

Fiche pratique – Sécurité et accès centralisés

Protéger vos données et gérer vos accès de manière centralisée est essentiel pour éviter les pertes d'informations, les piratages et les oublis de mots de passe. Cette fiche vous explique comment mettre en place une organisation sécurisée et efficace avec ProtonPass et d'autres bonnes pratiques.

Objectif

Centraliser la gestion de vos mots de passe et sécuriser vos données tout en les rendant accessibles rapidement et uniquement aux personnes autorisées.

Étapes pour sécuriser vos accès

- Utiliser un gestionnaire de mots de passe – Adoptez ProtonPass pour stocker et gérer tous vos identifiants de manière chiffrée et sécurisée.
- Créer des mots de passe forts et uniques – Chaque compte doit avoir un mot de passe différent, long et complexe (lettres, chiffres, symboles).
- Activer l'authentification à deux facteurs (2FA) – Ajoutez une couche de sécurité supplémentaire sur vos comptes sensibles (emails, banque, réseaux sociaux).
- Organiser vos accès par dossiers – Classez vos identifiants dans ProtonPass par catégories (pro, perso, administratif...) pour les retrouver facilement.
- Sauvegarder vos données importantes – Utilisez un service de stockage sécurisé (Google Drive, Dropbox, Proton Drive) et chiffrez les documents sensibles.

Bonnes pratiques

- Ne partagez jamais vos mots de passe par email ou messagerie non sécurisée.
- Mettez à jour vos mots de passe tous les 6 à 12 mois pour les comptes sensibles.
- Vérifiez régulièrement les connexions à vos comptes pour détecter toute activité suspecte.
- Utilisez un mot de passe maître très fort pour ProtonPass, et ne le stockez nulle part.

Exemple d'organisation dans ProtonPass

- Dossier Professionnel – Emails pro, CRM, outils internes
- Dossier Personnel – Réseaux sociaux, emails personnels, services de streaming
- Dossier Administratif – Banque, impôts, assurances

Conclusion

Avec ProtonPass et une bonne organisation de vos accès, vous protégez efficacement vos données tout en les rendant accessibles uniquement aux personnes autorisées. Une sécurité numérique bien gérée est un investissement essentiel pour votre tranquillité d'esprit.