel de l'expéditeur en écrivant l'adresse manuellement dans votre barre de recherche.

Un simple rappel peut tout changer.  
Demandez votre sticker  
Windows + L !