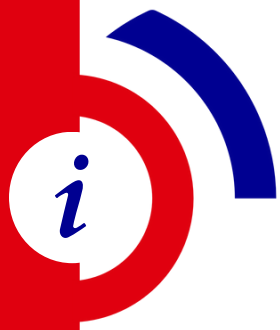
FICHE RÉFLEXE



BONNES PRATIQUES À ADOPTER POUR UN MOT DE PASSE SÉCURISÉ

CYBER RÉUNION

CYBER RÉUNION

L'UTILISATION DE MOTS DE PASSE FORTS ET UNIQUES

POURQUOI UN MOT DE PASSE SÉCURISÉ EST ESSENTIEL ?

Un mot de passe est la première ligne de défense contre les cyberattaques. Un mot de passe faible ou réutilisé augmente considérablement le risque de piratage de compte, de vol d'identité ou de fraude en ligne

CRÉEZ UN MOT DE PASSE FORT

- Minimum 12 caractères (idéalement 16 ou plus).
- Mélangez majuscules, minuscules, chiffres et caractères spéciaux (@, !, #, ?...).
- Évitez les informations personnelles comme votre nom, date de naissance, numéro de téléphone.

EXEMPLES DE MOT DE PASSE :

✗ mots de passe faibles
- 123456,
- password,
- azerty

✓ mots de passe forts
- GF!98MN4$XQZ!KL
- Q3F+MBU@9+J?71?"!
- UQYVB$M,ZG8B

CRÉEZ UN MOT DE PASSE UNIQUE POUR CHAQUE COMPTE

Pourquoi ?

- Un même mot de passe sur plusieurs comptes = Risque accru.
- Si un site est piraté et votre mot de passe divulgué, tous vos autres comptes sont en danger.

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

- Permet de stocker et générer des mots de passe complexes.
- Accès sécurisé avec un seul mot de passe maître.
- Exemples : KeePass (**gratuit**), Bitwarden, Dashlane, 1Password, ou équivalent.

ACTIVEZ L'AUTHENTIFICATION À DEUX FACTEURS (2FA)

- Ajoutez une couche de sécurité supplémentaire en activant la 2FA sur vos comptes **selon les procédures en vigueur de vos fournisseurs de services en ligne**.
- Préférez une application d'authentification (FreeOTP, 2FA Authenticator, ou d'autre application de double authentification des fournisseurs de services en ligne) plutôt que le SMS.

À RETENIR

- Un mot de passe long, unique et complexe pour chaque compte.
- Ne jamais réutiliser un mot de passe.
- Utiliser un gestionnaire de mots de passe.
- Activer l'authentification à deux facteurs (2FA).

En appliquant ces bonnes pratiques, vous réduisez considérablement les risques de piratage et protégez efficacement vos informations personnelles !

RESSOURCES UTILES

- CNIL
- Cybermalveillance.gouv.fr
- Guide de l'ANSSI

RETROUVEZ TOUTES NOS PUBLICATIONS SUR

www.cyber-reunion.fr