

Sécurisation du compte Omnivox (double facteur d'authentification)

Omnivox permet maintenant une configuration du double facteur d'authentification. Ceci permet de mieux sécuriser votre compte en demandant une information supplémentaire autre que votre mot de passe. N'oubliez pas d'ajouter l'application mobile Omnivox.

Nous vous proposons 2 méthodes pour le faire. La première méthode est disponible que pour les personnes étudiantes.

Méthode 1 : Sécurisation par l'application mobile Omnivox à partir de votre cellulaire

À la première utilisation d'Omnivox, vous aurez le message de « Validation en 2 étapes ». Si vous remettez à plus tard la configuration du double facteur d'authentification, vous pourrez aller dans services et cliquer « Validation en 2 étapes » ou dans le « Quoi de neuf ».



ou



Cliquez sur « commencer » dans la page ci-dessus.

Validation en 2 étapes

Vous devez mettre en place la validation d'identité en 2 étapes pour votre compte utilisateur.

La validation en 2 étapes consiste à fournir deux types d'informations pour confirmer votre identité. Après avoir entré votre identifiant et votre mot de passe, un code de sécurité à usage unique vous sera envoyé. Vous devrez entrer ensuite ce code pour vous connecter à votre compte.

Cette validation d'identité en 2 étapes a pour but de rendre la connexion à votre compte encore plus sécuritaire.

Remettez à plus tard

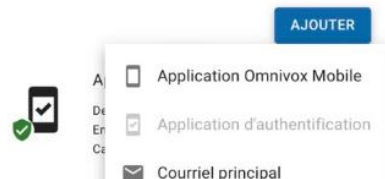
COMMENCER

Comme vous avez déjà l'application Omnivox, le système va automatiquement détecter l'installation de votre appareil dans la liste. Cliquez sur votre appareil (comme dans l'exemple ci-



cellulaire dans la liste. Cliquez sur votre appareil (comme ci-dessus) :

Note : Dans le cas où la fenêtre de gauche n'apparaît pas, il vous suffira de sélectionner « application Omnivox mobile ».



Le système enverra un code unique temporaire par une notification sur votre appareil mobile. Dans l'exemple ci-dessous, le code est 257645 (ce code sera différent à chaque utilisation). Assurez-vous que les notifications d'Omnivox soient activées. Retournez dans l'application Omnivox et entrez ce code.




Par la suite, vous pouvez ajouter un courriel pour valider votre identité et cliquer suivant. Vous allez recevoir un code dans votre **courriel**. Vous devez entrer ce code dans « code de sécurité » et faire « valider ».



Votre validation en 2 étapes est maintenant terminée. Cliquez sur « Continuer ».

Activation terminée

 Validation en 2 étapes
activée

Dès votre prochaine connexion, vous devrez confirmer votre identité à l'aide d'une des méthodes associées à votre compte.

La gestion de ces méthodes s'effectue à partir du service "Validation en 2 étapes" disponible dans le menu des services.

 CONTINUER

Lors de votre prochaine connexion à partir d'un ordinateur (ou après 30 jours où vous n'avez pas validé votre identité sur l'application mobile), le système vous demandera d'entrer un code temporaire unique. Vous recevrez une notification venant de l'application mobile d'Omnivox sur votre cellulaire. Vous devrez entrer le code à l'écran de connexion et cliquer « valider ».

Méthode #2 : Sécurisation par Microsoft Authenticator (à partir d'un ordinateur)

Avant d'utiliser cette méthode, vous devez avoir installé l'application Microsoft Authenticator. Cette application est nécessaire pour l'authentification à Microsoft Office365 du Cégep. Si ce n'est pas déjà le cas, [svp cliquez ici pour la procédure pour le faire.](#)

Connectez-vous à Omnivox par votre navigateur Internet (ex. : Microsoft Edge). Vous aurez le message suivant, veuillez cliquer « commencer ».

Validation en 2 étapes

Vous devez mettre en place la validation d'identité en 2 étapes pour votre compte utilisateur.

La validation en 2 étapes consiste à fournir deux types d'informations pour confirmer votre identité. Après avoir entré votre identifiant et votre mot de passe, un code de sécurité à usage unique vous sera envoyé. Vous devrez entrer ensuite ce code pour vous connecter à votre compte.

Cette validation d'identité en 2 étapes a pour but de rendre la connexion à votre compte encore plus sécuritaire.

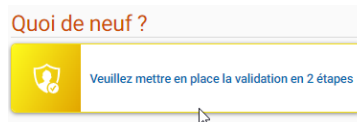
[Remettre à plus tard](#)

COMMENCER

Note : Si vous cliquez « remettre à plus tard », pour faire la configuration, vous devez cliquer « veuillez mettre en place la validation en 2 étapes » dans la section « Quoi de neuf » ou cliquer « Validation en 2 étapes » dans le profil personnel.



OU



Vous aurez la page suivante.

Ajout d'une application d'authentification

1. Si vous ne possédez d'application d'authentification sur votre appareil mobile, nous vous suggérons d'installer Microsoft Authenticator ou Google Authenticator disponibles sur le App Store ou le Google Play Store.
2. Par la suite, veuillez scanner le code QR ci-dessous avec votre application d'authentification en utilisant votre appareil mobile.
3. Une fois le compte ajouté à votre application d'authentification, appuyez sur le bouton Suivant afin de saisir un deuxième code généré par votre application et de valider le processus.

Attention: Ne pas utiliser votre application appareil (si vous)



Je ne suis pas et ne veux pas scanner ce code

[Remettre à plus tard](#)

SUIVANT

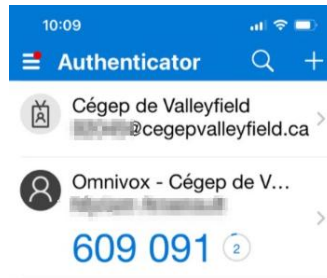
En même temps que cette page s'affiche, vous devez ouvrir votre application d'authentification.



Dans l'application, vous devez cliquer en haut à droite sur les 3 points (ou le +) et/ou cliquez sur « ajouter un compte » et choisissez « compte professionnel ou scolaire ». Sélectionnez « scanner un code QR » et pointer votre cellulaire vis-à-vis le code QR qui est à l'écran



Balayez le code QR à l'écran. Dans l'application « Microsoft Authenticator », cliquez Omnivox pour afficher le code temporaire unique.



Retournez dans Omnivox et cliquez « suivant » sur l'écran affichant le code QR. Vous aurez ensuite la fenêtre suivante. De là, entrez le code que vous avez affiché sur votre cellulaire et cliquez « valider ».



Par la suite, vous pouvez ajouter un courriel pour valider votre identité et cliquer suivant. Vous allez recevoir un code dans votre **courriel**. Vous devez entrer ce code dans « code de sécurité » et faire « valider ».

Ajout d'un courriel

La configuration d'un courriel principal comme méthode de validation d'identité est très importante afin d'activer la validation en 2 étapes pour votre compte utilisateur. Un code de sécurité sera envoyé à ce courriel afin de confirmer votre identité.

Courriel*
courriel@mail.com



Validation du courriel

Afin de confirmer le courriel à ajouter comme méthode de validation d'identité en 2 étapes, veuillez utiliser le code de sécurité ci-dessous.

Votre code de sécurité:

Code de sécurité (6 chiffres)*
000000

Demander un nouveau code

Mettre en place une autre méthode de validation d'identité

Remettre à plus tard

SUIVANT

RETOUR

VALIDER

Votre validation en 2 étapes est maintenant terminée. Cliquez sur « Continuer ».

Activation terminée



Validation en 2 étapes
activée

Dès votre prochaine connexion, vous devrez confirmer votre identité à l'aide d'une des méthodes associées à votre compte.

La gestion de ces méthodes s'effectue à partir du service "Validation en 2 étapes" disponible dans le menu des services.

CONTINUER

Lors de votre prochaine connexion, vous devrez afficher le code temporaire unique sur votre cellulaire dans l'application Microsoft Authenticator (comme précédemment). **Vous devez donc conserver l'application sur votre cellulaire.**

Vous devrez entrer le code à l'écran de connexion et cliquer « valider ». Si vous n'avez pas accès à votre cellulaire, vous pouvez cliquer « valider mon identité à l'aide d'une autre méthode » et vous pourrez choisir d'envoyer un code à votre courriel principal.

Note : Si vous utilisez un ordinateur non partagé avec d'autres utilisateurs, vous pouvez cocher « j'utilise un appareil de confiance ». Ainsi, vous ne serez pas obligé d'entrer un code unique pendant 30 jours.