

Comptes : protection et secours

Passkeys, MFA et récupération · Mémo à conserver sans y inscrire de secrets

Comparer

- Mot de passe : unique, long, généré par un gestionnaire.
- TOTP : code temporaire ; la graine et son QR code restent secrets.
- Passkey : authentification liée au service, résistante au phishing de connexion.

Choisir

- Identifie le fournisseur qui stocke/synchronise la passkey.
- Distingue synchronisation et authenticateur lié à un appareil.
- Une clé USB OTP n'est pas automatiquement une clé FIDO2.

Préparer le secours

- Vérifie et protège l'email de récupération.
- Enregistre un second moyen, si le service le permet, et range-le séparément.
- Garde les codes de récupération dans un stockage protégé accessible sans le téléphone.

Tester sans se bloquer

- Commence sur un compte test, sans effacer de téléphone ni retirer le dernier accès.
- Essaie la connexion principale dans un autre profil de navigateur.
- Simule la perte : n'utilise pas le téléphone et essaie le secours.

Résultat attendu

- L'accès de secours fonctionne sans le moyen déclaré perdu.
- Les dépendances et les notifications de sécurité sont comprises.
- Marque les codes consommés ; renouvelle et range le lot si nécessaire.

Entretenir

- Note service, moyens, emplacement des secours et date du dernier essai.
- Refais le test après changement d'appareil ou de fournisseur.
- Une passkey ne protège pas toutes les sessions ni tous les parcours de récupération.

Article complet, exercices et sources : blog.gringao.fr/cyber-passkeys-double-authentication-recuperation/