

## Instructions de configuration de l'authentification multifactorielle (MFA)

L'État de New York a commencé à utiliser l'authentification multifactorielle (MFA) sur certaines de ses applications destinées au public. La MFA est un moyen de garantir la sûreté et la sécurité de votre compte. Il faut un deuxième facteur pour prouver que vous êtes bien celui que vous prétendez être, au-delà du simple mot de passe. Si vous utilisez une application protégée par MFA, même si quelqu'un devine ou vole votre mot de passe, il ne pourra pas se connecter sans votre second facteur. Alors qu'un mot de passe est quelque chose que vous connaissez, le second facteur est quelque chose que vous êtes (généralement lu par un dispositif biométrique) ou quelque chose que vous avez.

**Conseil :** Il est recommandé de configurer plus d'une méthode d'authentification multifactorielle.

**Conseil :** Si vous devez configurer une méthode d'authentification multifactorielle qui utilise une application pour téléphone (Okta Verify ou Google Authenticator), téléchargez l'application avant de cliquer sur le bouton « Setup » de la page du navigateur « Set up multifactor authentication ». Les deux méthodes d'authentification multifactorielle qui utilisent des applications sont Okta Verify et Google Authenticator. Pour télécharger votre application maintenant, [cliquez ici pour Android](#) et [ici pour les appareils Apple](#).

**REMARQUE :** Toutes les captures d'écran proviennent d'un écran d'ordinateur, à moins qu'il ne s'agisse d'un téléphone portable.

### Index

[Configuration de Google Authenticator Authentification en plusieurs étapes](#)

[Téléchargement de Google Authenticator pour Android](#)

[Téléchargement de Google Authenticator pour Apple](#)

[Utilisation de l'application](#)

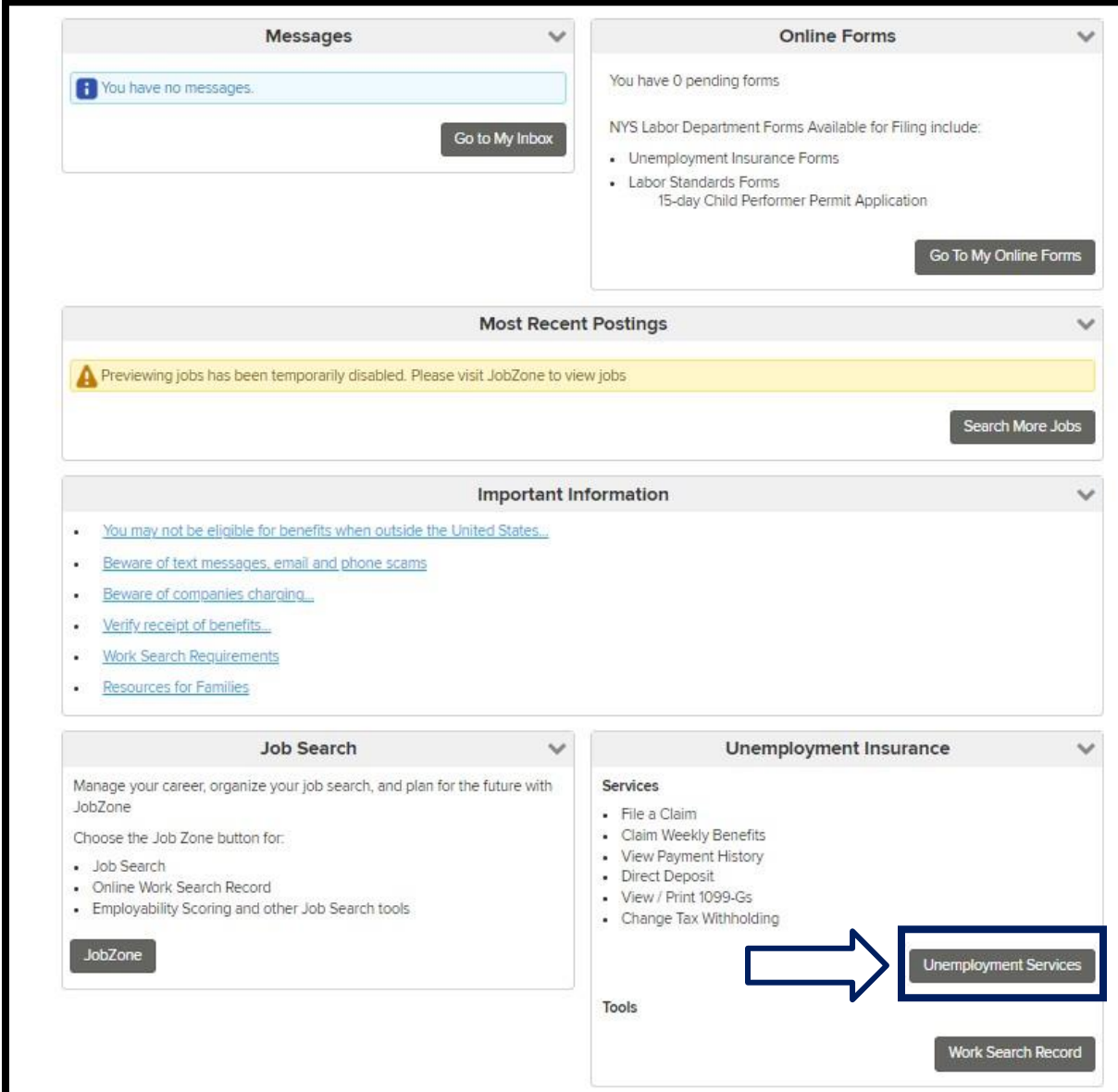
[Instructions pour la saisie d'une clé de paramétrage](#)

[Instructions pour scanner un code QR](#)

[Messages d'erreur potentiels](#)

## Configuration de l'authentification multifactorielle Google Authenticator

Si vous n'êtes pas encore inscrit à la MFA, vous serez invité à vous inscrire après vous être connecté aux services de travail en ligne et avoir cliqué sur le bouton de demande « Services de chômage ».

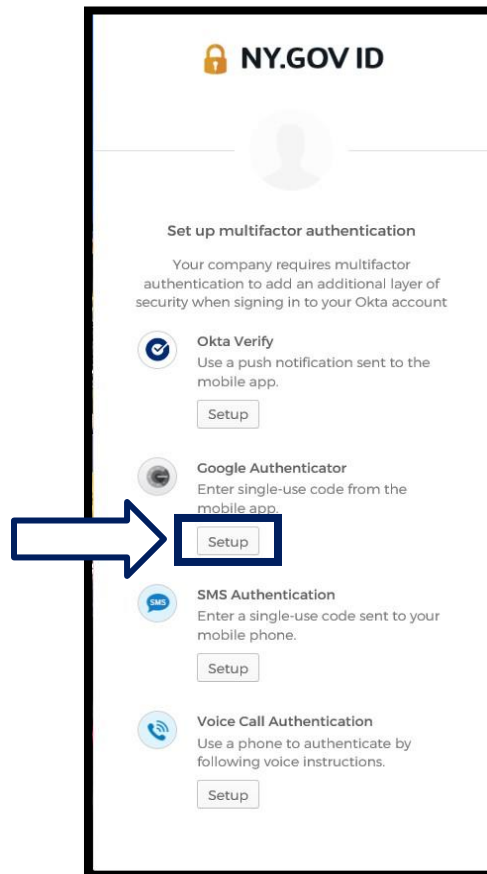


The screenshot shows a user dashboard with several sections:

- Messages:** "You have no messages." with a "Go to My Inbox" button.
- Online Forms:** "You have 0 pending forms." and a list of forms available for filing: Unemployment Insurance Forms, Labor Standards Forms, and 15-day Child Performer Permit Application. Includes a "Go To My Online Forms" button.
- Most Recent Postings:** A yellow warning banner: "Previewing jobs has been temporarily disabled. Please visit JobZone to view jobs." with a "Search More Jobs" button.
- Important Information:** A list of links: "You may not be eligible for benefits when outside the United States...", "Beware of text messages, email and phone scams", "Beware of companies charging...", "Verify receipt of benefits...", "Work Search Requirements", and "Resources for Families".
- Job Search:** "Manage your career, organize your job search, and plan for the future with JobZone." Includes a "Job Zone button for:" list: Job Search, Online Work Search Record, and Employability Scoring and other Job Search tools. Includes a "JobZone" button.
- Unemployment Insurance:** "Services" list: File a Claim, Claim Weekly Benefits, View Payment History, Direct Deposit, View / Print 1099-Gs, and Change Tax Withholding. Includes a "Tools" section with a "Work Search Record" button. A blue callout box highlights the "Unemployment Services" button, with a blue arrow pointing to it from the right.

Sur l'écran de votre ordinateur, vous verrez un écran qui vous demande de configurer votre authentification multifactorielle.

1. Sur votre téléphone intelligent, téléchargez l'application Google Authenticator.
2. Sur l'écran de votre ordinateur, cliquez sur Setup (Configuration) sous Google Authenticator pour commencer le processus d'installation.



3. Un nouvel écran s'ouvrira sur le moniteur de votre ordinateur. Choisissez l'iPhone ou l'Android en fonction de votre appareil. Si vous avez une tablette Apple, choisissez iPhone.

**Si vous avez un Android, vous verrez ceci :**



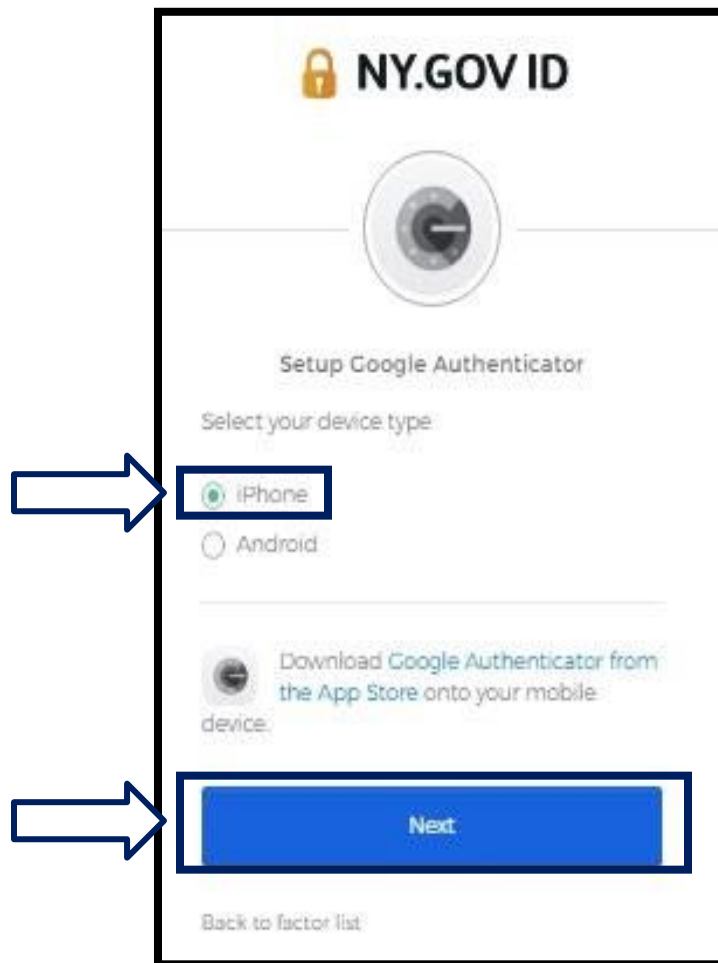
Il vous sera demandé de télécharger l'application Google Authenticator depuis le Google Play Store. Si vous ne l'avez pas encore fait, vous devriez télécharger cette application dès maintenant.

[Cliquez ici pour obtenir des instructions sur la façon de télécharger l'application Google Authenticator sur votre appareil Android.](#)

4. Cliquez sur le bouton Suivant.

[Cliquez ici pour continuer.](#)

Si vous choisissez iPhone, vous verrez ceci :



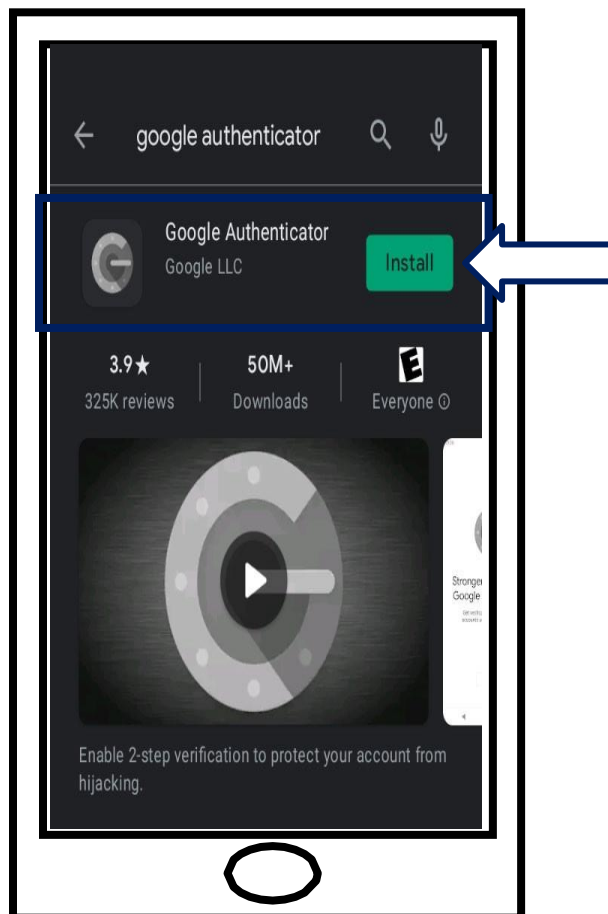
Il vous sera demandé de télécharger l'application Google Authenticator depuis l'App Store. Si vous ne l'avez pas encore fait, vous devriez télécharger cette application dès maintenant.

[Cliquez ici pour obtenir des instructions sur la façon de télécharger l'application Google Authenticator sur votre appareil Apple.](#)

5. Cliquez sur le bouton Suivant.

## Instructions pour le téléchargement de l'application Google Authenticator sur un appareil Android.

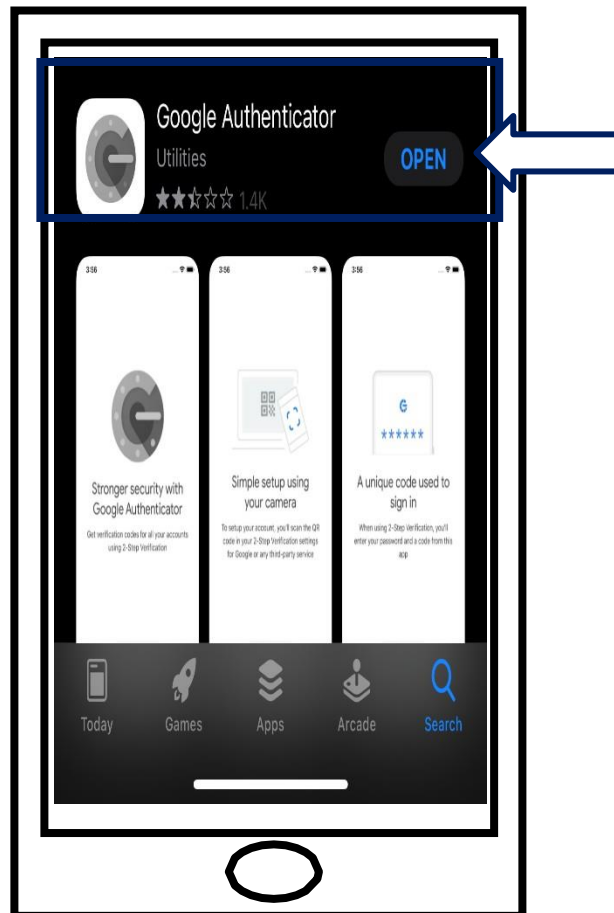
6. Sur votre smartphone ou votre tablette, accédez à Google Play. Assurez-vous que votre smartphone ou votre tablette utilise la dernière version du système d'exploitation (OS).
7. Dans Google Play, recherchez l'application Google Authenticator.
8. Une fois que vous avez trouvé l'application, téléchargez-la et installez-la sur votre smartphone ou votre tablette. *(REMARQUE : L'application peut apparaître légèrement différente selon la version du téléphone)*



[Cliquez ici pour revenir à la page principale.](#)

## Instructions pour le téléchargement de l'application Google Authenticator sur un appareil Apple.

9. Sur votre smartphone ou votre tablette, accédez à l'App Store. Assurez-vous que votre smartphone ou votre tablette utilise la dernière version du système d'exploitation (OS).
10. Dans l'App Store, recherchez l'application Google Authenticator.
11. Sélectionnez l'application mobile Google Authenticator.
12. Téléchargez et installez l'application.



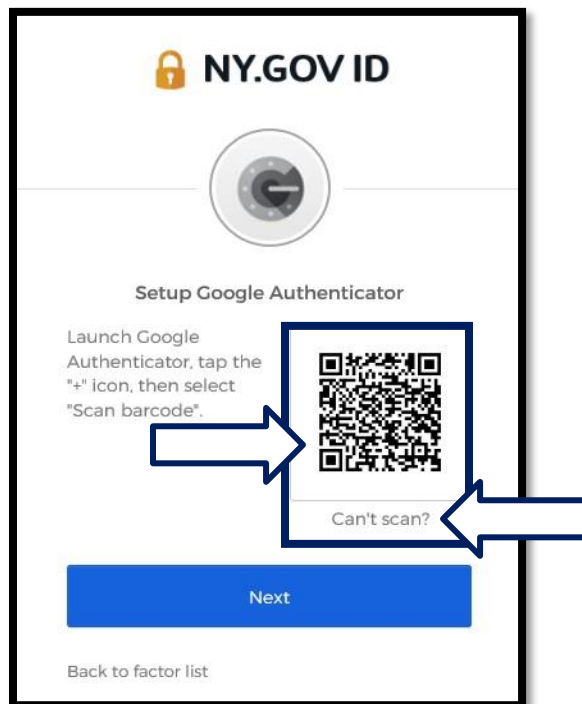
13. Une fois que vous avez installé l'application Google Authenticator sur votre smartphone ou votre tablette, accédez à l'application sur votre appareil et ouvrez-la.

[Cliquez ici pour revenir à la page principale.](#)

Ouvrez l'application Google Authenticator sur votre smartphone ou votre tablette.

14. L'écran de votre ordinateur affiche maintenant une boîte de dialogue contenant un code de réponse rapide (QR).

- Si vous ne parvenez pas à scanner le code QR, cliquez sur l'option **Can't Scan ?** sous le code QR sur l'écran de votre ordinateur. [Cliquez ici pour obtenir des instructions concernant l'option Can't Scan.](#)

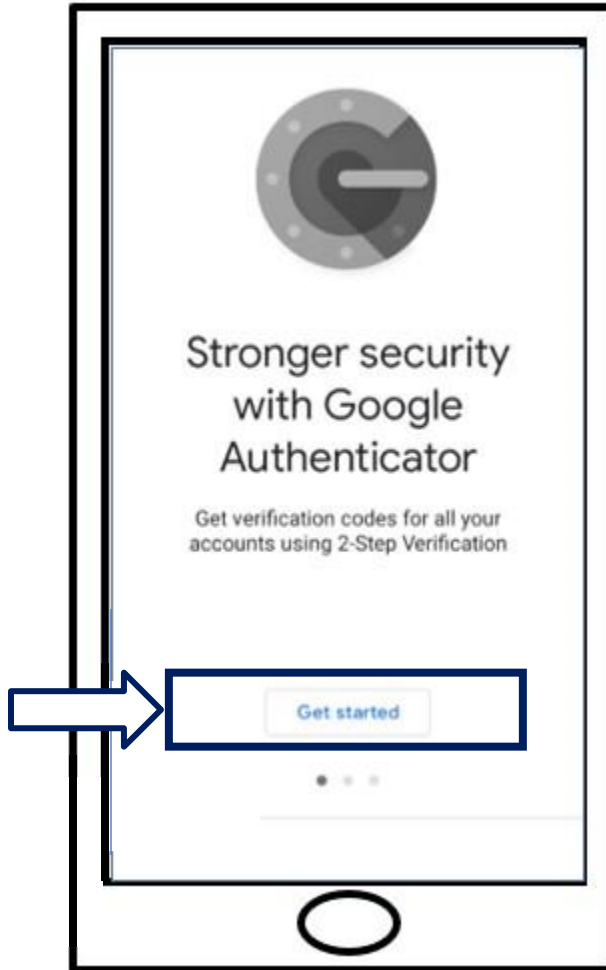


15. Accédez à votre application Google Authenticator et ouvrez-la.



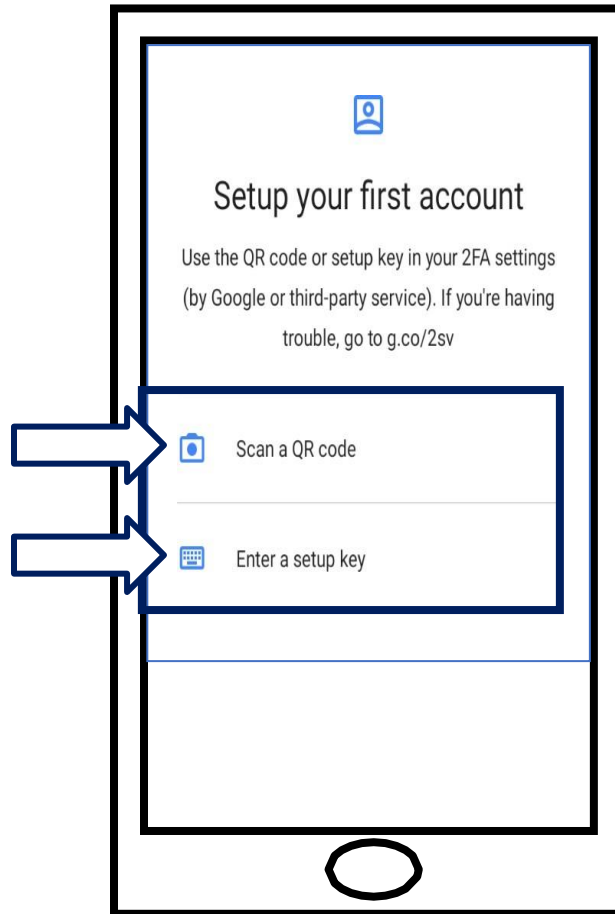
## Utilisation de l'application Google Authenticator

16. Sur votre smartphone, vous verrez cet écran.



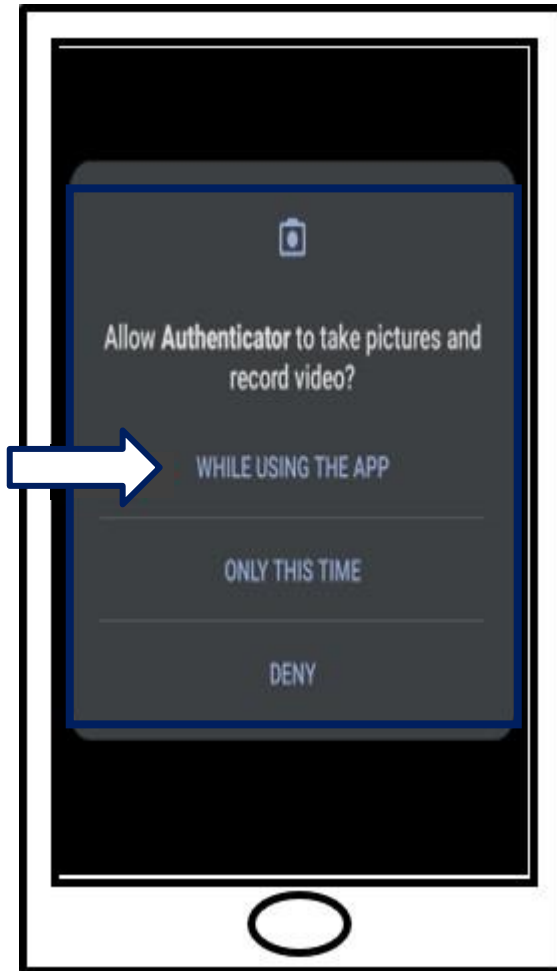
17. Cliquez sur **Get Started (Démarrer)**.

18. Cet écran s'ouvre. Vous aurez le choix entre **scanner un code QR** ou **Saisir une clé de configuration**. Choisissez-en un.



## Instructions pour utiliser l'application Google Authenticator afin de scanner un code QR : Sur un appareil Android

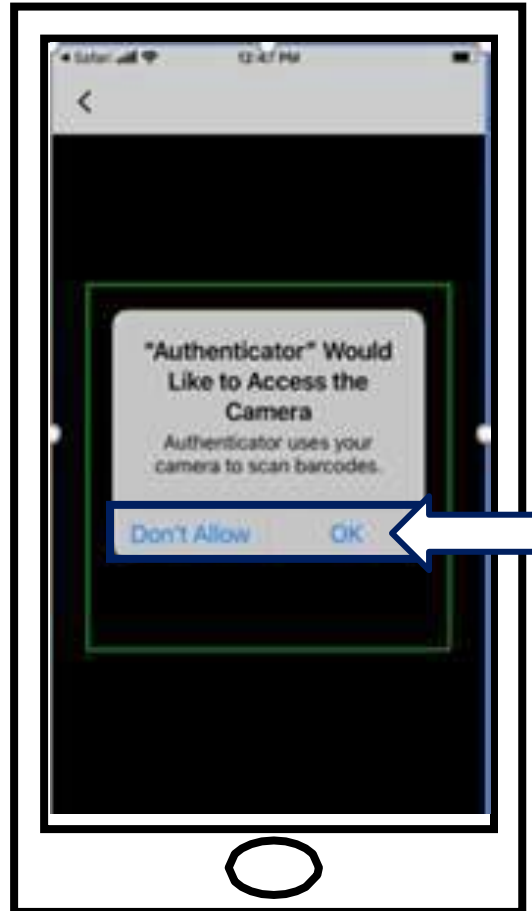
19. L'application vous demandera la permission d'utiliser votre appareil photo. Cliquez sur **Pendant l'utilisation de l'application**.



20. Accéder à [Scanner le code QR.](#)

## Sur un appareil Apple

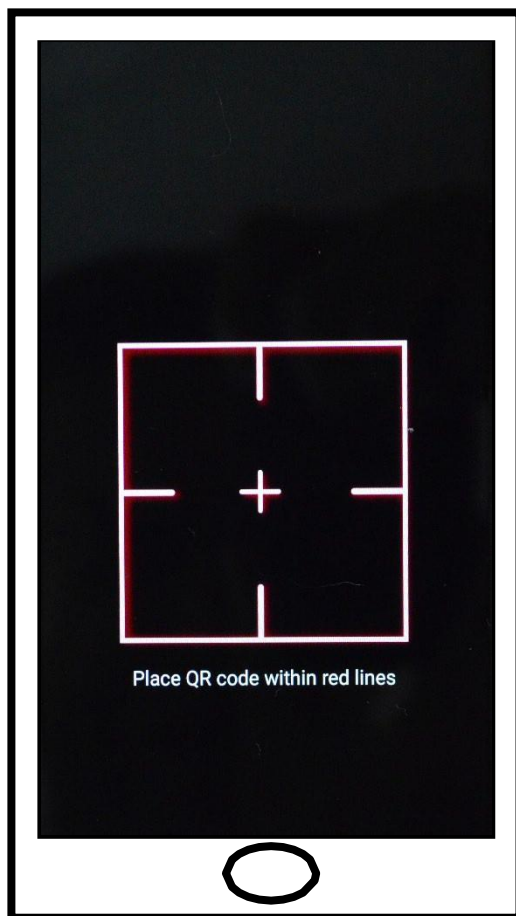
21. Vous verrez un message indiquant que « *Authenticator* » souhaite accéder à la caméra. Cliquez sur **OK**.



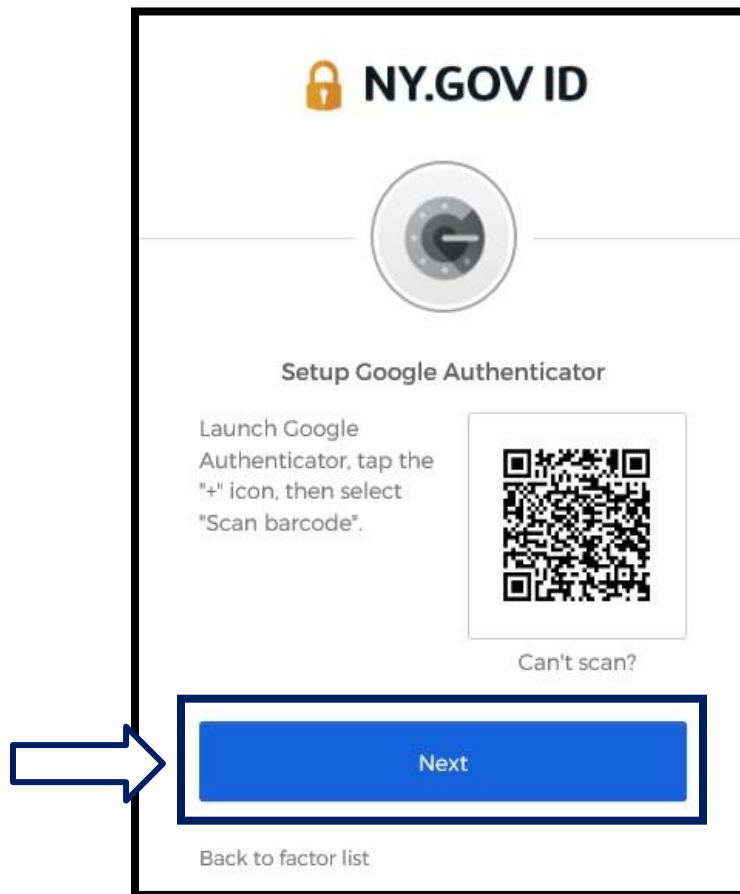
22. Procédez à [Scanner un code QR](#).

**Scanner un code QR**

23. L'écran de votre smartphone affiche maintenant un écran vide avec un carré au centre.



24. Dirigez l'appareil photo de votre smartphone ou de votre tablette vers le code QR qui se trouve sur l'écran de votre ordinateur (voir l'image ci-dessous), de sorte que le code QR sur l'écran de l'ordinateur apparaisse dans la case verte sur l'écran de votre smartphone. L'application scanne automatiquement le code sur votre téléphone ou votre tablette.



25. Procédez aux étapes [Saisir votre code](#) .

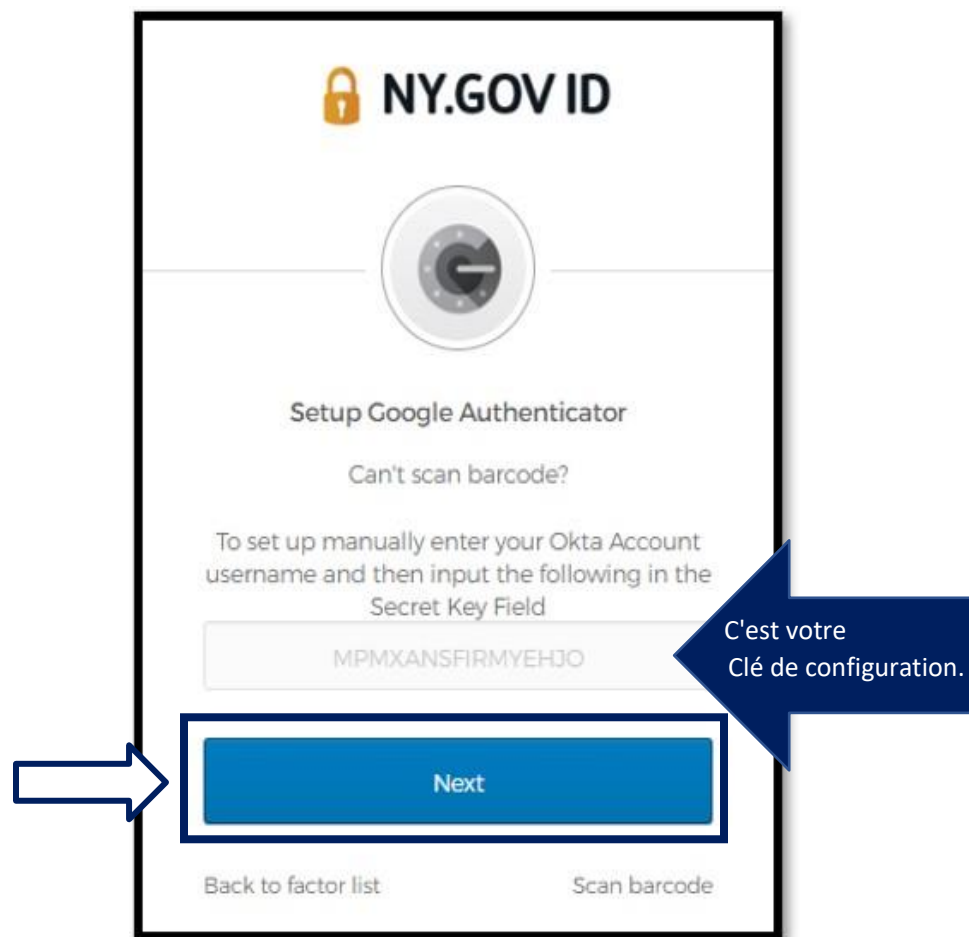
## Instructions sur la façon de saisir une clé de configuration (si vous ne pouvez pas scanner un code QR).

26. Si vous ne pouvez pas scanner le code, à l'étape 13 ci-dessus, sélectionnez **Entrer une clé de configuration.**

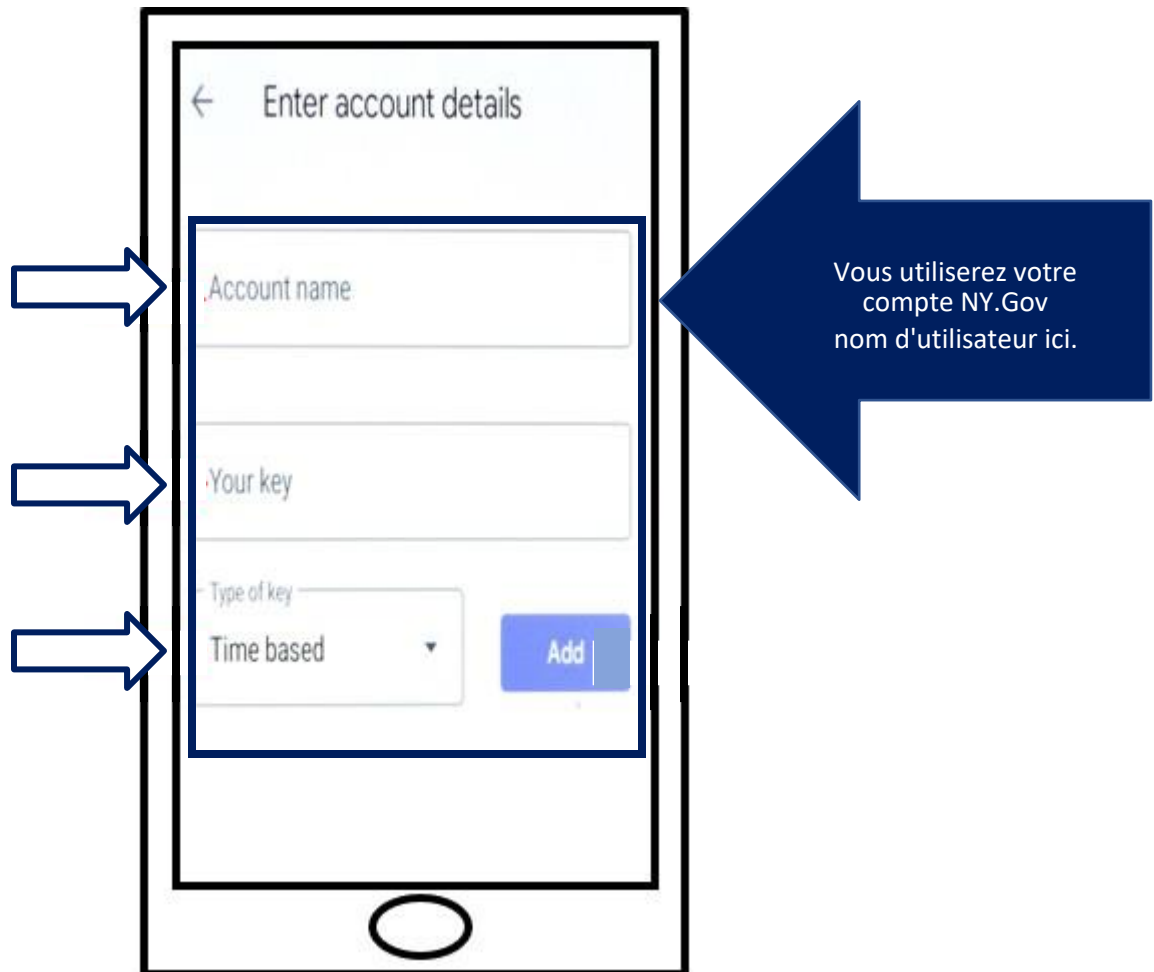
**Conseil :** [Cliquez ici pour connaître les autres raisons possibles de cette erreur et savoir comment les corriger.](#)

27. Sur l'écran de votre ordinateur, vous verrez apparaître une clé secrète. Il s'agit du code que vous allez saisir dans l'application Google Authenticator. Un écran contenant les instructions pour saisir une clé de configuration s'affiche.

REMARQUE : Pour procéder à cette étape, vous devez d'abord configurer la méthode d'authentification multifactorielle Okta Verify.



28. Sur votre application Google Authenticator, entrez votre nom de compte NY.gov, entrez votre clé secrète, sélectionnez Time based (En fonction du temps).



29. Cliquez sur le bouton **Add (Ajouter)**.

30. Procédez aux étapes [Saisir votre code](#) .



## Saisir votre code

31. Une fois que l'application a réussi à scanner le code QR, votre smartphone affiche un écran avec votre nom d'utilisateur et un code à six chiffres. Il s'agit du code que vous allez entrer dans l'ordinateur aux étapes suivantes. Ce code change toutes les 30 secondes.



32. Tapez le code de votre application dans le champ Entrer le code sur l'écran de votre ordinateur et cliquez sur **Vérier**.

NY.GOV ID

Setup Google Authenticator

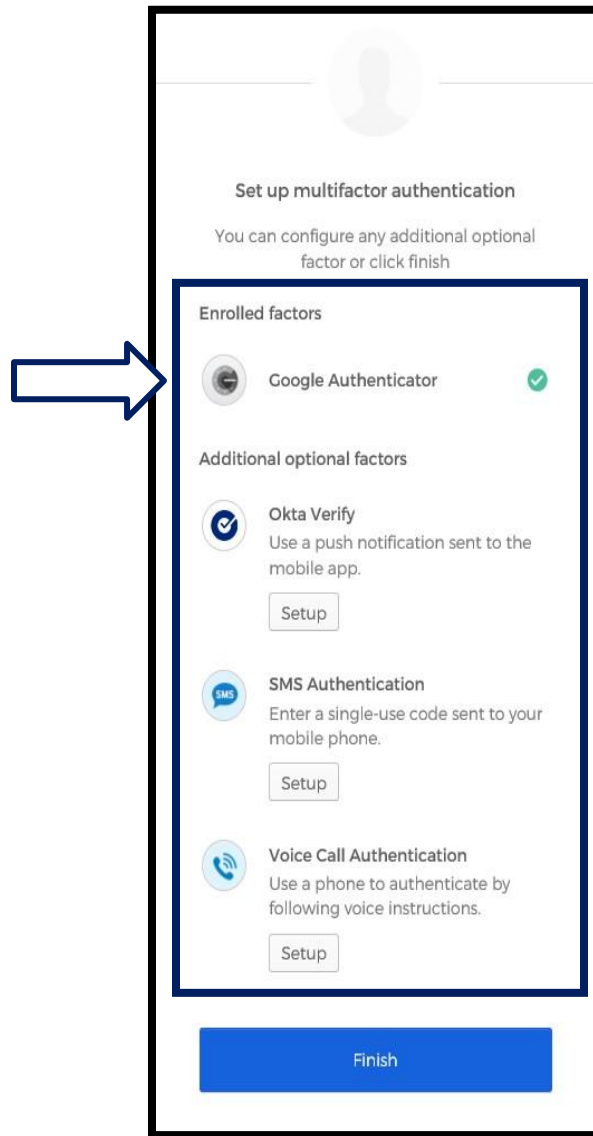
Enter code displayed from the application

Enter Code

Verify

[Back to factor list](#)

33. Vous serez redirigé vers l'écran d'inscription où vous pourrez configurer une autre méthode d'authentification multifactorielle. Remarquez que Google Authenticator figure désormais sous la rubrique des facteurs enregistrés. Il est recommandé de configurer plus d'une méthode d'authentification multifactorielle.

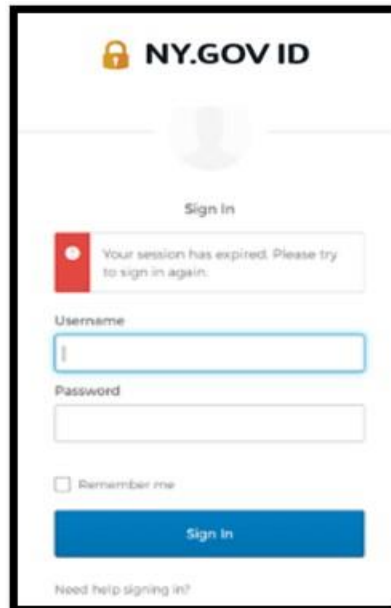


34. Lorsque vous avez configuré toutes les méthodes d'authentification multifactorielle que vous souhaitez, cliquez sur le bouton Finish (Terminer).

- Conseil : Si vous devez configurer une méthode d'authentification multifactorielle qui utilise une application téléphonique, téléchargez les applications avant de cliquer sur le bouton Setup (Configuration) de la page du navigateur « Set up multifactor authentication » (Configurer l'authentification multifacteur). Les deux méthodes d'authentification multifactorielle qui utilisent des applications sont Okta Verify et Google Authenticator.

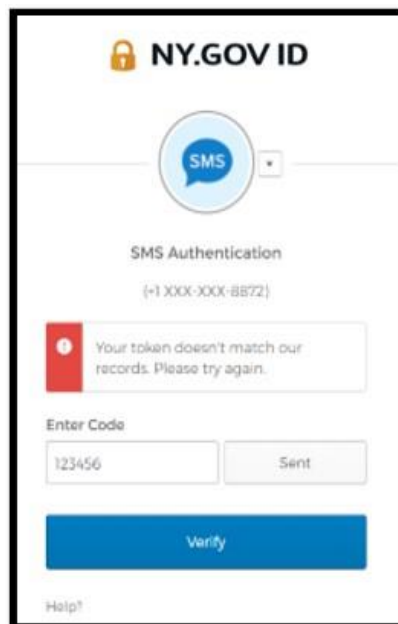
## Messages d'erreur potentiels et comment les résoudre.

- Message d'erreur : La session a expiré.
- Remède : Le client doit s'identifier à nouveau.



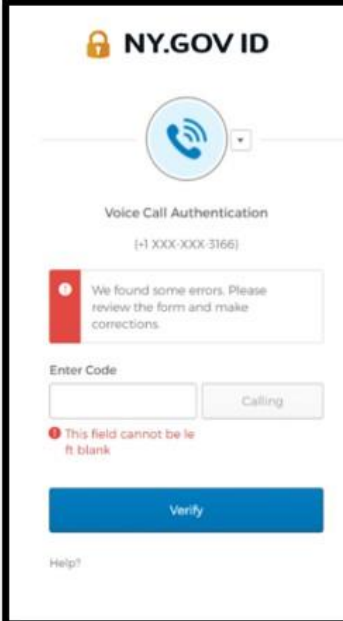
The screenshot shows the NY.GOV ID sign-in interface. At the top, there is a lock icon and the text "NY.GOV ID". Below this is a "Sign In" button. A red error message box states: "Your session has expired. Please try to sign in again." Below the error message are input fields for "Username" and "Password". There is a "Remember me" checkbox and a "Sign In" button. At the bottom, there is a link that says "Need help signing in?"

- Message d'erreur : Le jeton ne correspond pas.
- Remède :
  1. Le client doit vérifier l'exactitude.
  2. Le client doit « Envoyer » le code à nouveau.



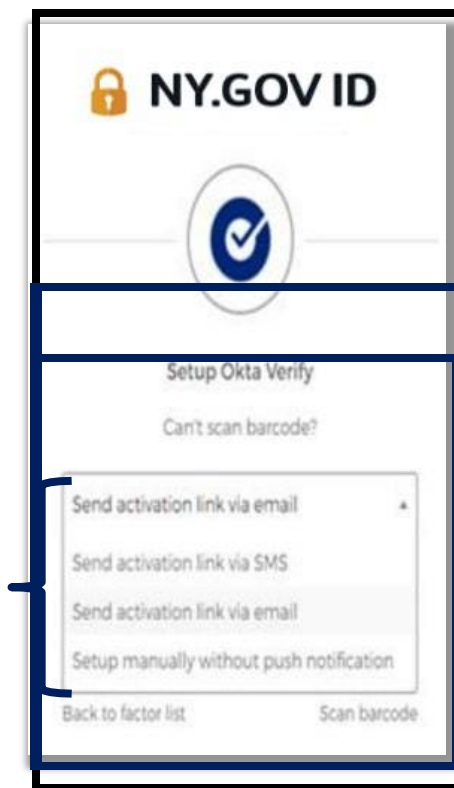
The screenshot shows the NY.GOV ID SMS Authentication interface. At the top, there is a lock icon and the text "NY.GOV ID". Below this is an "SMS" button. Below the button is the text "SMS Authentication" and a phone number placeholder "(+1 XXX-XXX-8872)". A red error message box states: "Your token doesn't match our records. Please try again." Below the error message is an "Enter Code" input field containing "123456" and a "Sent" button. Below these is a "Verify" button. At the bottom, there is a link that says "Help?"

- Message d'erreur : Erreur trouvée.
- Remède : Le client doit saisir le code.



The screenshot shows the NY.GOV ID Voice Call Authentication interface. At the top, there is a lock icon and the text "NY.GOV ID". Below this is a circular icon with a telephone handset and a checkmark. The text "Voice Call Authentication" and the phone number "(+1 XXX-XXX-3166)" are displayed. A red error message box states: "We found some errors. Please review the form and make corrections." Below the error message is a section labeled "Enter Code" with an empty input field and a "Calling" button. A red error message below the input field reads: "This field cannot be left blank". At the bottom of the form is a blue "Verify" button and a "Help?" link.

- Message d'erreur : Le code-barres ne se scanne pas.
- Remède :
  1. Essayez les méthodes alternatives indiquées.
    - « Envoyer l'activation par SMS » – le client peut saisir un numéro de téléphone.
    - « Configuration manuelle sans push » – Le client verra un code temporaire.
    - « Envoyer un e-mail d'activation » – Le client recevra un e-mail sur le compte de messagerie utilisé pour la création de son compte.



2. Assurez-vous que l'appareil du client a « autorisé » l'accès à la caméra. ([cliquez ici pour obtenir les instructions](#))

[Retour à la page principale](#)