FICHE RÉFLEXE

SÉCURISEZ VOS ACCÈS

L'IMPORTANCE D'UN MOT DE PASSE COMPLEXE

QU'EST-CE QU'UN MOT DE PASSE COMPLEXE ?

Un mot de passe robuste, c'est un mot de passe :

- Long et varié : **13 caractères ou plus.**
- Contenant un mélange de lettres **majuscules,** lettres **minuscules, chiffres, caractères spéciaux** (ex. @, #, $).
- **Non basé sur des informations personnelles** évidente (nom, date de naissance).

BONNES PRATIQUES

#1 Changez votre mot de passe régulièrement ou lorsque vous constatez une compromission.

#2 Utilisez un mot de passe différent pour chaque application.

#3 Si disponible, activer l'authentification multi-facteurs (MFA) pour vous connecter en validant votre identité par mail ou par SMS

#4 Créez un mot de passe en utilisant une passphrase. Choisissez une phrase, puis prenez la première lettre de chaque mot ou des syllabes en ajoutant des symboles ou chiffres.
Exemple : « **T**ous **m**es**(@i) M0**ts de **P**ass**($)**es s(**5**)ont **p**rotégés **P**ar l'**AmN3**sie **!** » peut donner **Tm@iM0dP$e5pPAmN3!**

#5 Utilisez un gestionnaire de mot de passe pour centraliser l'ensemble de vos mots de passe.

#3

Pourquoi et comment activer l'authentification multi-facteurs (MFA)

L'authentification multi-facteurs (MFA) permet d'ajouter une barrière supplémentaire lors de l'accès aux systèmes d'information de l'établissement.

Il est possible de centraliser la réception du code demandé sur une application d'authentification, plutôt qu'un envoi par SMS ou par mail.

#5

Définition d'un gestionnaire de mot de passe

Il s'agit d'un outil qui stocke et protège tous vos mots de passe dans un coffre-fort numérique crypté. Au lieu de devoir mémoriser chaque mot de passe complexe, vous n'avez qu'à retenir un seul mot de passe principal pour accéder au gestionnaire. Il permet également de générer des mots de passe robustes et uniques pour chaque accès.

Si votre service manipule plusieurs mots de passe, **l'installation d'un gestionnaire de mots de passe, tel que Keepass, peut faire l'objet d'une demande** adressé par mail au service informatique.

MAUVAISES PRATIQUES

#1 Partager son mot de passe à une personne tierce, même à un collègue.

#2 Stocker un mot de passe en clair dans un fichier texte, sur un navigateur internet (Google Chrome, Mozilla Firefox..) ou un post-it

#3 Cliquer sur un lien douteux à partir d'un e-mail ou SMS suspect et saisir son mot de passe sur un site ou une application dont l'origine n'est pas vérifiée.

SIGNALEZ IMMÉDIATEMENT

- Si vous pensez qu'un tiers a obtenu votre mot de passe (ex. : email de réinitialisation reçu sans demande, alerte de sécurité signalant une tentative d'accès suspect)
- Si vous n'arrivez plus à accéder à un espace nécessitant un mot de passe
- Si vous constatez une activité suspecte sur votre compte

> Dans le cas d'un oubli de mot de passe :

- Utiliser la procédure de récupération sur l'espace concerné (« Mot de passe oublié »).
- Créer un mot de passe fort et unique en suivant les recommandations de sécurité ci-dessus.
- Mettre à jour les autres comptes si l'ancien mot de passe était utilisé ailleurs

> Dans le cas de vol de mot de passe ou de suspicion de compromission :

Avertir le service informatique
1017 ou 05 55 43 10 17

Demander à parler au **Référent Sécurité**

Ou nous contacter sur
informatique@ch-esquirol-limoges.fr