Aide-mémoire Bien BRANCHÉ pour bien VIEILLIR

GESTION DES COMPTES ET MOTS DE PASSE

1. Garder un cahier dédié

- Utiliser un petit cahier réservé aux comptes et mots de passe.
- Noter : nom du site, nom d'utilisateur, mot de passe et date pour la tracabilité.
- Bien identifier chaque compte et son utilité (ex : Google/Gmail, Apple/Appareil).
- Ranger le cahier dans un endroit discret mais accessible.

2. Utiliser un gestionnaire de mots de passe

- Un seul mot de passe primordial et gardient de tous à retenir.
- Les autres sont enregistrés automatiquement.
- Exemples : Trousseau iCloud, 1Password (payant), Bitwarden (accessible), NordPass.
- Plus sécuritaire que d'utiliser le même mot de passe partout.

3. Créer des mots de passe faciles à retenir

- Utiliser une phrase (ex. : MonChienAimeLesTartes@2024).
- Ou les initiales d'une phrase (ex. : Jdcqpam2024!).
- Mélanger un mot personnel + un mot associé au site (ex. : Café+Journal@Facebook)
- Éviter : dates de naissance, noms proches, 123456, même mot de passe pour tous les sites.

4. Organiser ses comptes

- Faire une liste des comptes importants (banque, courriel, Facebook…).
- Supprimer les anciens comptes inutiles.
- La plupart du temps, l'adresse courriel est l'identifiant à plusieurs comptes.
- Garder les adresses courriel à jour (les plus importants à retenir).
- Recommandé de changer les mots de passe importants 1 fois par an.

5. Activer l'authentification à double facteur

- Recommandé de protéger le courriel, car possède le plus d'informations sensibles.
- Recevoir un code par SMS ou dans une application.
- Protège fortement contre le piratage.
- Nécessite la plupart du temps un téléphone cellulaire et une connexion.

Aide-mémoire Bien BRANCHÉ pour bien VIEILLIR

GESTION DES COMPTES ET MOTS DE PASSE

6. Avoir une personne de confiance

- Indiquer où se trouve ses mots de passes et comptes en ligne.
- Utile en cas d'oubli, maladie ou urgence.

7. Noter les réponses de récupération

- Noter les réponses aux questions du type : « Votre plat préféré? ».
- Les conserver avec les mots de passe pour éviter d'oublier.

8. Se méfier des courriels suspects

- Ne jamais donner son mot de passe par téléphone ou courriel.
- Ne pas cliquer sur les liens douteux.
- Les banques et le gouvernement ne demandent jamais de mot de passe par courriel.
- En cas de doute → demander à quelqu'un.

9. Prendre son temps

- Ne jamais se presser.
- Si un message semble urgent ou stressant, c'est peut-être une arnaque.
- Toujours vérifier ou demander de l'aide.