FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

SÉCURISER SES COMPTES EN LIGNE AVEC L'AUTHENTIFICATION À DEUX FACTEURS

9 AVRIL 2026

Contenu

- En quoi consiste l’authentification à deux facteurs (A2F)
- Principales méthodes A2F
- À propos des **applications** A2F
- Activer l’utilisation d’une application A2F pour un compte
- Exemple d’activation du A2F: Facebook sur votre téléphone
- Que faire en cas de défaillance de votre méthode A2F

En quoi consiste l'authentification à deux facteurs (A2F)

- **A2F:** il s'agit d'une méthode simple et sûre fortement recommandée pour sécuriser davantage l'accès à nos comptes en ligne contenant des informations sensibles.

- Avec le A2F, **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 de sécurité…)

En quoi consiste l'authentification à deux facteurs (A2F)

- Dans certains cas, l'utilisateur peut choisir d'activer ou non le A2F lorsque le compte en ligne offre cette option. Dans d'autres cas, le A2F doit être obligatoirement activé lorsque l'option est offerte.

- **Il existe plusieurs méthodes d'authentification à 2 facteurs**. Les méthodes pouvant être utilisées varient selon le fournisseur du compte à protéger.

  - Pour certains comptes, une seule méthode est offerte (ex: Service d'authentification gouvernementale du gouvernement du Québec, Banque Nationale)

  - D'autres comptes offrent plusieurs options (ex: ARC, Facebook, Google, …)

  - Lorsque plusieurs options sont offertes, il est parfois requis ou possible d'activer plus qu'une option. Ainsi, en cas d'impossibilité d'utiliser une des options choisies, on peut ainsi se rabattre sur une seconde méthode (ex: ARC).

Principales méthodes d'authentification à 2 facteurs

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

- **Répondre à une question de sécurité** (authentification en 2 étapes plutôt que authentification à 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, Service d'authentification gouvernemental du Québec…)

Principales méthodes d'authentification à 2 facteurs

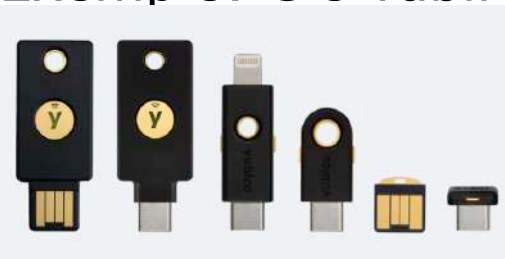
2.Méthodes basées sur un facteur de possession (suite):

- **Application d'authentification** générant à la chaîne des codes aléatoires uniques et temporaires (généralement 6 chiffres variant aux 30 sec).
  - **Méthode très répandue**: Facebook, Google, Firefox, PayPal, Amazon, Impôt Expert, ARC…
  - **Il existe de nombreuses d'applications d'authentification:**
    - Authy, Duo Mobile, 2FAS, Ente Auth, Google Authenticator, Microsoft Authenticator, etc.
    - Plusieurs gestionnaires de mots de passe offrent également la possibilité de générer ces codes, tel que Apple Mots de passe, Keeper, Bitwarden, 1Password, etc

Principales méthodes d'authentification à 2 facteurs

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

- **clé de sécurité physique** certifiée.
  - Exemple: Clé YubiKey (plusieurs modèles, dont la 5C NFC à 82 $ chez Amazon).



- **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. Google, Apple, Microsoft, Facebook, 1Password, Bitwarden, LastPass acceptent les clés Yubikey.

- Utile de posséder deux clés plutôt qu'une seule (en cas de perte d'une d'entre elles).

À propos des applications A2F

- **Pour une comparaison détaillée des différentes applications** offertes, voir les **références 2 et 5** à la fin de ce document.

- L'utilisation de son gestionnaire de mots de passe pour générer ses codes A2F est pratique, mais il y a un risque: si une personne non autorisée accède à vos mots de passe, elle accède aussi à vos codes A2F. C'est un peu comme mettre **« tous nos oeufs dans le même panier ».**

- Les fonctionnalités ou particularités offertes par les différentes applications A2F peuvent varier de l'une à l'autre:

    - Certaines applications nécessitent l'ouverture d'un compte, généralement gratuit. Exemple: Authy qui exige en plus un numéro de téléphone et Ente Auth.

À propos des applications A2F

- Alors que la plupart des applications peuvent être installées sur plusieurs de vos appareils tout en se synchronisant entre elles via votre compte cloud, **Duo Mobile** ne peut être installé que sur un seul appareil (pas de synchronisation cloud).

- Certaines applications vous offrent la possibilité de sauvegarder une **copie de vos jetons dans un fichier local protégé par un mot de passe** (exemple: 2FAS), ou **encore dans le cloud** auquel est relié votre appareil (ex: iCloud, Google Drive…).

- Selon les applications offrant la sauvegarde dans le cloud, celle-ci peut être **chiffrée de bout en bout** (exemple: 2FAS, Ente Auth, Duo Mobile…) **ou non** (exemple: Google Authenticator).

Comment activer l'utilisation d'une application A2F

1. Choisir et **télécharger dans votre (vos) appareil(s) l'application** que vous souhaitez utiliser.

2. **Accéder aux paramètres de sécurité de son compte à protéger** et sélectionner l'option « Validation en 2 étapes », « Authentification à 2 facteurs » ou autre option similaire.

3. **Sélectionner l'onglet avec un libellé du genre « Authenticator » ou « Application d'authentification »**. Un code QR et une clé secrète devraient s'afficher à l'écran.

Comment activer l'utilisation d'une application A2F

4. **Ouvrir votre application A2F dans un autre de vos appareils**, sélectionner l'option permettant d'ajouter un compte **et numériser le code QR**. Si vous n'avez pas d'autre appareil que celui sur lequel le code QR est affiché, **vous pouvez aussi simplement copier la clé secrète et la coller dans votre application A2F**.

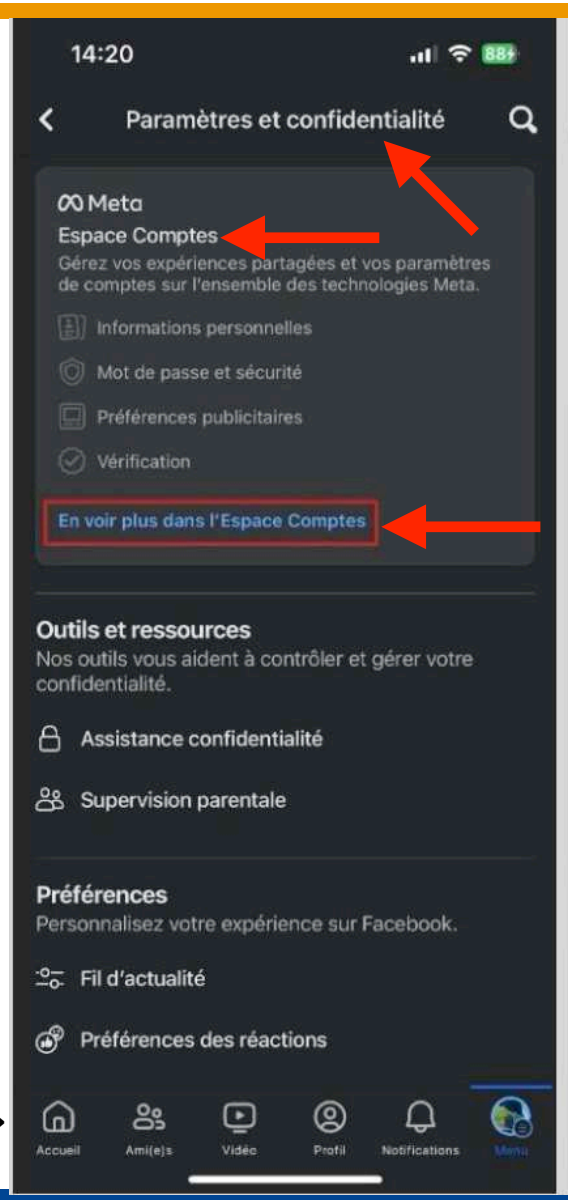
5. Votre application générera un code de 6 chiffres que vous devrez saisir dans votre compte. Ceci activera la double authentification.

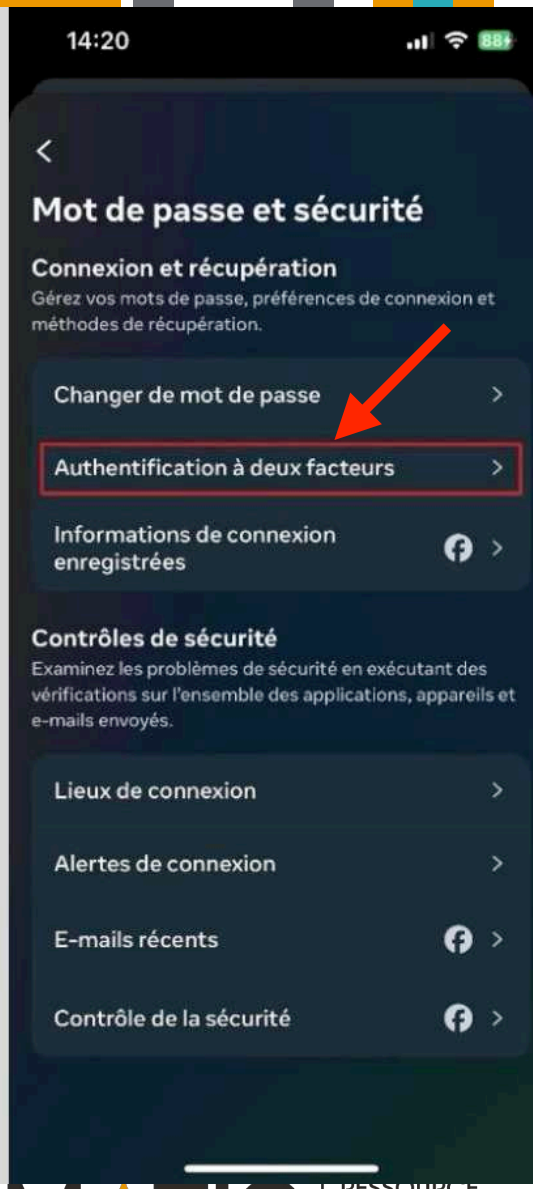
6. Dorénavant, pour accéder à votre compte, vous devrez saisir votre mot de passe et le code de 6 chiffres fourni par votre application A2F.

Exemple d'activation du A2F: Facebook sur votre téléphone

Ce qui suit est extrait de la **référence 10:**

- Dans le menu principal de l'application Facebook (coin supérieur gauche), sélectionner l'onglet « Paramètres et confidentialité», puis l'onglet « Paramètres » afin d'afficher la rubrique « Espace Comptes ».
- Appuyer sur « En voir plus dans l'espace compte »
- Sélectionner « Mot de passe et sécurité »
- appuyer sur l'onglet « Authentification à deux facteurs »

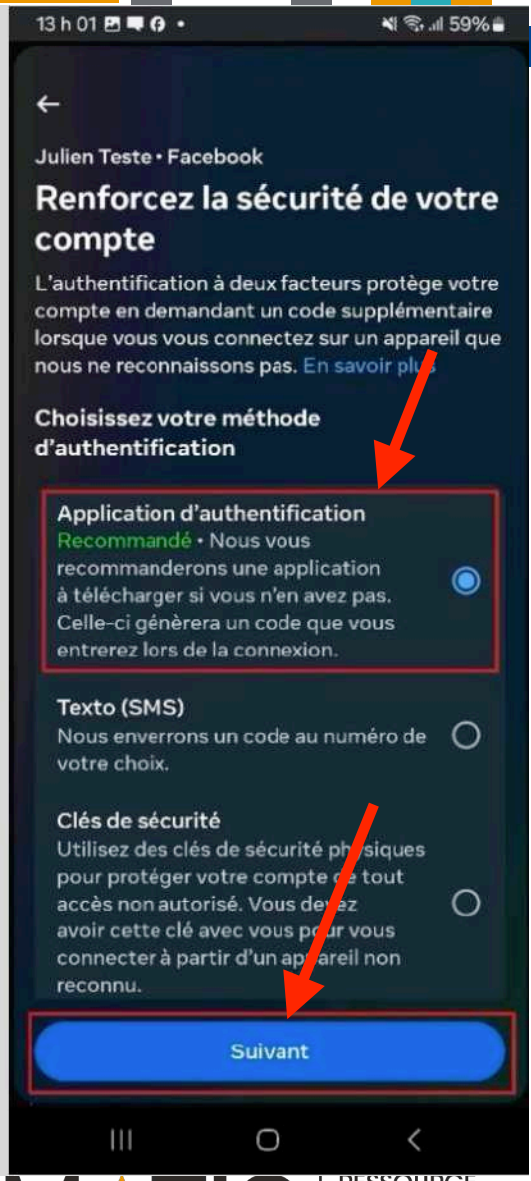




Exemple d'activation du A2F: Facebook sur votre téléphone

- Sélectionner votre compte Facebook, saisir votre mot de passe et appuyer sur « Continuer ».

- Sélectionner la méthode de double authentification que vous souhaitez utiliser. Ici, la méthode par application d'authentification est choisie. Appuyer enfin sur « Suivant ».

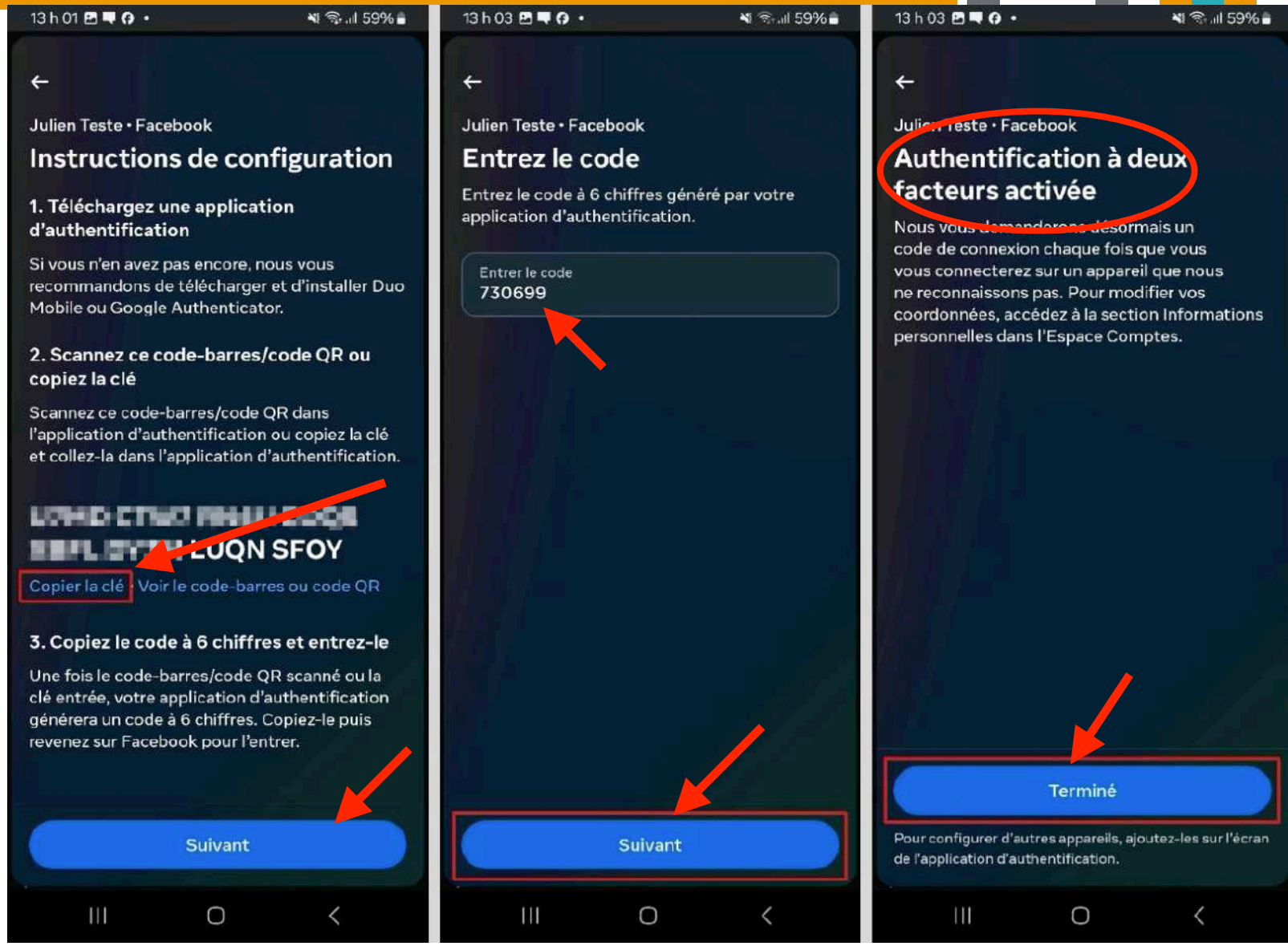


Exemple d'activation du A2F: Facebook sur votre téléphone

- Copier la clé affichée, ouvrir votre application d'authentification, y coller la clé et appuyer sur « Suivant ». Vous pouvez aussi numériser le code QR avec un autre appareil tel qu'expliqué précédemment.

- Saisir dans Facebook le code aléatoire de 6 chiffres généré par votre application, puis appuyer sur « Suivant ».

- L'authentification à 2 facteurs est maintenant activé. Il ne reste plus qu'à appuyer sur « Terminé ».



Que faire en cas de défaillance de votre méthode A2F

- De nombreux comptes en ligne offrent plusieurs options de double authentification. Cela offre la possibilité d'utiliser une autre méthode de A2F en cas de défaillance ou d'impossibilité d'utiliser votre première méthode.

- Parmi ces méthodes, on retrouve l'utilisation de **codes de secours (ou de récupération)** qui permet d'accéder à votre compte dans l'éventualité où vous ne pouvez pas fournir le code de double authentification requis.

- Un code de secours est une série de caractères 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.

Que faire en cas de défaillance de votre méthode A2F

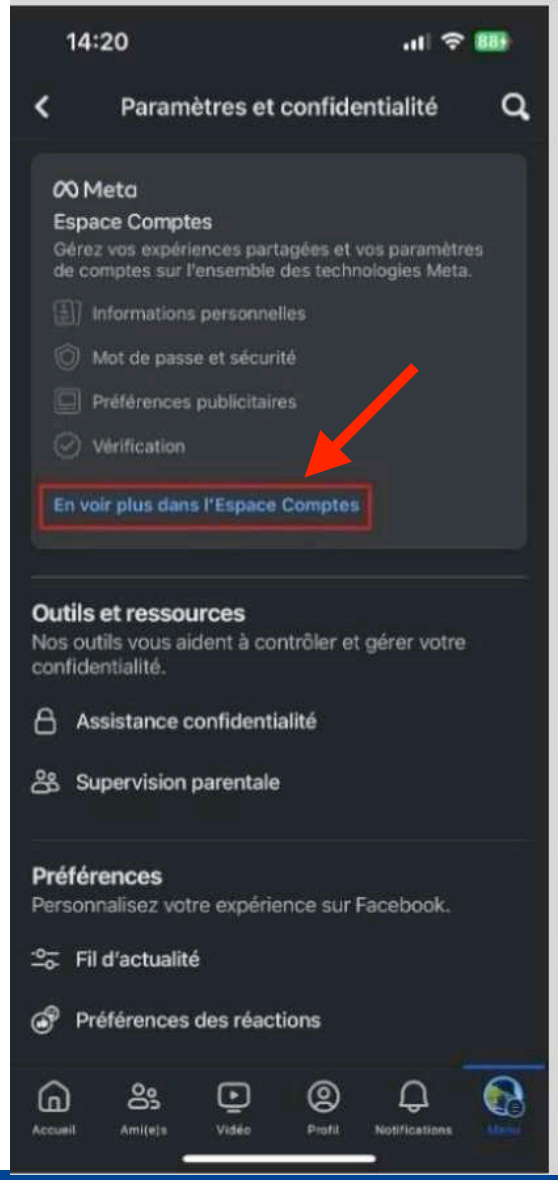
- Un code de secours ne peut être utilisé **qu'une seule fois**. Si vous devez l'utiliser, il est donc important de disposer d'un autre code de secours au cas où vous en auriez besoin ultérieurement.

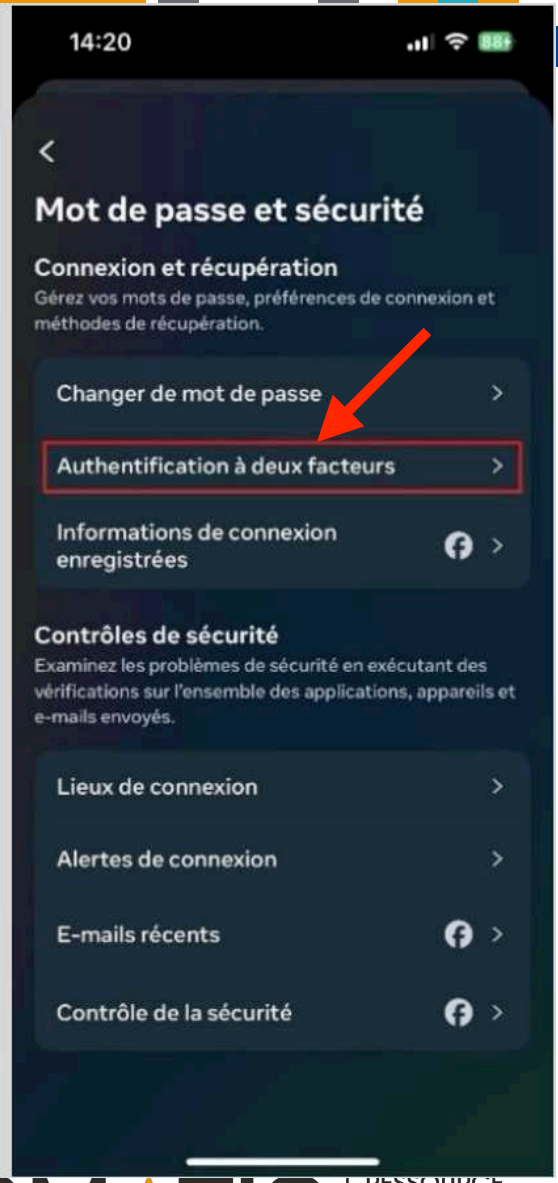
- Certains comptes fourniront une seul code de secours, alors que d'autres en fourniront plusieurs (jusqu'à 10 par exemple !).

- 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).

Exemple d'obtention de codes de secours: Facebook

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

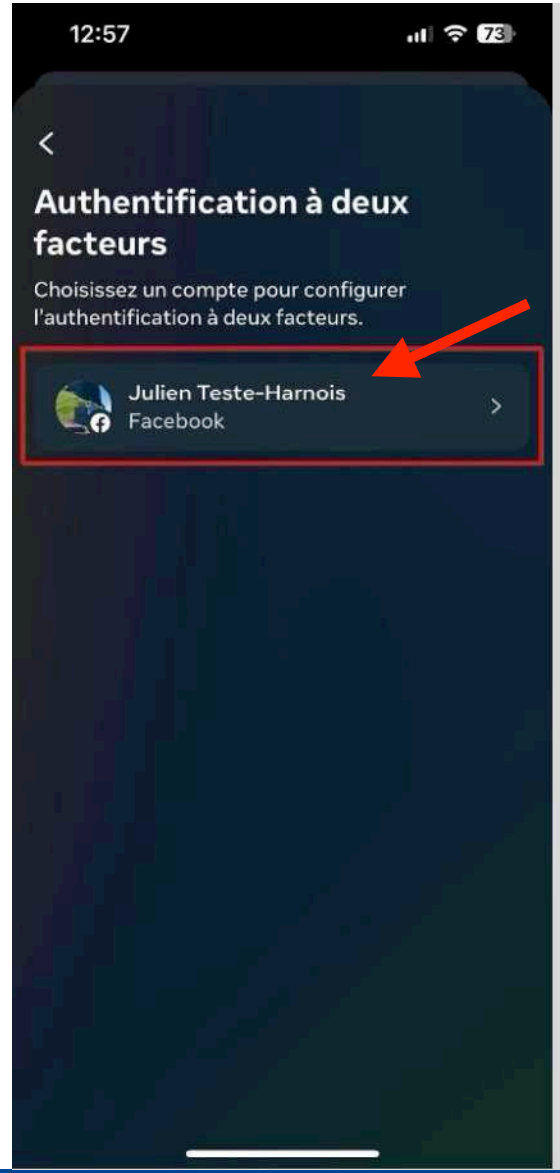


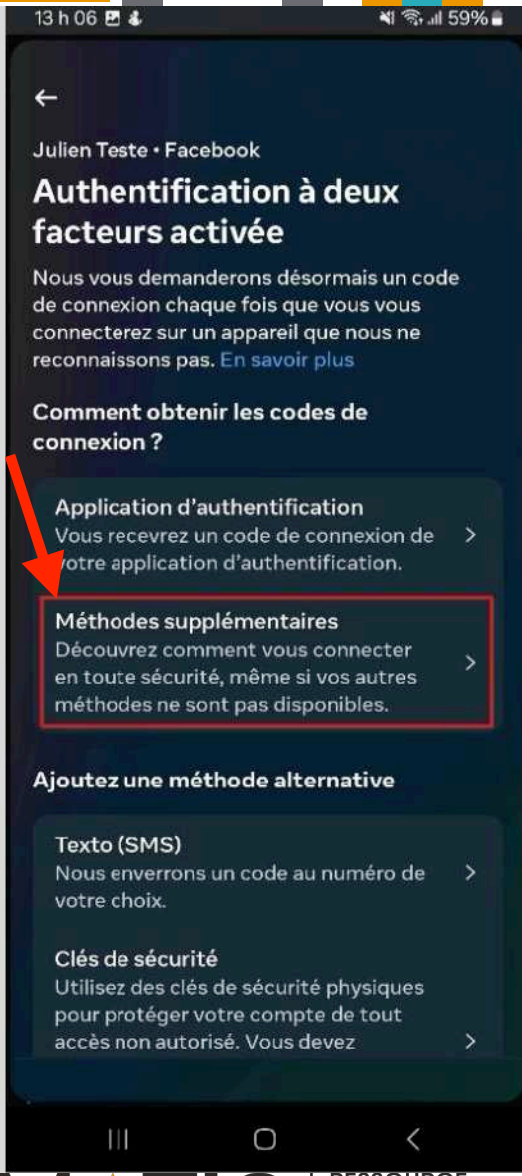


Exemple d'activation du A2F: Facebook sur votre téléphone

- Sélectionner votre compte Facebook, saisir votre mot de passe et appuyer sur « Continuer ».

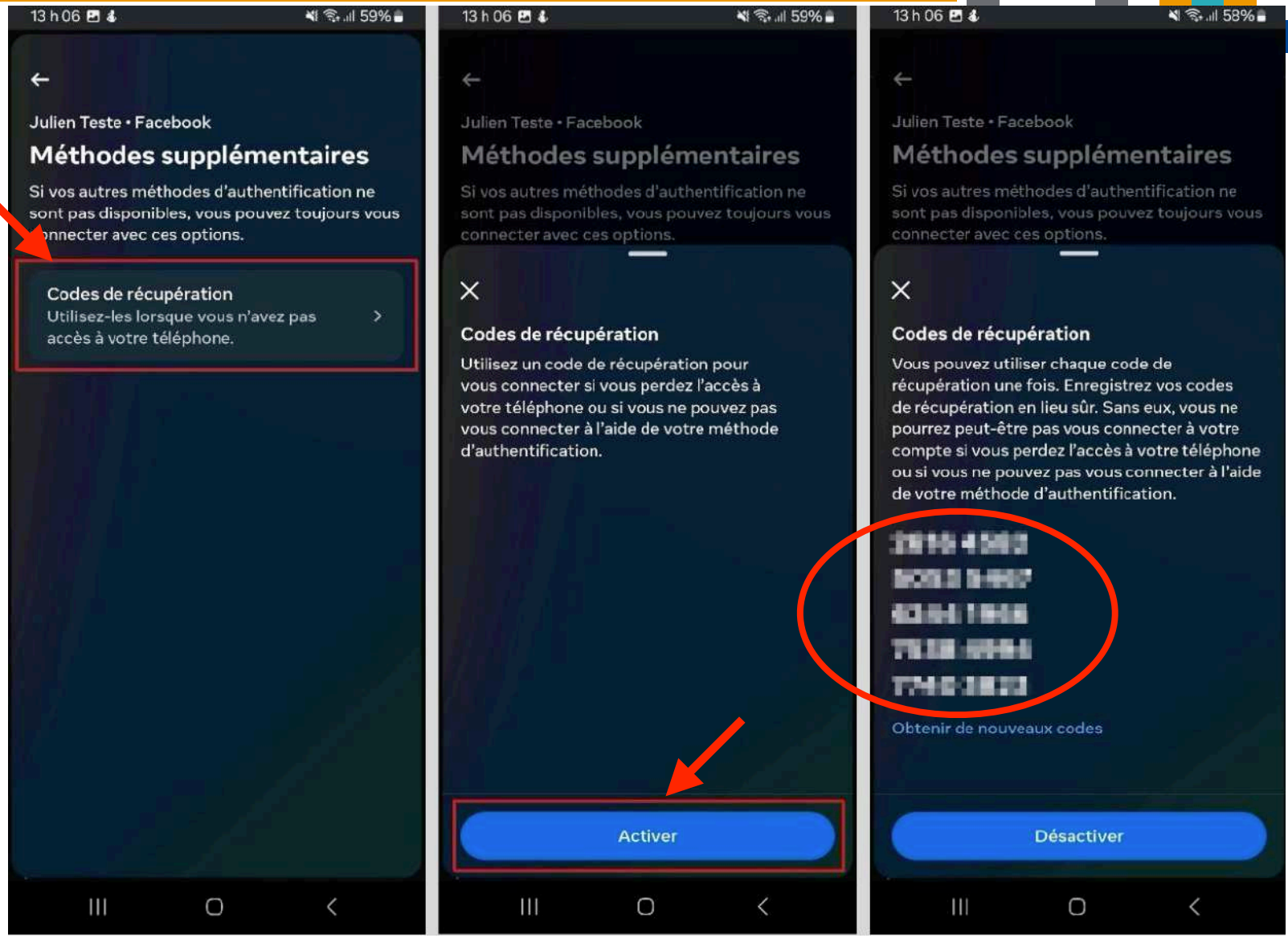
- Appuyer sur l'onglet « Méthodes supplémentaires ».





Exemple d'activation du A2F: Facebook sur votre téléphone

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



Références

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

2. Quelles sont les meilleures applications de double authentification (2FA) ? Comparatif 2026, Clubic 25 août 2025. https://www.clubic.com/guide-achat-538328-authentification-2fa-les-meilleures-applications-en-2024.html

3. Protégez vos comptes à l'aide d'une application d'authentification à double facteur. François Charron, 28 mai 2025. https://francoischarron.com/securite/logiciels-securite-prevention/protegez-vos-comptes-a-laide-dune-application-dauthentification-a-double-facteur/ve9i3UMndR/

4. Comment utiliser la double authentification (2FA), Just Geek 23 juin 2025. https://www.justgeek.fr/utiliser-double-authentification-2fa-139483/

5. 9 meilleures applications d'authentification à deux facteurs (2FA), Just Geek 19 mars 2025. https://www.justgeek.fr/meilleures-applications-authentification-a-deux-facteurs-2fa-79353/

Références

6. The Best Authenticator Apps for 2026. Key, Kim. PCmag.com, 19 mars 2026. https://www.pcmag.com/picks/the-best-authenticator-apps

7. The Best Two-Factor Authentification App. Eddy, Max. WireCutter, 18 février 2025. https://www.nytimes.com/wirecutter/reviews/best-two-factor-authentication-app/

8. The Best Security Key for Multi-Factor Authentification. Eddy, Max. WireCutter, 21 février 2025. https://www.nytimes.com/wirecutter/reviews/best-security-keys/

9. Birchall,Mark. What is SIM swapping and how to prevent it. Norton Blog, 13 février 2026.

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