Je veux garder l’accès à mes comptes quand je change de téléphone

Objectif : Vous établissez un plan fictif de changement ou de perte de téléphone qui conserve une voie d’accès indépendante et reconnaît les limites de la récupération.

Pour commencer : Savoir reconnaître le service et le compte que l’on souhaite utiliser. Le simulateur fonctionne sans compte, connexion, achat ni saisie de secret. N’y mettez jamais de mot de passe, code reçu, code de secours, numéro réel, QR de configuration ou donnée biométrique. Cet atelier approfondit les notions de compte déjà abordées ; il est distinct des évaluations des sept niveaux. Les clés d’accès exigent une compatibilité du service, du système, du navigateur et du mode de stockage choisi. Windows, macOS, Android et iOS-iPadOS n’offrent pas exactement les mêmes parcours ; les comptes professionnels peuvent dépendre d’un administrateur. Aucun réglage personnel n’est changé dans cet entraînement.

Durée d’entraînement indicative : 50 à 65 minutes, sans modification de compte

La situation d’exercice

Dans ce scénario fictif, Farid organise une exposition photo avec un compte inventé. Son téléphone habituel reçoit les confirmations de connexion. Il prépare un remplacement, mais il utilisera aussi une carte de situation où ce téléphone est devenu indisponible. Il dispose de cartes décrivant un autre appareil déjà reconnu, un moyen de secours conservé séparément et une ancienne méthode qui pourrait cesser de fonctionner. Aucune carte ne contient de vrai secret. Vous devez distinguer ce qui sert à se connecter, ce qui sert à récupérer l’accès et ce qui doit être vérifié avant d’abandonner l’ancien appareil. Un faux message vous invite à approuver une connexion inattendue. Votre mission est de choisir un ordre d’actions explicable, sans effectuer aucune connexion réelle.

1. Faire la carte des accès sans noter de secrets

Sur les cartes fictives, distinguez le nom du service, l’identifiant du compte et les moyens permettant de prouver que l’on peut l’utiliser. L’adresse de connexion n’est pas un mot de passe ; le déverrouillage du téléphone n’est pas automatiquement le mot de passe du service. Ajoutez une autre colonne pour les moyens de récupération déjà prévus. Certains services emploient des éléments différents pour la connexion courante et pour les incidents. Dans cet exercice, inscrivez uniquement des catégories comme « autre appareil » ou « moyen de secours séparé », jamais une valeur réelle qui permettrait d’entrer dans un compte.

Repérez les dépendances : si le seul moyen de recevoir une confirmation se trouve dans le téléphone qui est perdu, le parcours habituel peut être bloqué. Si une adresse de récupération dépend elle-même du compte que l’on veut récupérer, elle peut aussi ne pas être utile dans cette situation. Faites expliquer ces dépendances avec des cartes reliées plutôt qu’en ouvrant vos paramètres personnels. La messagerie principale mérite une attention particulière car elle peut recevoir des demandes de récupération d’autres services. La réussite de cette première étape est de voir ce qui reste disponible quand un élément manque, sans promettre qu’une récupération sera toujours

possible.

2. Comprendre la double authentification et les demandes inattendues

Associez les moyens fictifs à des catégories : quelque chose que l'on connaît, comme un mot de passe ; quelque chose que l'on possède, comme un appareil ou une clé ; et, selon le système, une caractéristique biométrique utilisée pour déverrouiller un moyen de connexion. La double authentification ajoute une vérification à la connexion usuelle et réduit les risques liés au seul vol d'un mot de passe. Les services peuvent parler de validation ou de vérification en deux étapes. Les méthodes disponibles diffèrent : application dédiée, notification, SMS ou clé, notamment. Deux mots de passe successifs ne constituent pas, à eux seuls, deux catégories de facteurs.

Lisez le faux message demandant d'approuver une connexion non commencée par Farid. Choisissez de ne pas l'approuver. Un code reçu ou une notification ne prouve pas que la personne qui vous contacte est légitime ; une demande inattendue doit être vérifiée depuis le service que vous ouvrez vous-même par son chemin habituel. Ne dictez pas un code à un interlocuteur et ne validez pas une demande pour la faire disparaître. Dans le simulateur, expliquez simplement le refus. Ces protections renforcent l'accès mais ne garantissent pas l'absence de toute fraude : le contexte, l'appareil et la vigilance restent nécessaires.

3. Distinguer une clé d'accès d'un code à recopier

Une clé d'accès, aussi appelée passkey, est un moyen de connexion pris en charge par le service et un dispositif compatible. Elle permet généralement de confirmer l'accès en déverrouillant l'appareil, par un code local ou une fonction biométrique. Ce n'est pas un nombre provisoire à recopier dans une conversation. Pour le compte Google, les données biométriques utilisées pour ce déverrouillage restent sur l'appareil et ne sont pas transmises à Google. L'emploi d'une clé d'accès réduit l'exposition à certains hameçonnages, mais il faut encore vérifier le contexte de connexion et protéger le déverrouillage de l'appareil.

Sur la carte correspondante, indiquez où la clé fictive est disponible : appareil, gestionnaire compatible ou clé matérielle selon le cas. Certaines clés peuvent être synchronisées par un gestionnaire ; d'autres restent liées à un support. N'en déduisez pas qu'elles seront accessibles sur n'importe quel nouveau téléphone. Vérifiez la documentation du service et du gestionnaire avant un changement réel. Ne créez pas une clé d'accès personnelle sur un appareil partagé pour terminer un exercice. Une clé d'accès peut modifier le parcours de connexion proposé sans supprimer les autres méthodes de récupération ; ce comportement doit être vérifié pour le compte concerné.

4. Préparer un changement pendant que l'ancien téléphone est disponible

Choisissez la situation où Farid possède encore l'ancien appareil. Classez les actions fictives : vérifier les moyens disponibles, préparer le nouveau dispositif selon l'aide officielle, confirmer qu'une méthode utilisable reste accessible, puis seulement envisager de retirer l'ancien moyen devenu inutile. Avoir le même numéro ne prouve pas que les confirmations d'une application ou les clés d'accès sont transférées. L'ordre prudent consiste à vérifier chaque méthode concernée, sans effacer l'ancien appareil trop tôt. Le formateur n'a besoin de voir ni un code, ni un QR, ni le contenu d'un gestionnaire pour constater que vous avez compris cet ordre.

Prévoyez un secours qui ne dépend pas entièrement du même téléphone : autre appareil déjà reconnu, méthode autorisée supplémentaire ou codes de secours lorsque le service en propose. Ces codes sont des secrets à conserver séparément et de manière adaptée ; l'atelier ne les affiche pas et ne demande pas leur emplacement précis. Pour Apple, un appareil de confiance et un numéro de téléphone de confiance sont deux notions distinctes. Un numéro supplémentaire peut aider s'il a été configuré auparavant et reste accessible. Pour un compte professionnel, la procédure de l'organisation et l'administrateur peuvent définir les méthodes possibles.

5. Construire un plan si le téléphone est perdu ou indisponible

Passez à la carte « téléphone indisponible ». Cherchez d'abord une méthode alternative déjà prévue, depuis un appareil connu et protégé : autre appareil reconnu, clé d'accès présente ailleurs ou secours enregistré auparavant, selon le service. Distinguez une panne temporaire d'une perte ou d'un vol. En cas de perte réelle, suivez l'aide officielle pour sécuriser le compte et l'appareil, retirer les moyens associés au téléphone perdu et contacter l'opérateur si nécessaire. Ce sont des décisions à préparer ici avec les cartes ; aucune déconnexion, suppression de clé, suspension de ligne ou modification de mot de passe n'est exécutée par le simulateur.

Si aucun moyen utilisable ne reste, choisissez la procédure officielle de récupération correspondant au compte et lisez ses limites. Apple indique qu'un délai peut être nécessaire. Microsoft précise que son formulaire ne permet pas de contourner une vérification en deux étapes lorsque toutes les méthodes de vérification sont devenues inaccessibles. Aucun interlocuteur ne peut donc promettre un rétablissement immédiat pour tous les comptes. Terminez en expliquant le parcours de Farid et le secours qui aurait évité le blocage. Écartez les messages qui promettent de récupérer le compte en échange de secrets ou d'un paiement : repartez de l'aide officielle du fournisseur.

Relire votre résultat

• Je distingue identifiant, mot de passe, déverrouillage local et moyen de récupération.

• Je refuse une approbation de connexion que je n'ai pas commencée.

• Je sais qu'une clé d'accès dépend de sa compatibilité et de son stockage.

• Je prévois une voie de secours indépendante avant d'abandonner un ancien téléphone.

• Je connais le chemin de l'aide officielle et je n'attends pas une récupération garantie.

En cas de difficulté

Tout laisser sur un seul téléphone

L'application de confirmation et le seul secours peuvent devenir inaccessibles ensemble. Préparez les alternatives proposées par le service avant l'incident ; le simulateur utilise seulement des catégories fictives.

Approuver pour faire cesser les notifications

Une demande inattendue n'est pas une formalité. Refusez l'approbation et vérifiez la situation par le chemin habituel du service, sans partager un code avec une personne qui vous contacte.

Effacer trop tôt l’ancien appareil

Un transfert de numéro ou de photos ne prouve pas que les méthodes de connexion ont suivi. Vérifiez d’abord les procédures et les moyens réellement utilisables, sans exposer leurs secrets au formateur.

Questions pour réviser

1. Quel exemple associe deux catégories différentes de facteurs ?

• Deux mots de passe connus de la même personne

• Un mot de passe et une confirmation par un dispositif que l’on possède

• L’identifiant du compte écrit deux fois

2. Farid reçoit une approbation de connexion alors qu’il ne se connecte pas. Que doit-il faire ?

• Approuver pour supprimer l’alerte

• Dicter immédiatement le code à l’appelant

• Refuser et vérifier depuis le service ouvert par son chemin habituel

3. Que faut-il vérifier avant de compter sur une clé d’accès sur un nouveau téléphone ?

• Le stockage de la clé et la compatibilité du service, du système et du gestionnaire

• Seulement la couleur du téléphone

• Seulement le transfert des photos

4. Quel ordre convient pour préparer un changement de téléphone ?

• Effacer l’ancien téléphone avant toute vérification

• Préparer et vérifier un accès utilisable et un secours avant de retirer l’ancien moyen

• Supprimer toutes les méthodes pour repartir de zéro

Retrouvez les explications dans le quiz interactif de la page. Les guides, attendus et grilles d’observation formateur restent dans le dossier privé.

Pour retrouver les commandes officielles

Cybermalveillance.gouv.fr : comprendre la double authentification

Compte Google : clés d’accès, compatibilité et appareils personnels

Compte Google : perte du téléphone et autres méthodes de vérification

Apple : appareils et numéros de téléphone de confiance

Microsoft : possibilités et limites du formulaire de récupération