

MISE EN CONTEXTE :

Seule, l'authentification par l'entremise de votre code d'utilisateur et mot de passe réseau n'offre pas une protection suffisante contre le cyber piratage. La configuration de la double authentification (2FA) sur votre compte réduit de 99,9% les risques de compromissions ou d'usurpation d'identité professionnelle.

Cette seconde vérification se fait à partir de votre téléphone intelligent à l'aide de l'application « **Microsoft Authenticator** ».



Il est suggéré d'effectuer cette configuration durant les heures d'ouverture de la DiSTI, soit du lundi au vendredi de 8 h à 17 h.

Légendes :



Étape à faire sur votre téléphone mobile (toutes les autres étapes se font sur votre ordinateur).



Attention, information importante!



Note, information additionnelle.



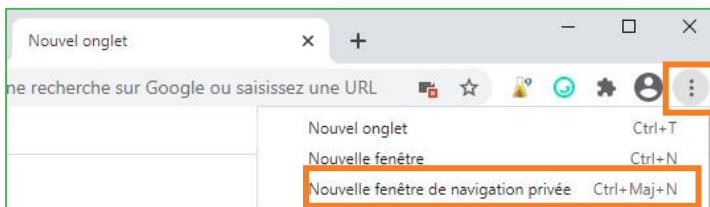
Sur votre ordinateur, affichage d'une nouvelle fenêtre contextuelle.

DÉMARCHE :

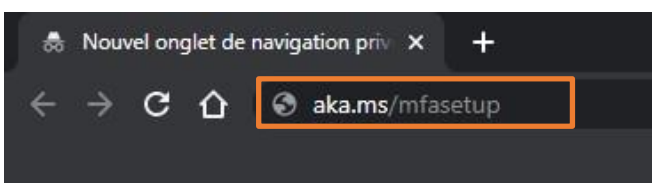
1. Sur votre ordinateur, ouvrez une fenêtre de navigation privée dans Google Chrome. Nous vous déconseillons de faire cette étape sur votre téléphone intelligent.



Pour ouvrir une fenêtre de navigation privée, allez dans Google Chrome et cliquez sur les 3 points verticaux en haut à droite du navigateur et sélectionnez **Nouvelle fenêtre de navigation privée**.



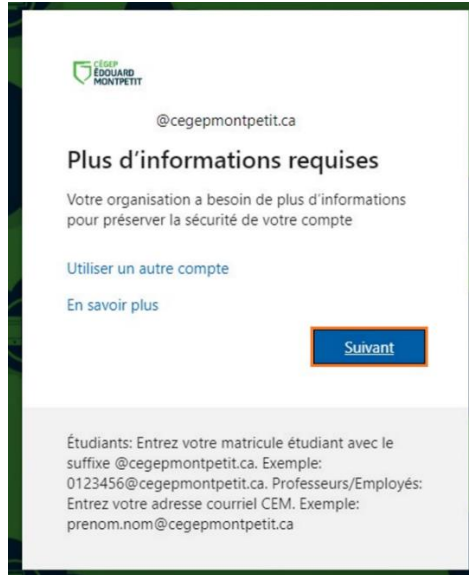
2. Insérez le lien suivant dans votre fenêtre de navigation privée : <https://aka.ms/mfasetup>



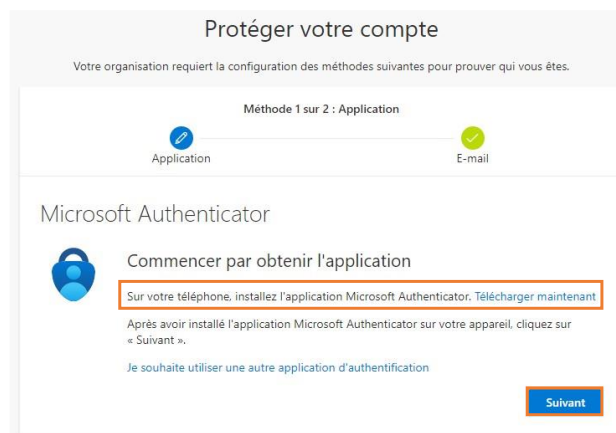
3. Entrez vos informations de connexion (1234567@cegepmontpetit.ca et mot de passe).



La fenêtre **Plus d'information requises** s'ouvrira. Cliquez sur **Suivant**



Vous êtes invités, tel qu'indiqué dans la fenêtre ci-dessous, à installer « **Microsoft Authenticator** ».

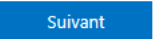


4. Sur votre téléphone, installez **l'application mobile**.

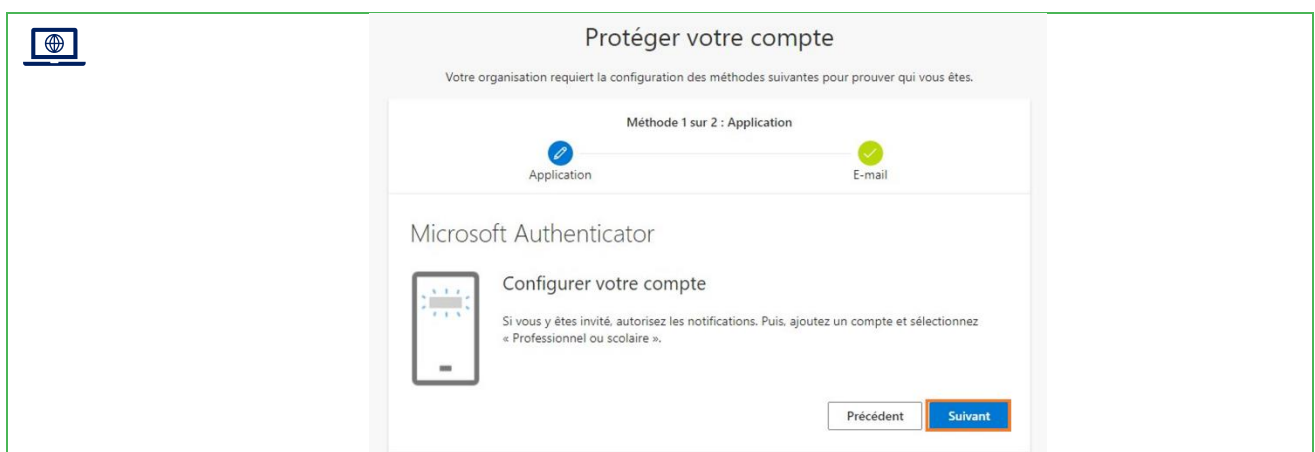


Sur votre téléphone intelligent, installez l'application « **Microsoft Authenticator** ».

Note : Si vous êtes physiquement au cégep lorsque vous effectuez cette étape, connectez-vous au réseau sans-fil **CAMPUS** plutôt que **CAMPUSPublic**.

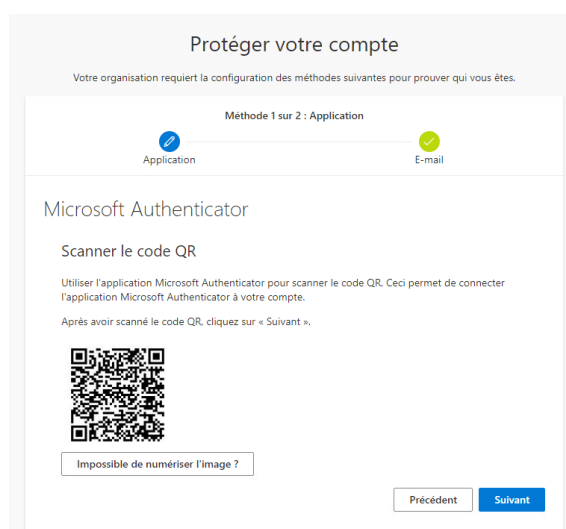
5. Après avoir installé « **Microsoft Authenticator** » sur votre téléphone, Allez sur votre ordinateur et cliquez sur  .

6. Cliquez sur **suivant** pour configurer votre compte





Lorsque cette fenêtre apparaît, passez à l'étape suivante **sans cliquer** sur un bouton

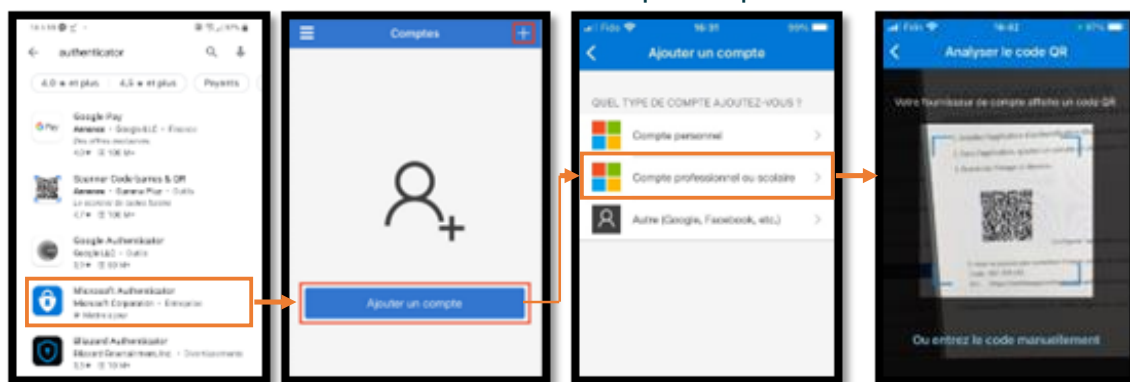


7. Sur votre téléphone, configurez l'application mobile.



Vous devez suivre les étapes pour configurer votre application « **Microsoft Authenticator** »

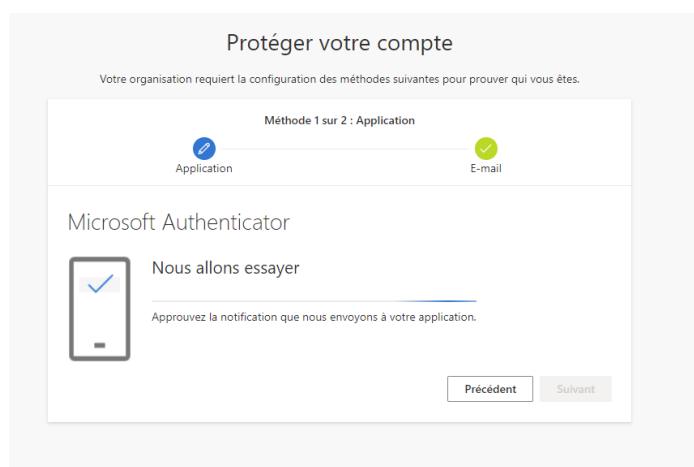
Note : Si vous êtes physiquement au cégep lorsque vous effectuez cette étape, connectez-vous au réseau sans-fil **CAMPUS** plutôt que **CAMPUSPublic**.

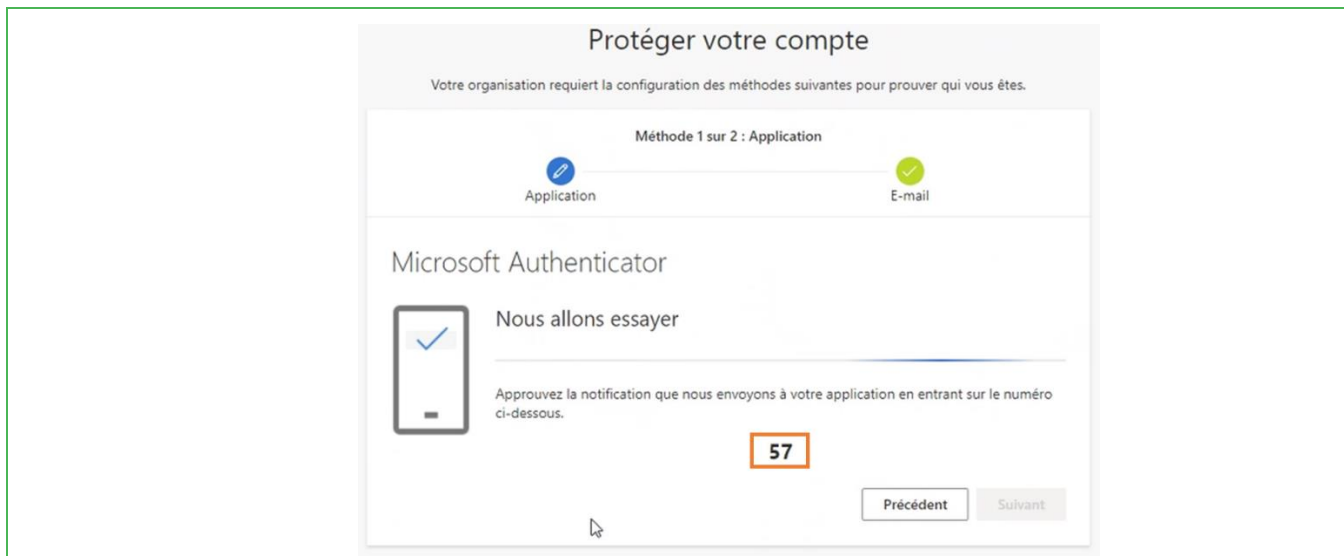


8. Dans le navigateur, cliquez sur  .

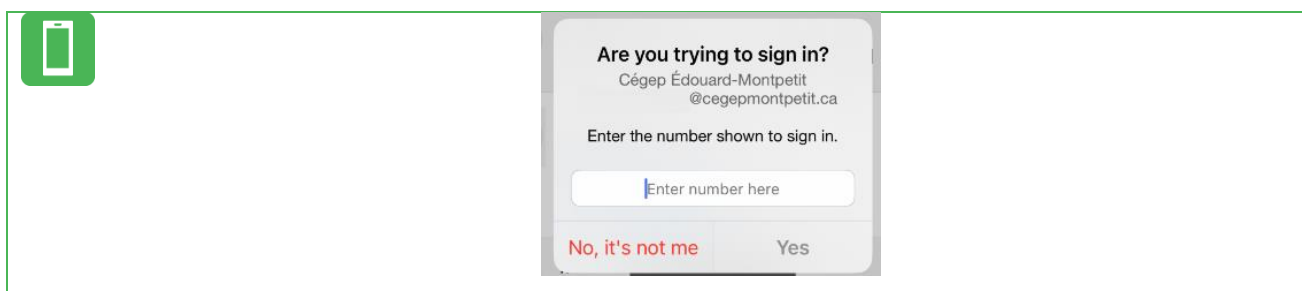


La fenêtre d'essai de la notification va s'afficher.

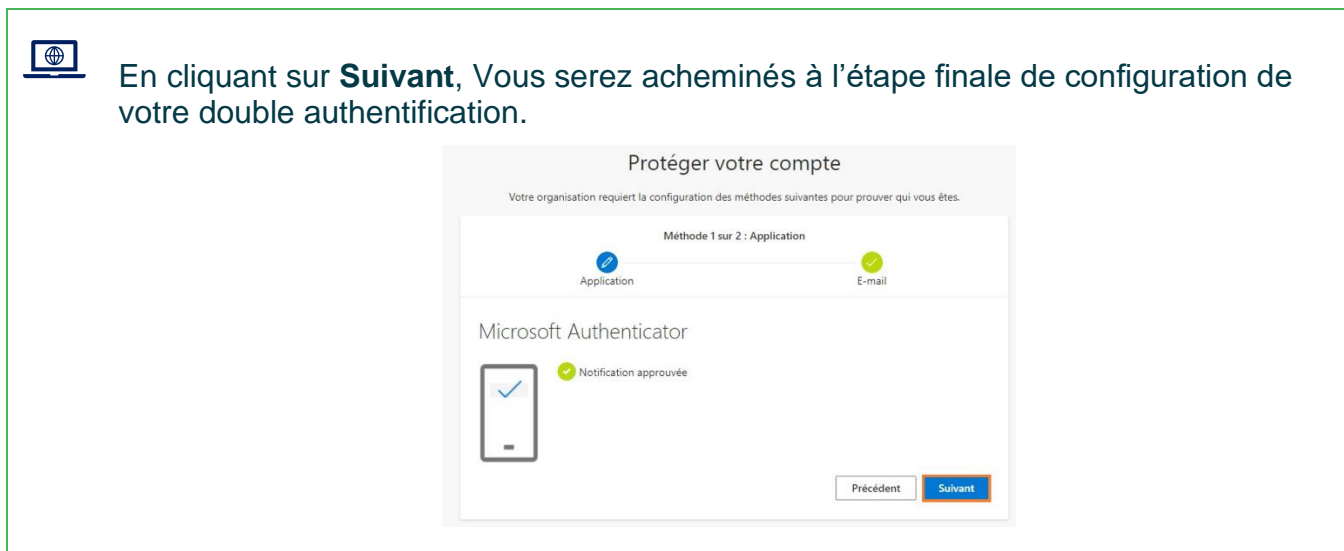




9. Vous recevrez la notification suivante sur votre téléphone intelligent que vous devrez **Approuver** en saisissant le numéro à l'écran de votre navigateur.



10. Dans le navigateur, cliquez sur  .



11. Opération réussie



12. Le système vous invite, cette fois, à valider votre code à nouveau.

 Le numéro à deux chiffres doit être saisi dans l'application sur votre téléphone.




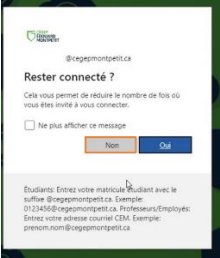
13. Approuvez la demande de connexion sur votre téléphone.

 Sur votre téléphone intelligent, saisissez, dans la zone de texte, le chiffre qui s'affiche sur votre fenêtre de navigateur.

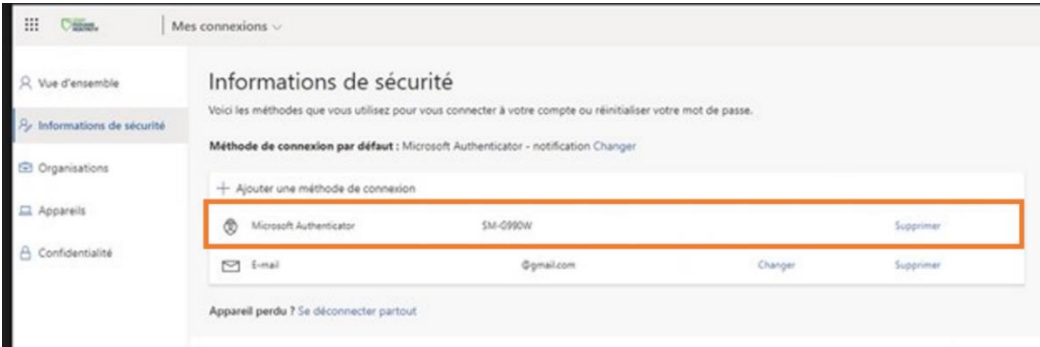



14. Cliquez sur **Non** ou **Oui** pour passer à la fenêtre des **Informations de sécurité**.

 Cliquez sur **Non**



Le nom de votre téléphone devrait apparaître ici



 Lorsque vous vous connecterez sur un système informatique, vous aurez à confirmer votre identité à l'aide de votre téléphone.
**** Important **** Il peut s'écouler jusqu'à 72 heures avant de recevoir vos prochaines demandes d'authentification.

Fin de la procédure