Préparer la récupération d’un compte sans révéler ses secrets

Savoir quoi vérifier avant de perdre un téléphone ou un moyen de connexion. La fiche prépare un plan de secours sans écrire de mot de passe ni de code dans l’exercice.

Le geste à reprendre : Préparer la récupération d’un compte sans révéler ses secrets

Temps indicatif : 15 à 20 minutes ; pauses possibles.

Matériel : Cas fictif sur papier ou document ; aucun compte réel à ouvrir ou à modifier.

Le cas fictif

FICHE FICTIVE — COMPTE DU CLUB

Messagerie de récupération : encore accessible.

Ancien téléphone : fonctionne et reste connecté.

Nouveau téléphone : accès au compte non testé.

Demande inattendue d’approbation : reçue ce matin.

Travail : écrire un ordre de vérification et prévoir un secours séparé, sans saisir de vrai identifiant, code ou mot de passe.

1. Repérer les accès qui servent de point d’appui

Lisez le cas et identifiez la messagerie de récupération ainsi que l’appareil encore utilisable. Un compte peut dépendre d’un autre accès pour une procédure de secours. Ne recopiez aucune adresse personnelle dans cette fiche : utilisez seulement les rôles du cas fictif.

2. Distinguer les moyens de connexion

Dans votre préparation, distinguez mot de passe, approbation sur un appareil, clé d’accès et moyen de secours. Leur disponibilité dépend du service et de l’appareil. Un secret conservé uniquement dans le téléphone à remplacer n’est pas un secours séparé de ce téléphone.

3. Préserver l’ancien accès pendant le contrôle

Proposez de vérifier les moyens autorisés et de tester le nouvel accès avant de retirer l’ancien moyen. L’exercice ne réalise aucun changement de sécurité. Pour un compte réel, suivez l’aide du service et utilisez des appareils personnels ou autorisés.

4. Prévoir une récupération officielle

Écrivez comment rejoindre l’aide de récupération depuis le service habituel si le téléphone devient indisponible. Ne promettez pas un accès immédiat : les contrôles et délais varient. Les codes de secours réels doivent rester protégés et séparés des documents ordinaires de formation.

5. Refuser une approbation non demandée

Dans le cas, ne validez pas la demande inattendue pour la faire disparaître. Notez une vérification depuis le service connu et un recours adapté si un incident est suspecté. Le plan remis au formateur contient les décisions et leurs raisons, jamais les secrets de la personne.

Vérifier votre résultat

• Les dépendances entre accès sont identifiées.

• Le secours est distinct du téléphone principal.

• L’ancien moyen reste disponible jusqu’aux contrôles utiles.

• La récupération prévue passe par le service officiel.

• Aucun secret ou identifiant réel n’apparaît dans ma préparation.

Ces contrôles préparent l’autonomie et ne remplacent pas l’observation d’une manipulation. Les documents formateur restent dans le dossier privé.

Pour retrouver les commandes officielles

Cybermalveillance.gouv.fr : comprendre la double authentification

Compte Google — Récupération officielle du compte