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

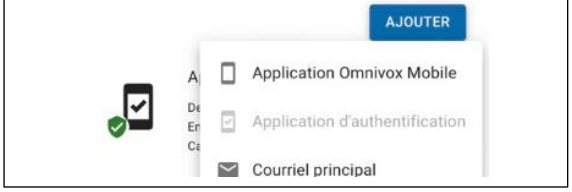
À la première utilisation d'Omnivox, vous aurez le message de « Validation en 2 étapes ». Si vous remettez à plus tard la configuration du double facteur d'authentification, vous pourrez aller dans services et cliquer « Validation en 2 étapes » ou dans le « Quoi de neuf ».

ou

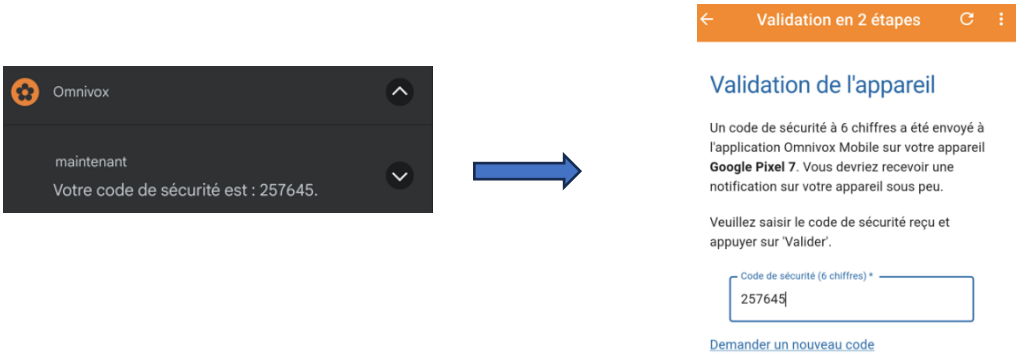
Cliquez sur « commencer » dans la page ci-dessus.

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

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

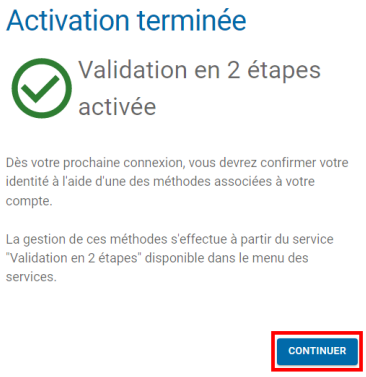


Le système enverra un code unique temporaire par une notification sur votre appareil mobile. Dans l'exemple ci-dessous, le code est 257645 (ce code sera différent à chaque utilisation). Assurez-vous que les notifications d'Omnivox soient activées. Retournez dans l'application Omnivox et entrez ce code.



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 ».

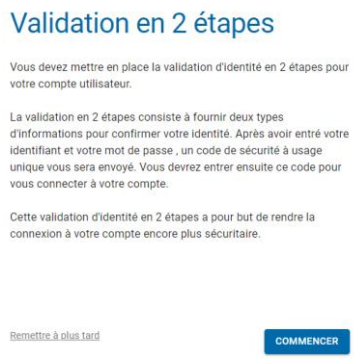


Lors de votre prochaine connexion à partir d'un ordinateur (ou après 30 jours où vous n'avez pas validé votre identité sur l'application mobile), le système vous demandera d'entrer un code temporaire unique. Vous recevrez une notification venant de l'application mobile d'Omnivox sur votre cellulaire**.**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

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

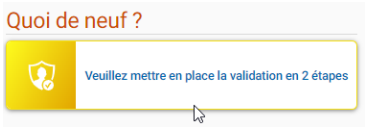
Avant d'utiliser cette méthode, vous devez avoir installé l'application Microsoft Authenticator. Cette application est nécessaire pour l'authentification à Microsoft Office365 du Cégep. Si ce n'est pas déjà le cas, [svp cliquez ici pour la procédure pour le faire.]

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



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

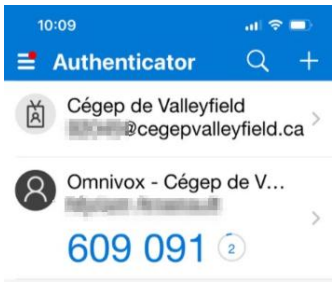


Vous aurez la page suivante.

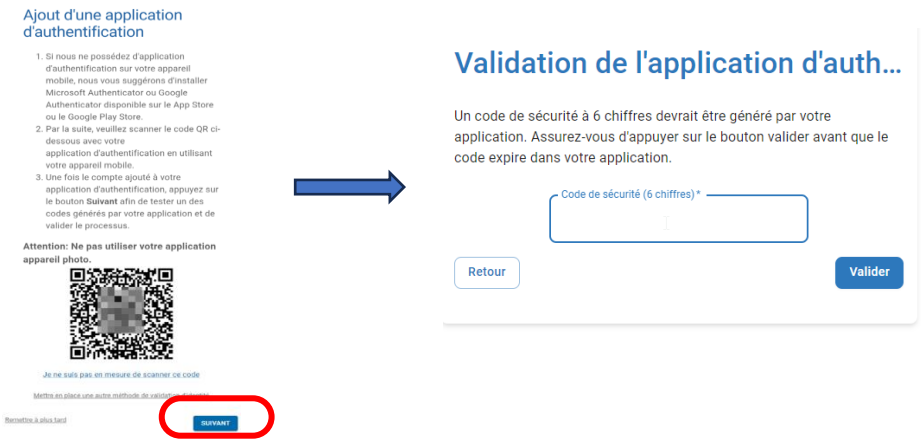
En même temps que cette page s'affiche, vous devez ouvrir votre application d'authentification.

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.

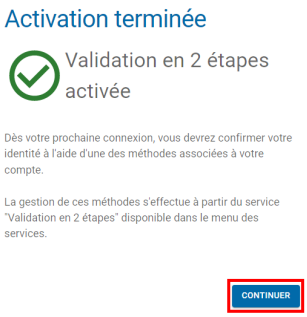


Retournez dans Omnivox et cliquez « suivant » sur l'écran affichant le code QR. Vous aurez ensuite la fenêtre suivante. De là, entrez le code que vous avez affiché sur votre cellulaire et cliquer « valider ».



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 ».

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