



COMMENT CRÉER UN BON MOT DE PASSE EN COLLECTIVITÉ

LONG ET COMPLEXE

Ex: R#7vLm9!zB

- 12 caractères minimum
- Majuscules, minuscules, chiffres & symboles



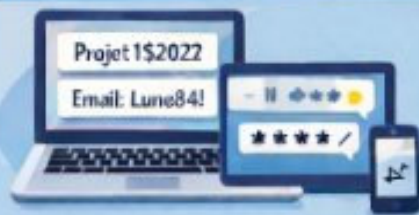
ÉVITER LES MOTS COURANTS



- 123456
- motdepasse
- admin

Pas de noms communs ni de dates de naissance

UNIQUE À CHAQUE COMPTE



Un mot de passe différent pour chaque compte, et notamment pour le compte professionnel !

ON N'UTILISE NI LA DATE DE NAISSANCE NI LE PRENOM...



... des enfants, de son animal ou de sa belle-mère



CHANGER RÉGULIÈREMENT

Mettre à jour ses mots de passe



NE PAS PARTAGER

Ne jamais divulguer son mot de passe, même à un collègue de confiance !



SÉCURITÉ & PROTECTION DANS LA COLLECTIVITÉ

Memo CYBERSECURITE de la DSI



Menaces	Bonne pratique associée
Le Cheval de Troie : logiciel malveillant	Éviter de cliquer sur des liens ou pièces jointes suspects
Le Rançongiciel : chiffre vos données contre une rançon	Vérifier l'expéditeur et ne pas ouvrir de fichiers suspects
Le Spyware : logiciel espion	Se méfier des pop-ups et fausses alertes
Le Pretexting : Création d'un faux scénario pour obtenir des informations	Vérifier l'identité via un autre canal en cas de doute (appel, teams...)
Credential stuffing : réutilisation d'identifiants volés sur d'autres comptes	Utiliser des mots de passe uniques
Le Business Compromise / arnaque au président : usurpation d'un email de direction	Confirmer la demande par téléphone ou outil interne (Teams)
Le Brute Force : essayer des mots de passe jusqu'à trouver le bon	Créer un mot de passe long et complexe
Le Password Spraying : tester des mots de passe courant sur beaucoup de comptes	Éviter les mots de passe fréquemment utilisés
Spear Phishing : phishing ciblé	Je limite la diffusion d'informations personnelles et professionnelles sur les réseaux tous publics
Usb Drop Attack laisser une clé infectée dans un lieu public	Ne jamais brancher de périphérique inconnu (clé usb, disque dur externe)
Interception des identifiants / mots de passe	Dans les lieux publics, je privilégie une connexion en 3G ou 4G et évite les WIFI publics
Risque de perte / fuite de données	J'enregistre mes fichiers de travail uniquement sur les espaces de stockage de la Collectivité (Bureautiques / Teams)
Shadow it : utilisation de logiciels à la sécurité douteuse	Pour partager des documents, j'utilise uniquement les plates-formes sécurisées validées par la DSI
Vol de mon matériel informatique	Je garde en lieu sûr mes équipements informatiques professionnels



Bonnes pratiques contre le phishing
Vérifier l'expéditeur des mails reçus: attention aux adresses proches mais fausses (ex. .gouv-fr.com).
Se méfier de l'urgence : “action immédiate”, “compte bloqué”, “dernier rappel” = gros signal d’alerte.
Ne jamais cliquer trop vite sur un lien ou une pièce jointe inattendue.
Survoler les liens pour voir la vraie URL avant de cliquer.
Ne jamais transmettre mot de passe, code MFA ou données sensibles par mail.
En cas de doute : ne rien faire et signaler à la DSI

⚠ SHADOW IT : l’informatique de l’ombre
Cela peut :
•Créer des failles de sécurité
•Exposer des données sensibles
•Poser des problèmes légaux (RGPD, confidentialité)
•Empêcher les sauvegardes officielles

Un outil pro utilisé sans validation de la DSI = un risque pour la sécurité.
👉 Pas validé = pas sécurisé.
👉 Pas sécurisé = données en danger.