FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

SÉCURISER NOS COMPTES DE RÉSEAUX SOCIAUX ET AUTRES COMPTES EN LIGNE

28 MARS 2024

Contenu

Partie 1: Comptes de réseaux sociaux: guides Resolock

1. Présentation des guides Resolock
2. Sujets abordés
3. Protection de la vie privée
4. Téléchargement des guides Resolock
5. Nomenclature typique d’une page

Partie 2: Le double facteur d’authentification

1. En quoi consiste le double facteur d’authentification (2FA)
2. Principales méthodes de 2FA
3. Les codes de secours en cas de défaillance du 2FA
4. Exemple d’activation du 2FA: Facebook sur votre téléphone

Partie 1
Comptes de réseaux sociaux: guides Resolock

Présentation des guides Resolock

- **Resolock est une entreprise spécialisée dans la sécurisation des réseaux sociaux** des entreprises et des OBNL (organismes à but non lucratif).

- **Elle a publié des guides numériques** avec des instructions détaillées et des exemples pratiques permettant de comprendre et de configurer les paramètres de confidentialité et de sécurité des comptes de réseaux sociaux suivants:

  - Facebook
  - X
  - Instagram
  - LinkedIn
  - TikTok
  - Snapchat

Guides Resolock: sujets abordés

- **Localiser les paramètres** de son compte à partir d'un ordinateur ou d'un appareil mobile

- **Les 3 mesures cruciales pour sécuriser son compte**:
  - un mot de passe robuste: 12 caractères au minimum et idéalement 18 caractères composés de minuscules, majuscules, chiffres et caractères spéciaux
  - activer la double authentification
  - activer les alertes de connexions

- **Comment protéger votre vie privée en choisissant bien les données que nous publions et à qui nous les rendons accessibles** (contenu variant selon le réseau social)

- **Comment supprimer votre compte de réseau social**

- **Que faire si votre compte a été piraté**

Guides Resolock: protection de la vie privée

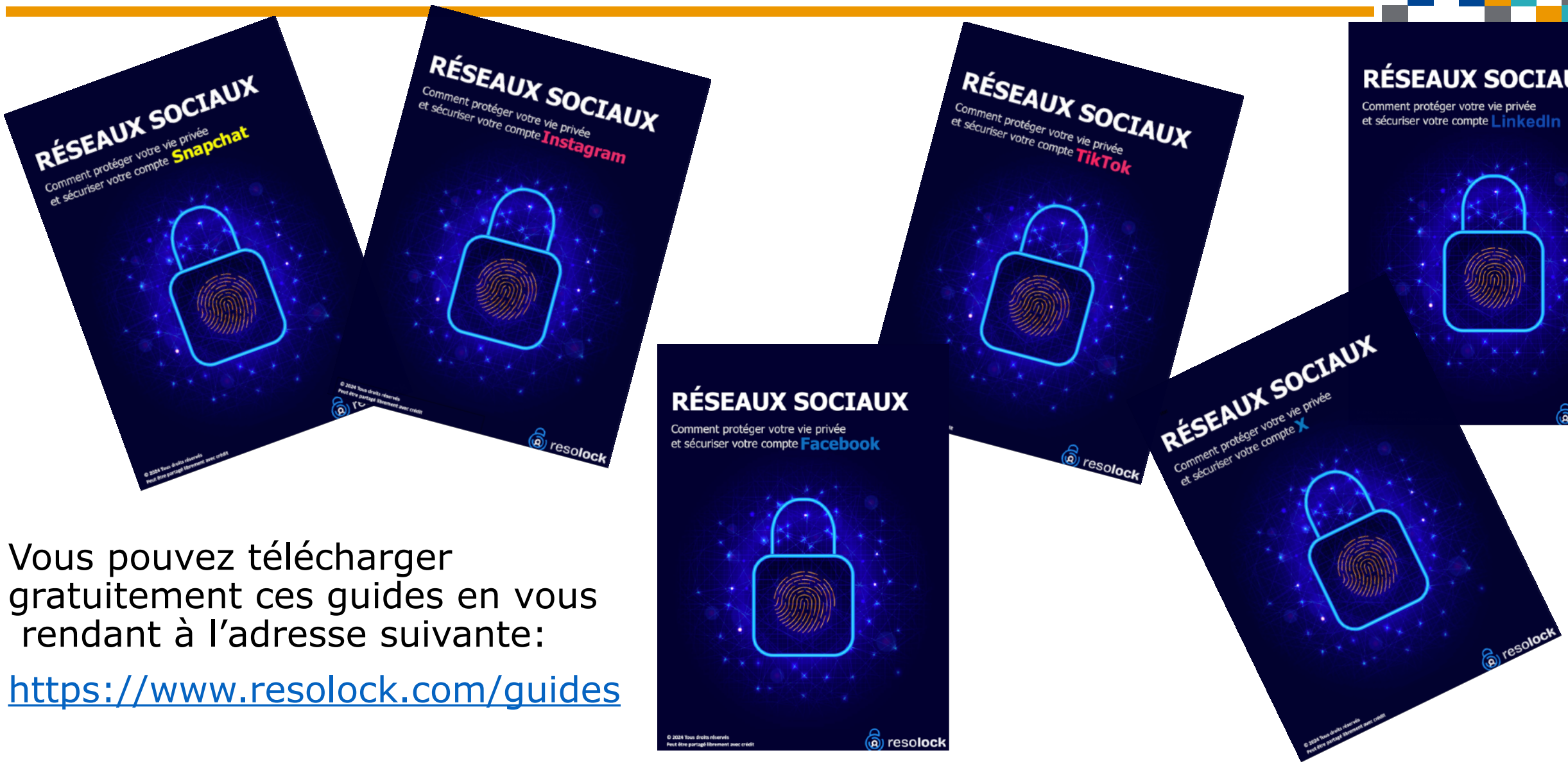
- **L'auteur passe en revue chacun des paramètres de confidentialité disponibles, explique leur signification, leur impact et donne son opinion sur la meilleure configuration à appliquer.**

- **Quelques exemples pour Facebook:**
  - Gérer qui peut vous envoyer des invitations
  - Qui peut voir votre liste d'amis
  - À qui le réseau social peut suggérer votre profil
  - L'affichage ou non de votre profil sur les moteurs de recherche
  - Qui peut vous envoyer des invitations par message
  - Qui peut voir vos stories
  - Qui peut voir ce que d'autres personnes publient sur votre profil
  - Etc.

Guides Resolock: protection de la vie privée

- **Quelques exemples pour Instagram:**
  - Les 3 types de comptes possibles
  - Supprimer un abonné de votre compte
  - Comment vous obtenez des invitations par message
  - Qui peut vous ajouter aux groupes
  - Qui peut répondre à vos stories
  - Qui peut commenter vos publications
  - Qui peut vous mentionner et vous identifier
  - Etc.

Téléchargement des guides Resolock



Vous pouvez télécharger gratuitement ces guides en vous rendant à l'adresse suivante:

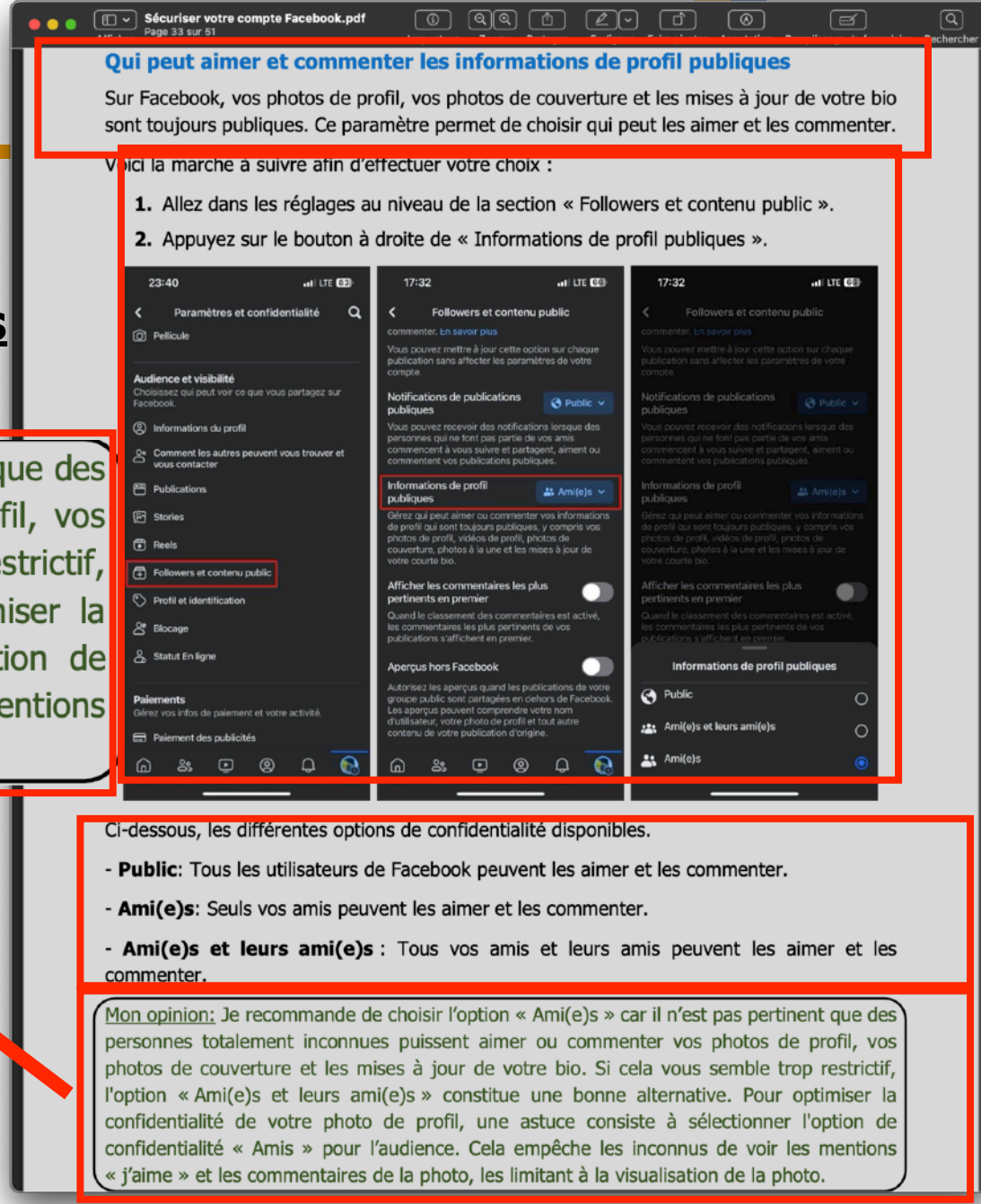
https://www.resolock.com/guides

Nomenclature typique d'une page

Exemple: page 33 du guide Resolock concernant Facebook (référence 1):

<u>Qui peut aimer et commenter les informations de profil publiques</u>:

<u>Mon opinion:</u> Je recommande de choisir l'option « Ami(e)s » car il n'est pas pertinent que des personnes totalement inconnues puissent aimer ou commenter vos photos de profil, vos photos de couverture et les mises à jour de votre bio. Si cela vous semble trop restrictif, l'option « Ami(e)s et leurs ami(e)s » constitue une bonne alternative. Pour optimiser la confidentialité de votre photo de profil, une astuce consiste à sélectionner l'option de confidentialité « Amis » pour l'audience. Cela empêche les inconnus de voir les mentions « j'aime » et les commentaires de la photo, les limitant à la visualisation de la photo.



Partie 2
Le double facteur d’authentification (2FA)

En quoi consiste le double facteur d'authentification (2FA)

- **2FA:** Méthode très efficace pour sécuriser davantage l'accès à nos comptes de réseaux sociaux et à nos autres comptes en ligne contenant des informations sensibles

- Avec le 2FA, **il faut fournir 2 facteurs d'authentification** pour accéder à notre compte**:**

  - **Facteur no 1**: quelque chose que nous **connaissons** (mot de passe) **ou** qui nous est **intrinsèque** (reconnaissance biométrique via une clé d'accès)

  - **Facteur no 2**: **fournir en plus** quelque chose lié à ce que nous **possédons** (un téléphone, une clé physique…)

En quoi consiste le double facteur d'authentification (2FA)

- Pour les sites web qui accepte le 2FA: généralement, l'utilisateur peut choisir de l'activer ou non.

- **L'authentification 2FA peut se faire de plusieurs manières**, variant selon les entreprises/services avec lesquels nous transigeons.

Principales méthodes de 2FA

1. **Méthode basée sur un facteur de connaissance:**

- **Répondre à une question de sécurité** (authentification en 2 étapes plutôt que authentification par double facteur)
  Exemple: Banque Royale

2. **Méthodes basées sur un facteur de possession:**

- **Notification push** transmise à un appareil « de confiance » et demandant d'approuver ou refuser l'accès au compte (ex: Apple, Google)

- **Code d'accès temporaire** reçu par téléphone, SMS ou courriel (ex: ARC, BNC, Revenu Québec…)

Remarque: l'utilisation d'un code transmis à notre téléphone cellulaire est parfois jugée moins sécuritaire car possibilité de fraude par échange de carte SIM (« Sim Swap », soit la prise de contrôle de votre compte de téléphonie cellulaire par des fraudeurs)

Principales méthodes de 2FA

2.Méthodes basées sur un facteur de possession (suite):

- Codes aléatoires uniques et temporaires (généralement 6 chiffres variant aux 30 sec), générés à la chaîne par votre appareil au moyen d'une application d'authentification (« software token »)

  - **Exemples d'applications d'authentification (voir la référence 3)**
    - Aegis Authenticator (pour Android)
    - Authy
    - 2FA Authenticator (2FAS)
    - Google Authenticator
    - Microsoft Authenticator
  - Plusieurs gestionnaires de mots de passe offrent également la possibilité de générer ces codes, tel que Keeper, Bitwarden, 1Password, etc.
    Leur degré de sécurité est-il équivalent à celui des applications ???

Principales méthodes de 2FA

2.Méthodes basées sur un facteur de possession (suite):

- **clés physiques de sécurité** certifiées (« hardware token »)
  - **Confirme votre identité par échange de clés cryptographiques utilisant le protocole d'authentification FIDO** (similaire aux clés d'accès)
  - Généralement considérée comme la méthode la plus sécuritaire, mais usage moins répandu que celui des applications d'authentification
  - Utile de posséder deux clés plutôt qu'une seule (en cas de perte d'une d'entre elles)
  - Exemples: Clé Google Titan, Clé YubiKey (plusieurs modèles, dont la 5C NFC vendue 75 $ chez Amazon).

Principales méthodes de 2FA

- **Remarques**
  - Quelques entreprises/services acceptant les clés **YubiKey**: Google, Apple, Microsoft, Facebook, 1Password, Bitwarden, LastPass.
  - Quelques entreprises/services acceptant les applications 2FA (**Google Authenticator, Authy, Microsoft Authenticator, etc)**: Facebook, Google, Firefox, PayPal, Amazon, Impôt Expert.

Les codes de secours en cas de défaillance du 2FA

- Un **code de secours est une série de chiffres générés lors de la configuration** de la double authentification pour un de vos comptes en ligne, notamment lors de l'utilisation d'une application d'authentification.

- Le code de secours permet d'accéder à votre compte dans l'éventualité où vous ne pouvez pas fournir le code de double authentification requis.

- Exemples: votre appareil contenant votre application de double authentification n'est pas disponible, votre application de 2FA est inopérante, etc.

- Certains comptes fourniront une seul code de secours, alors que d'autres en fourniront plusieurs (jusqu'à 10 par exemple!).

Les codes de secours en cas de défaillance du 2FA

- Certains comptes en ligne ne fournissent pas de codes de secours lorsque vous configurer la double authentification, mais elles offrent généralement la possibilité d'utiliser une autre méthode de 2FA en cas de défaillance de votre application d'authentification (ex: code transmis à votre téléphone).

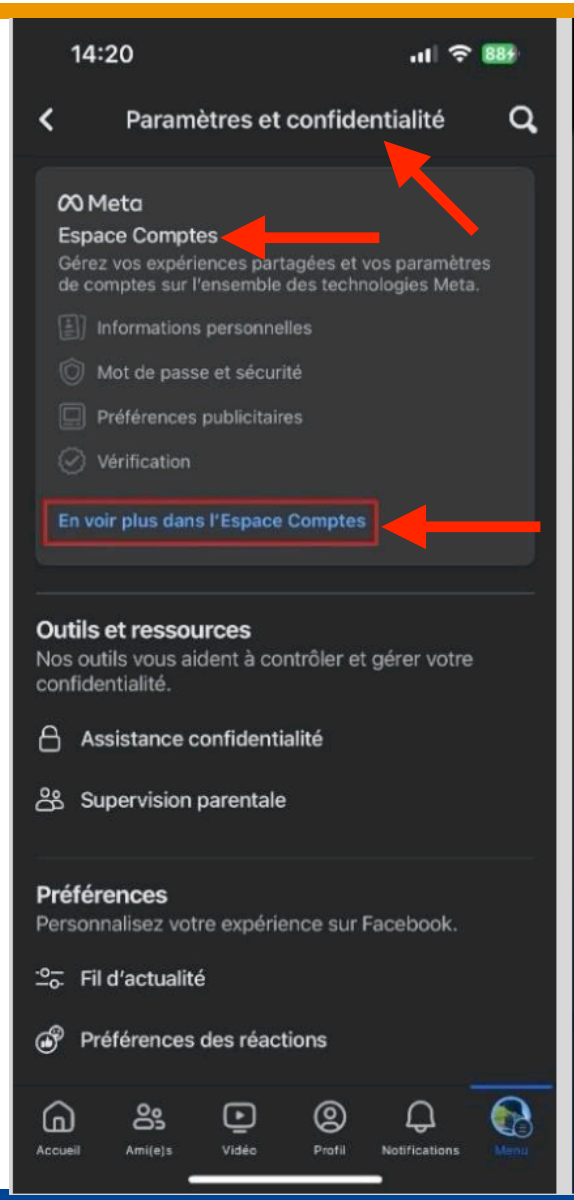
- **Un code de secours ne peut être utilisé qu'une seule fois**. Si vous devez l'utiliser, il est donc important de disposer d'un autre code de secours au cas où vous en auriez besoin ultérieurement.

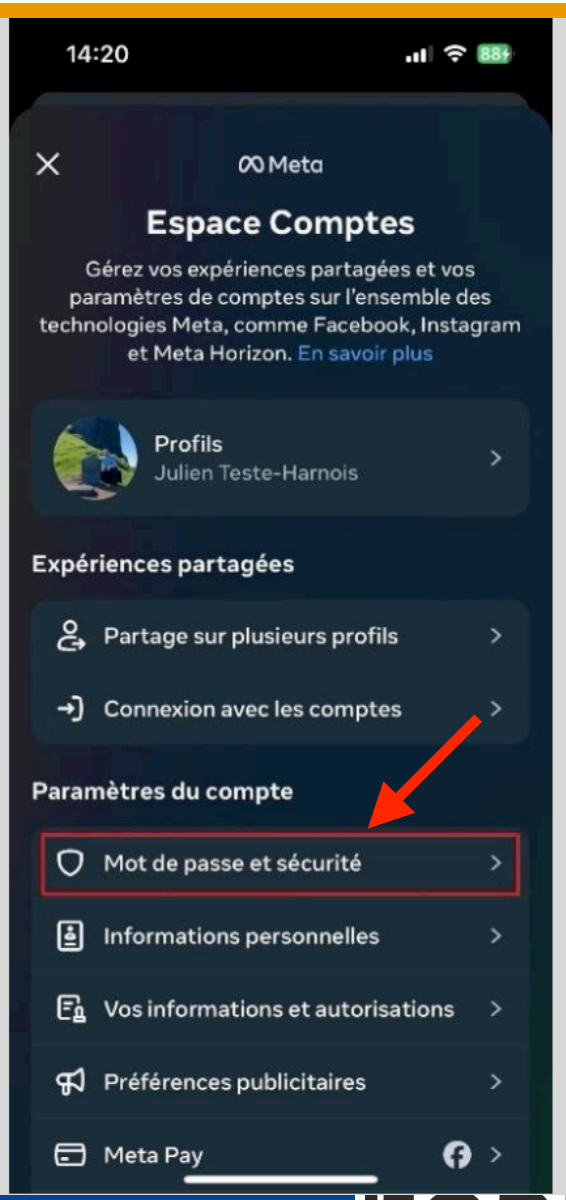
- Il est important de **conserver votre (vos) code(s) de secours en lieu sûr** et de pouvoir y avoir accès en cas de perte de vos appareils (téléphone, tablette, ordinateur, clé physique).
  Exemples: dans une note papier déposée dans un endroit confidentiel ou dans un fichier protégé par un mot de passe sauvegardé sur le cloud.

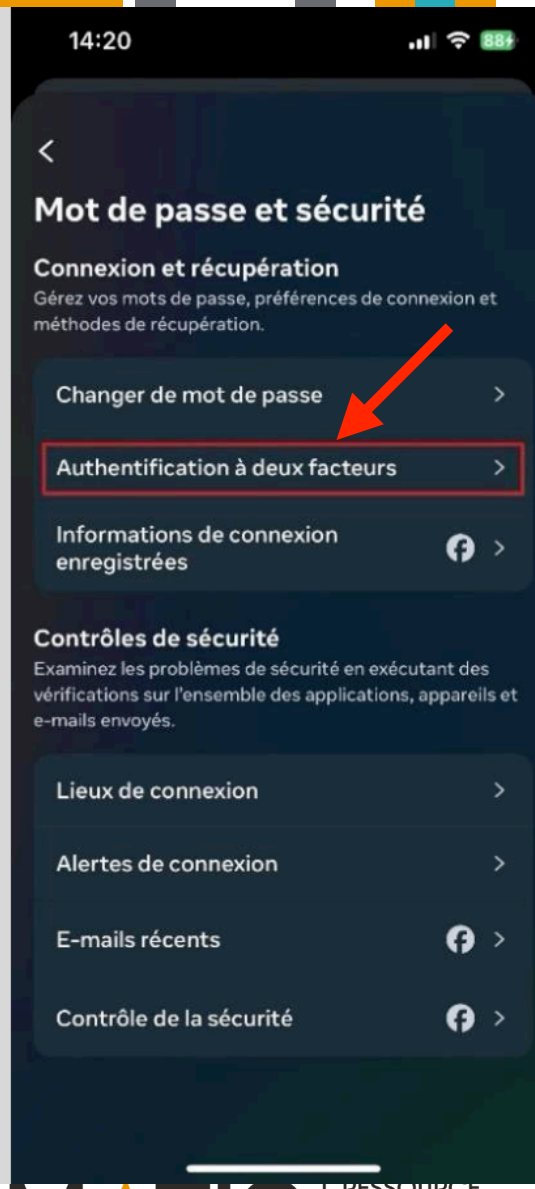
Exemple d'activation du 2FA: Facebook sur votre téléphone

Ce qui suit est extrait de la **référence 1:**

1. Dans le menu principal de l'application, sélectionner l'onglet « Paramètres » de la section « Paramètres et confidentialité » afin d'afficher la rubrique « Espace Comptes ».
2. Sélectionner « En voir plus dans l'espace Comptes », puis « Mot de passe et sécurité » et enfin appuyer sur l'onglet « Authentification à deux facteurs ».

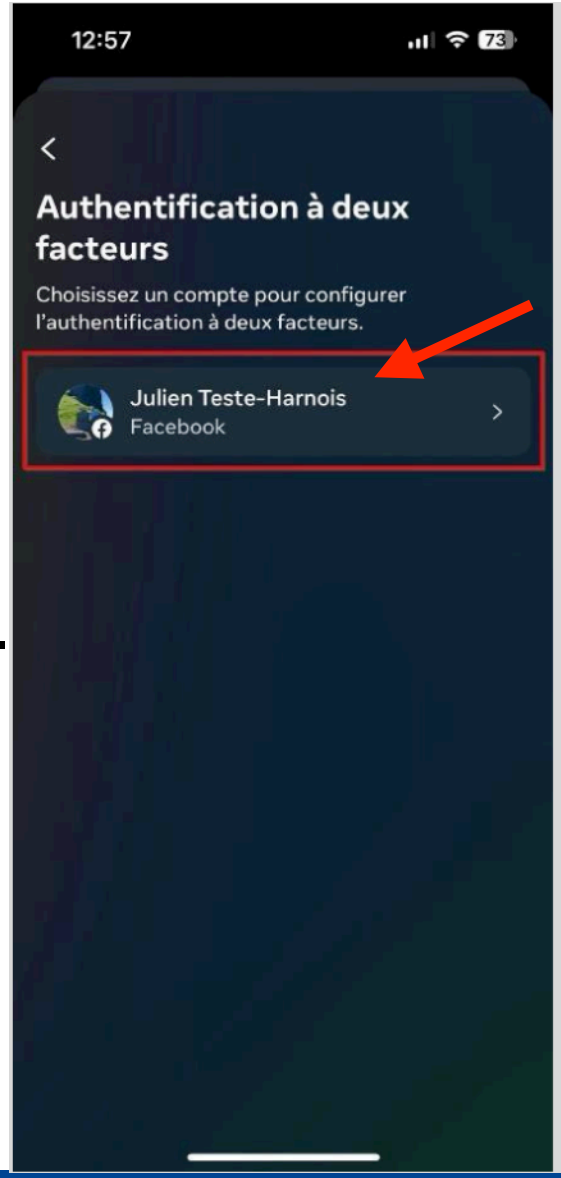


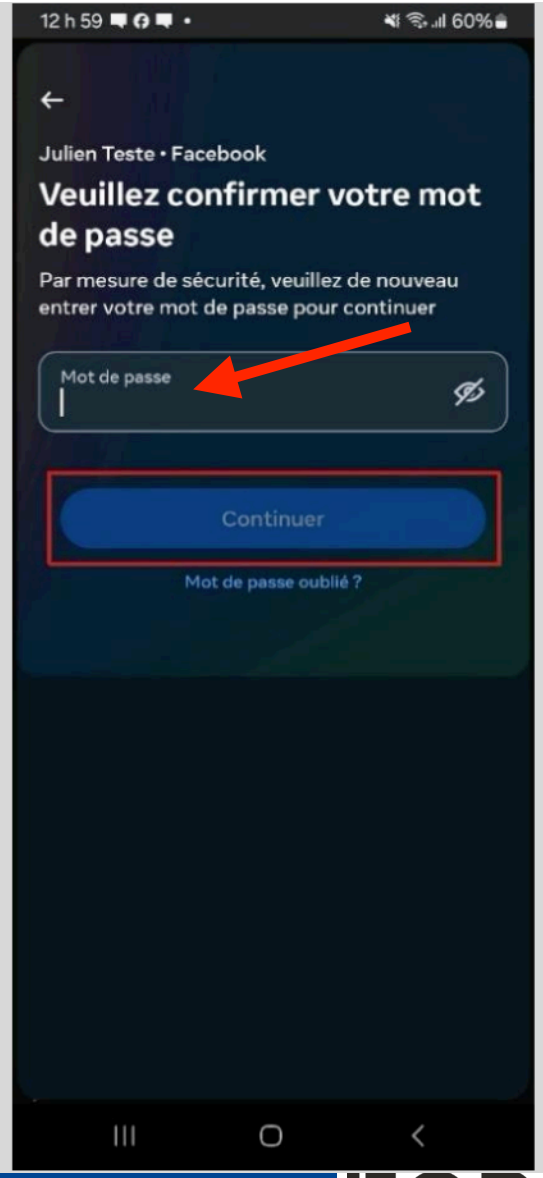


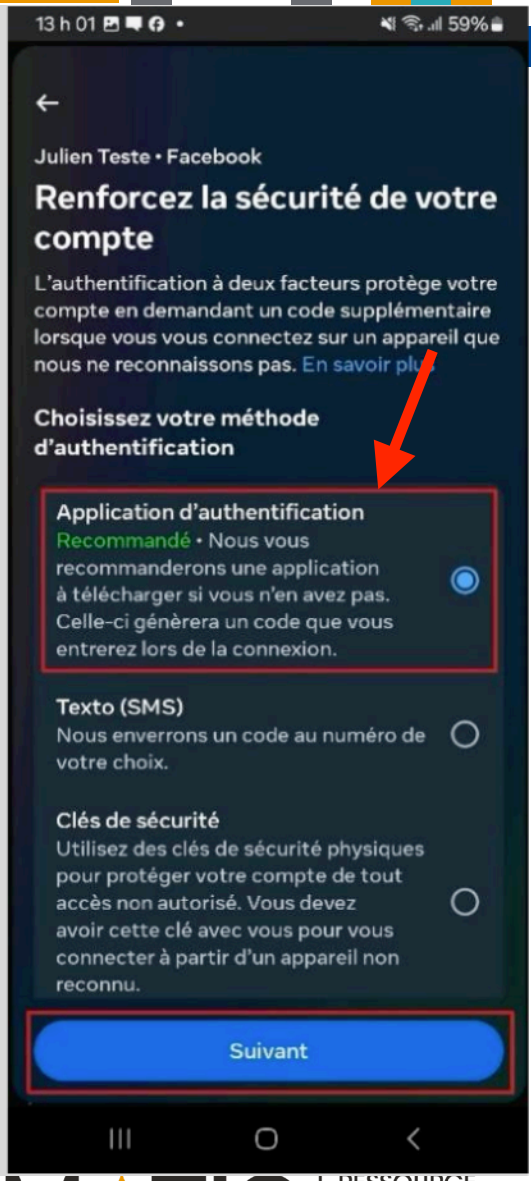


Exemple d’activation du 2FA: Facebook sur votre téléphone

3. Sélectionner votre compte Facebook, saisir votre mot de passe et appuyer sur « Continuer ».
4. Sélectionner la méthode de double authentification que vous souhaitez utiliser. Ici, la méthode par application d’authentification est choisie. Appuyer enfin sur « Suivant ».

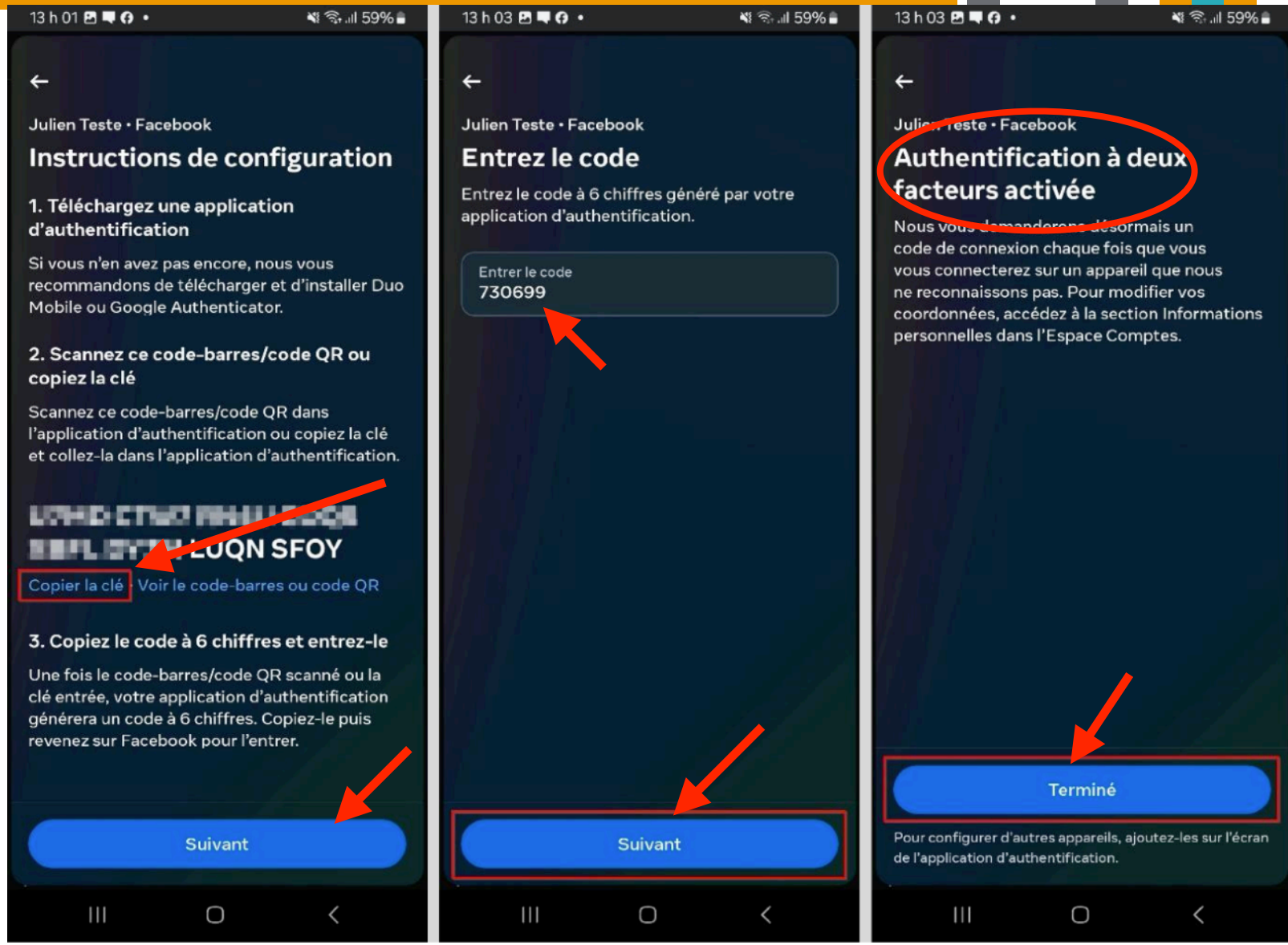






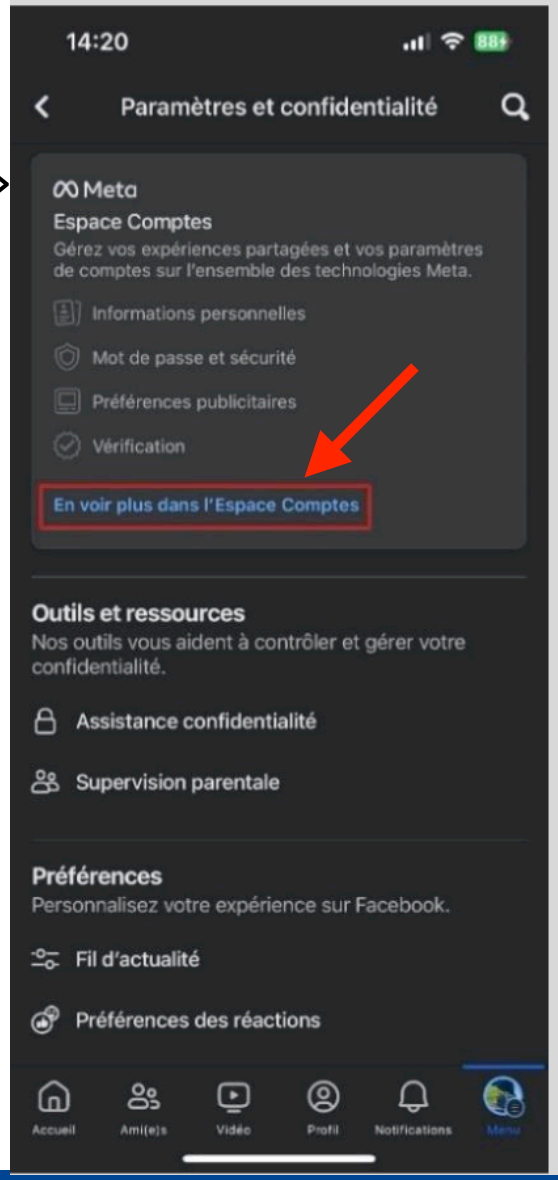
Exemple d'activation du 2FA: Facebook sur votre téléphone

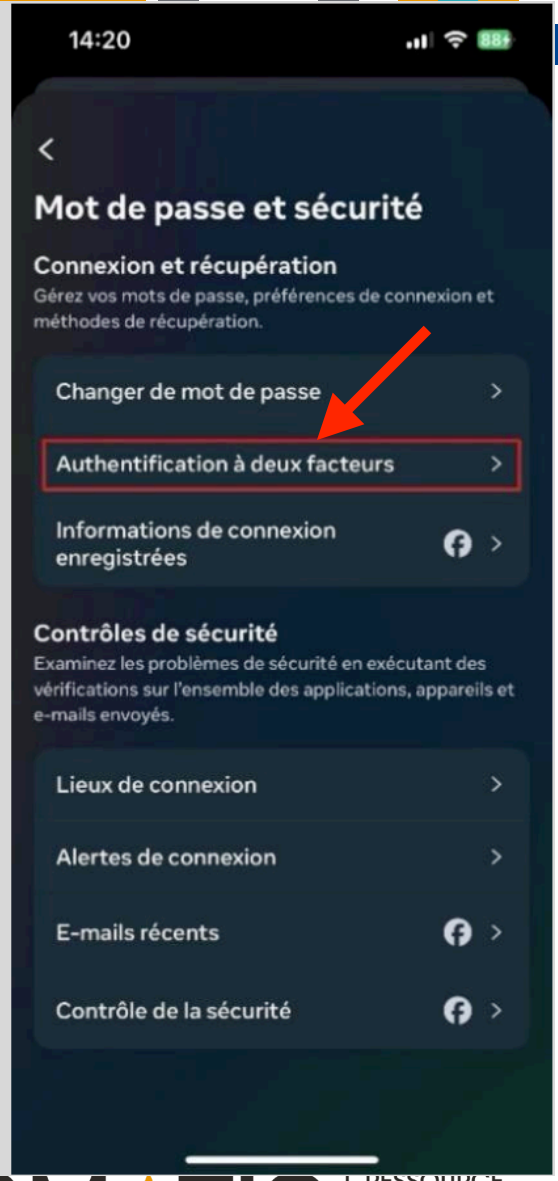
5. Copier la clé affichée, ouvrir votre application d'authentification, y coller la clé et appuyer sur « Suivant ».
6. Saisir dans Facebook le code aléatoire de 6 chiffres généré par votre application, puis appuyer sur « Suivant ».
7. L'authentification à 2 facteurs est maintenant activé. Il ne reste plus qu'à appuyer sur « Terminé ».



Exemple d'activation du 2FA: Facebook sur votre téléphone

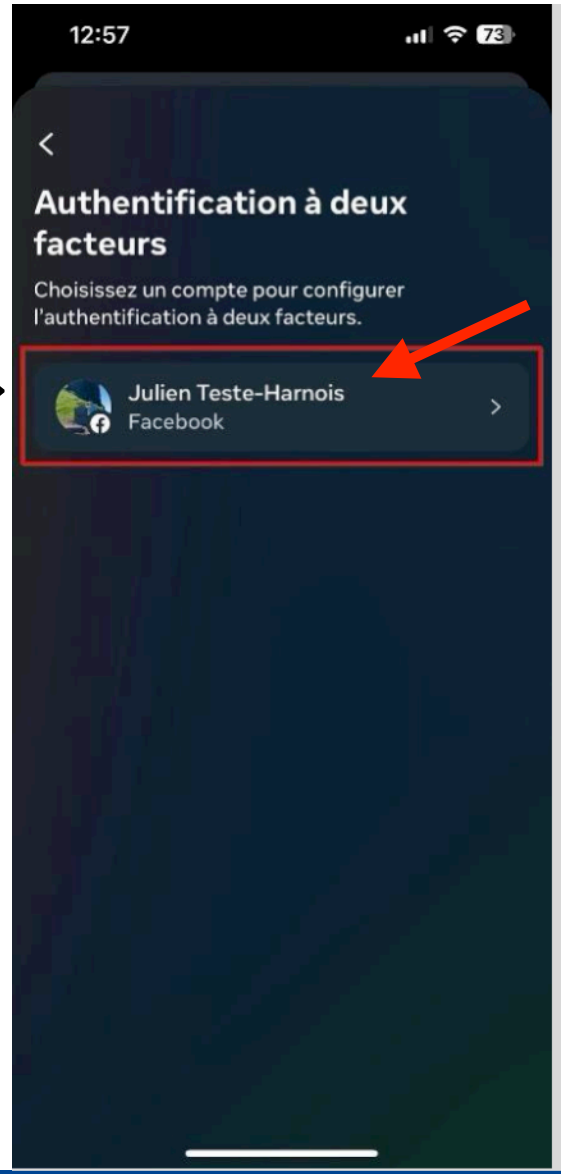
8. Pour obtenir vos codes de secours, retourner à la rubrique « Espace Comptes » choisir « Mot de passe et sécurité », puis « Authentification à deux facteurs ».

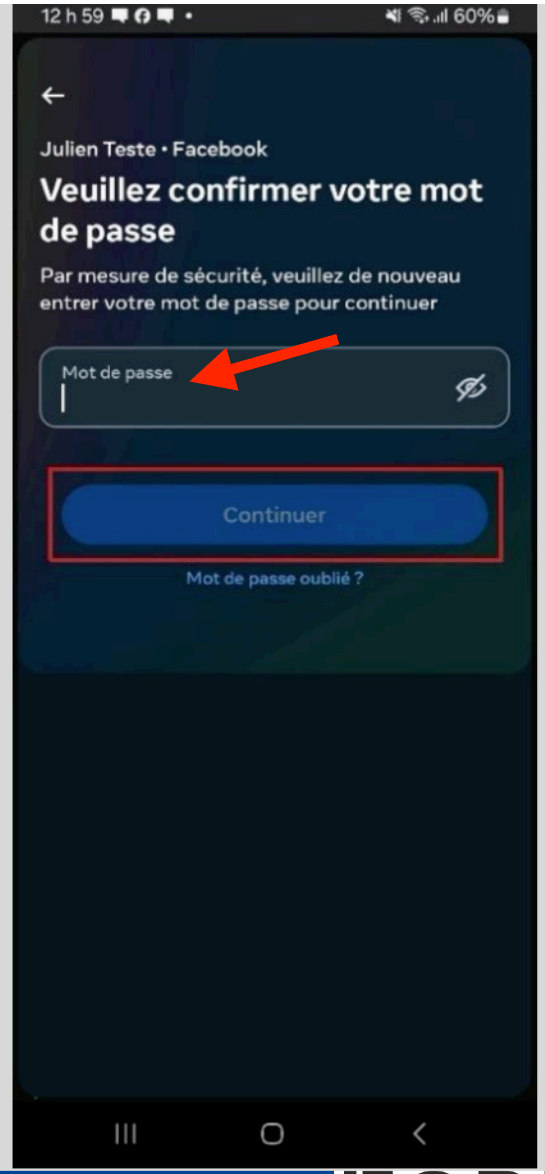


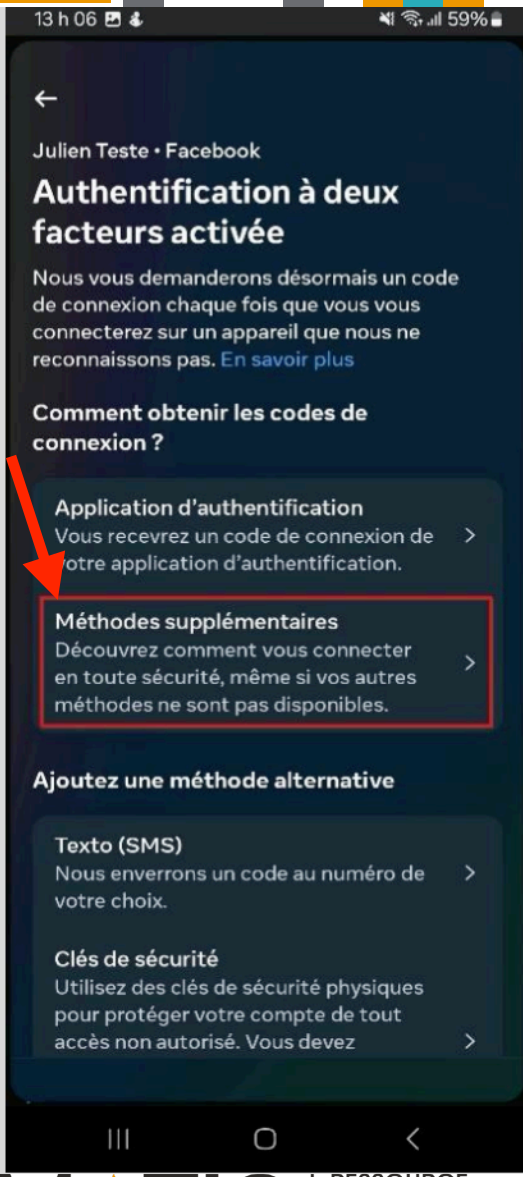


Exemple d'activation du 2FA: Facebook sur votre téléphone

9. Sélectionner votre compte Facebook, saisir votre mot de passe et appuyer sur « Continuer ».
10. Appuyer sur l'onglet « Méthodes supplémentaires »

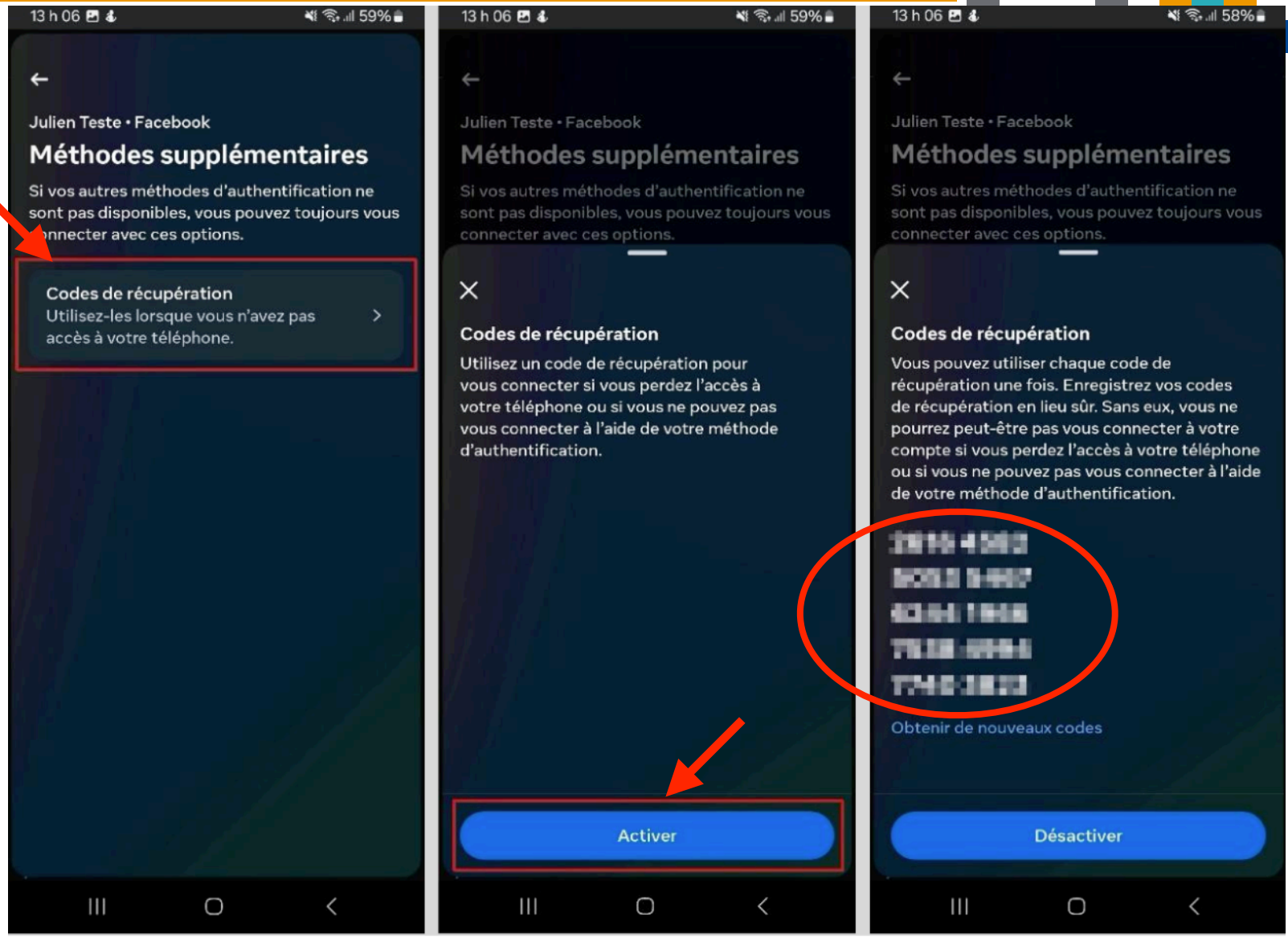






Exemple d'activation du 2FA: Facebook sur votre téléphone

11. Appuyer sur « Codes de récupération » puis sur « Activer ».
12. Récupérer vos codes de secours et conserver les dans un lieu sûr.



Références

1. Réseaux sociaux: comment protéger votre vie privée et sécuriser votre compte Facebook. Guide publié par Resolock, 2024. https://www.resolock.com/guides

2. What is Two Factor Authentification ?, Twilio Docs, https://www.twilio.com/docs/glossary/what-is-two-factor-authentication-2fa

3. The Best Authenticator Apps for 2024. Muchmore, Michael. PCmag.com, 15 décembre 2023. https://www.pcmag.com/picks/the-best-authenticator-apps

4. The Best Security Key for Multi-Factor Authentification. Eddy, Max. WireCutter, 5 janvier 2024.https://www.nytimes.com/wirecutter/reviews/best-security-keys/

5. Rafter,Dan. What is SIM swapping? SIM swap fraud explained and how to help protect yourself. Norton Blog, 13 juin 2023.

Questions ?