GRADeS inéa

Sant& Numérique
Hauts-de-France

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Hauts-de-France

CYBER RÉFLEXES inéa

De bons gestes à adopter

1 MOT DE PASSE SOLIDE ET DIFFÉRENT POUR CHAQUE COMPTE

BONNES PRATIQUES

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

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.

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

GRADeS inéa Sant& Numérique Hauts-de-France

BONNES PRATIQUES

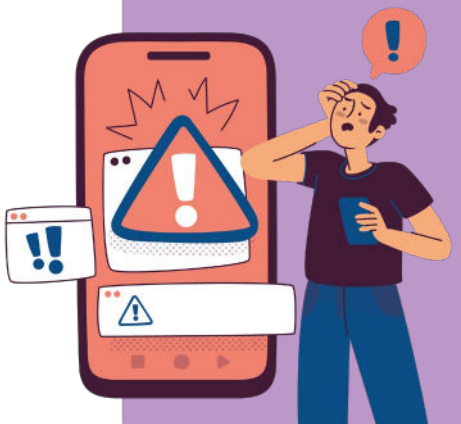
Ne cliquez jamais sur un lien sans vérification préalable

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

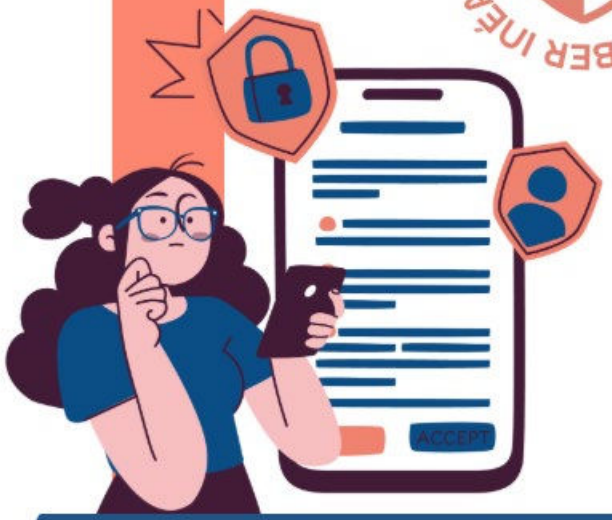
Utilisez une messagerie professionnelle dotée d'un filtre anti-hameçonnage

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.



"LES BONS GESTES CYBER"



COMMENCER

GRADeS inéa Sant& Numérique Hauts-de-France

inéa Sant& Numérique Hauts-de-France

SCANNER et TESTER
vos connaissances
en cybersécurité !


inéa
Sant& Numérique
Hauts-de-France