CÉGEP DE SAINT-HYACINTHE

Guide de l'authentification à deux facteurs (A2F/MFA)

Table des matières

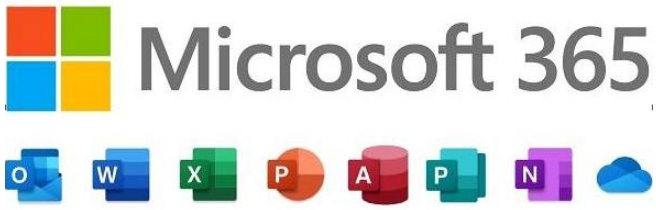
Version : 8 août 2024

CÉGEP DE SAINT-HYACINTHE

Comprendre l'authentification à deux facteurs

Le 2e facteur est une 2e information qu'un système exige occasionnellement, en plus du mot de passe, pour accéder à votre compte Microsoft 365 du Cégep. Son objectif principal est de rehausser la sécurité liée à votre compte, afin notamment de vous prémunir des dangers associés au vol de mot de passe (vol de données, d'identité, etc.).

Les systèmes qui exigeront une authentification à deux facteurs sont principalement les applications de la suite « Microsoft 365 », à savoir notamment la suite bureautique « Office » (Outlook, Word, Excel, Powerpoint, etc.), autant sur votre bureau qu'en ligne. Sont également concernées les applications de bureau et en ligne telles que OneDrive, Microsoft Teams, etc. Les versions mobiles (iOS, Android) sont également concernées.



L'authentification à deux facteurs ne s'applique pas aux systèmes et services suivants:

- L'ouverture d'une session sur votre ordinateur (*par contre, si Teams et/ou OneDrive démarrent automatiquement, le 2e facteur pourrait vous être demandé immédiatement à la suite de l'ouverture de votre session*);
- L'ouverture d'une session sur le Portail Omnivox;
- Le démarrage d'applications qui n'appartiennent pas à l'écosystème Microsoft 365 ou qui n'utilisent pas les services d'authentification de Microsoft (exemple: Clara, Impero, Zoom, etc.)

Également, il faut comprendre que le deuxième facteur n'est pas exigé à chaque connexion, mais bien dans certaines conditions précises :

Scénario	Deuxième facteur exigé
Ordinateur du Cégep, connecté au réseau du Cégep ou connecté par VPN	Très rarement*
Appareil personnel, connecté au réseau du Cégep	Rarement
Appareil personnel, connecté de la maison	Occasionnellement**
Nouvel appareil personnel, première connexion de la maison	Toujours
Changement de mot de passe, hors du réseau du Cégep	Toujours
Délai d'inactivité de 90 jours sur l'appareil	Toujours
Connexion à partir d'un lieu inhabituel (ex : autre pays) ou facteurs de risques élevés (ex : comportement inhabituel)	Variable, selon les algorithmes du fournisseur et nos réglages

**Habituellement exigé une seule fois, lors de l'inscription à l'A2F*
***Selon que vous vous déconnectiez ou non de vos applications, notamment.*

CÉGEP DE SAINT-HYACINTHE

Choisir d'utiliser un appareil mobile ou non

Il vous faut d'abord déterminer si vous comptez utiliser un appareil mobile (personnel ou appartenant au Cégep : téléphone portable, tablette, ou tout autre dispositif Android ou Apple iOS). Si la réponse est non, vous devrez choisir entre l'option 2 et 3. Il convient de ne choisir qu'une seule option.

✓ **OPTION 1 – APPAREIL MOBILE (MEILLEURE OPTION – la plus conviviale, sécuritaire, etc.)**
Si vous possédez un téléphone mobile et que vous consentez à l'utiliser comme deuxième facteur, voici les choix qui s'offrent à vous (il est recommandé d'en sélectionner au moins deux):

- Utiliser l'application d'authentification « Microsoft Authenticator » sur son appareil mobile (**méthode recommandée, la plus sécuritaire et ne nécessitant pas de connexion Internet, sauf pour l'installation**).

Microsoft Authenticator

- Utiliser un téléphone portable pour recevoir un code par texto (SMS) ou un appel téléphonique automatisé.
- Utiliser son téléphone de bureau avec son extension pour recevoir un appel téléphonique automatisé.

✓ **OPTION 2 – JETON LOGICIEL (KEEPASSXC)**
Si vous ne possédez pas d'appareil mobile, ou que vous ne souhaitez pas l'utiliser pour ces fins, vous pouvez installer un logiciel sur votre ordinateur personnel, qui prendra le rôle de jeton (la procédure pour ce faire est ici). Gratuit, disponible en français, il peut être installé autant sur Windows, que Mac et Linux et vous fournira un code qui changera aux 30 secondes.

✓ **OPTION 3 – JETON PHYSIQUE (OPTION OFFERTE AUX EMPLOYÉS SEULEMENT; n'est pas offerte aux retraités, entraîneurs sportifs et étudiants)**
Si vous ne possédez pas d'appareil mobile, ou que vous ne souhaitez pas l'utiliser pour ces fins, vous devrez vous procurer un « jeton physique » au CAT (la procédure pour ce faire est ici).

Il mesure 2.5 pouces, il peut s'attacher à votre porte-clés et fonctionne à batterie. Il vous fournira un code qui changera aux 30 secondes et il ressemble à ceci:

CĒGEP DE SAINT-HYACINTHE

Inscription à l'authentification à deux facteurs en libre-service

Notes : cette procédure ne concerne que les utilisateurs qui souhaitent configurer un appareil mobile. Pour les employés qui souhaitent obtenir un jeton physique, il faut se référer à cette section. Si vous avez déjà effectué la configuration initiale de vos facteurs de double authentification et que vous souhaitez les modifier, référez-vous plutôt à cette section.

ATTENTION!

- ✓ **Il est fortement recommandé d'utiliser l'application « Microsoft Authenticator », notamment parce qu'elle est la plus conviviale, la plus sécuritaire et peut être utilisée sans connexion Internet une fois installée.**
- ✓ **Il est important de configurer au moins deux facteurs pour pouvoir se dépanner en libre-service. Le premier facteur dont vous effectuerez la configuration deviendra votre facteur principal. Si vous en configurez un second, vous pourrez possiblement y recourir si votre facteur principal fait défaut, ce qui vous évitera de devoir contacter le soutien technique. Nous recommandons l'utilisation de l'application « Microsoft Authenticator » comme moyen principal, puis le numéro de téléphone mobile comme moyen secondaire.**

Voici les deuxièmes facteurs qui sont proposés avec un appareil mobile (typiquement : cellulaire) :

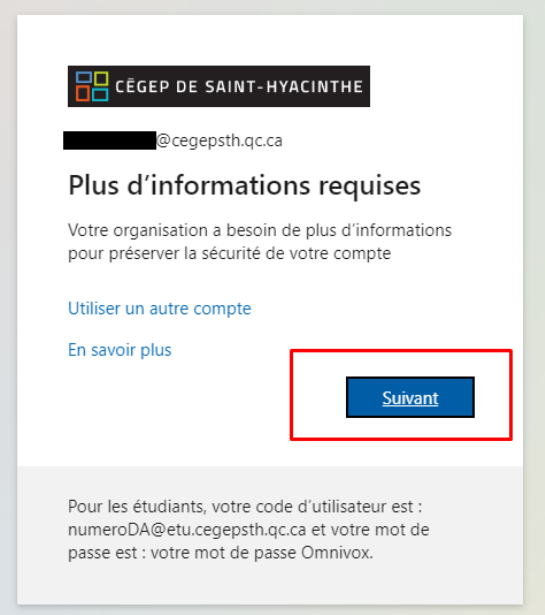
Pour configurer **l'application avec « Microsoft Authenticator » (option recommandée)**, la procédure est ici.

Pour configurer un **numéro de téléphone mobile (excluant le téléphone fixe du bureau)**, la procédure est ici.

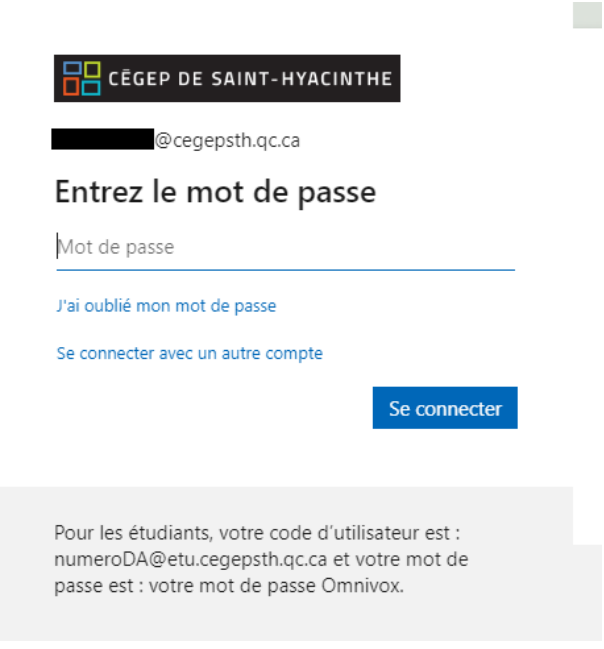
Pour configurer le **téléphone fixe du bureau (avec extension)**, notez qu'il est fortement déconseillé de l'utiliser comme deuxième facteur principal puisque ce moyen deviendra inutile si vous devez travailler ou accéder à vos courriels de l'externe. La procédure est ici.

Application « Microsoft Authenticator »

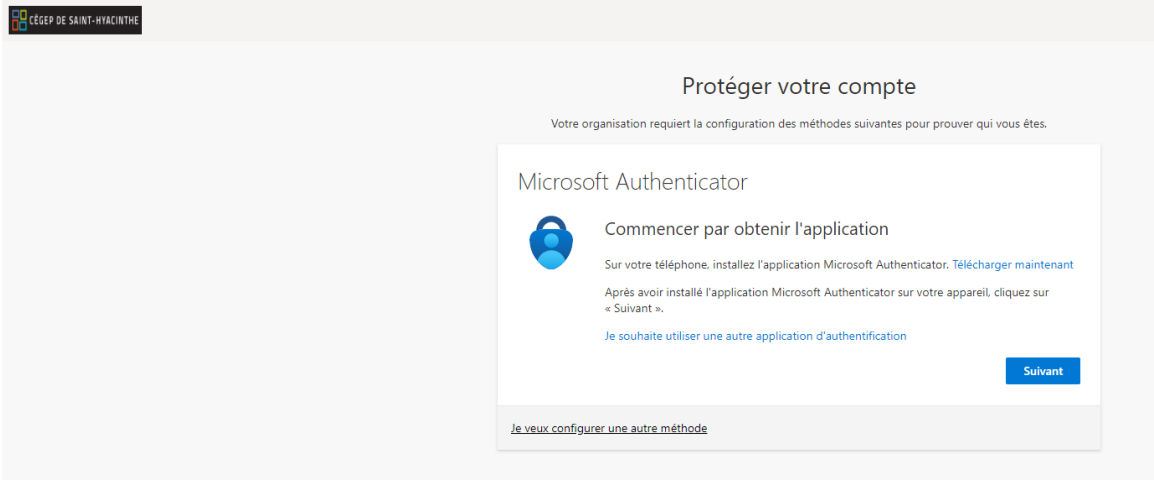
1. Démarrez un navigateur (Chrome, Edge, etc.) et connectez-vous à https://aka.ms/mfasetup. Vous pourriez voir cet écran suivant. Si c'est le cas, vous pouvez cliquer sur « Suivant » (sinon vous pouvez passer à la prochaine étape) :



2. Vous pouvez ensuite entrer votre mot de passe :



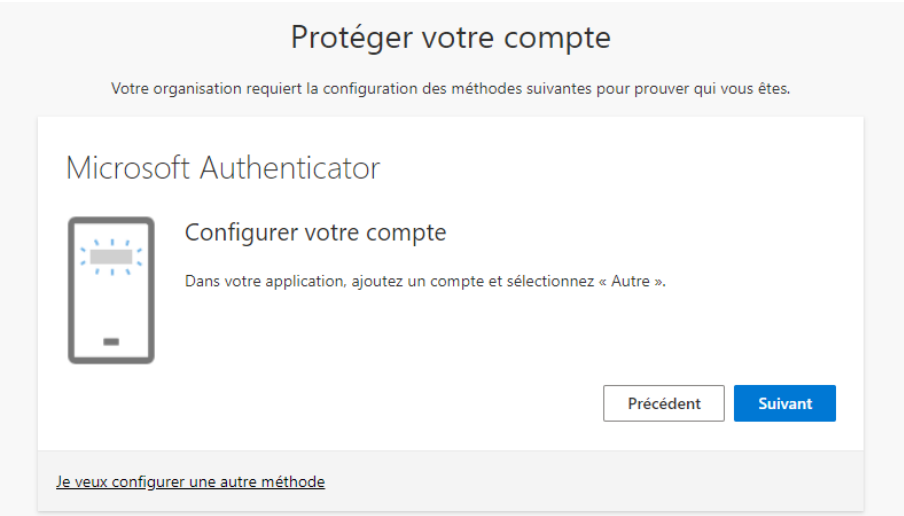
3. Vous devriez ensuite voir cet écran (Attention! Vous verrez un autre écran si vous avez déjà configuré votre numéro de téléphone : référez-vous à cette section si c'est le cas):



4. Téléchargez et installez l'application Microsoft Authenticator sur votre téléphone intelligent Android ou iOS.

5. Sur l'ordinateur, cliquer sur « Suivant ».

6. La fenêtre suivante s'affichera. Vous pouvez à nouveau cliquer sur « Suivant » :



7. La fenêtre suivante montrera un code QR (semblable à un code-barres). Ouvrez sur votre appareil mobile (téléphone ou tablette) l'application « *Microsoft Authenticator* ». *Si un code (ou empreinte digitale ou autre) vous est demandé pour l'ouverture d'Authenticator, il s'agit simplement du code de verrouillage de votre téléphone, qui est habituellement un code de type « PIN » à 4 ou 6 chiffres!*

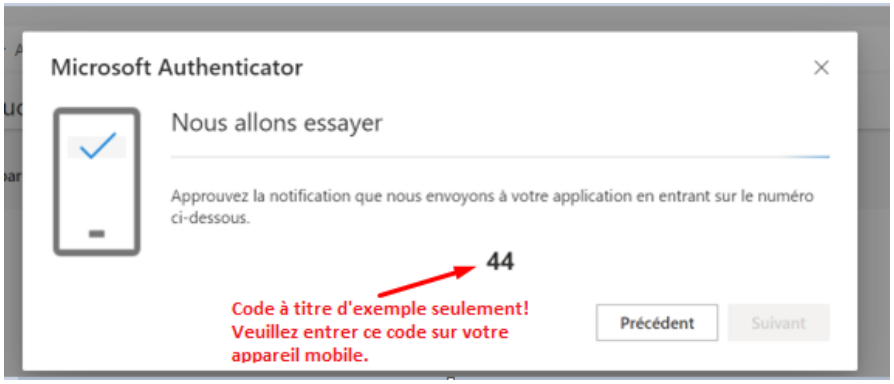
8. Appuyez sur le bouton qui permet l'ajout d'un compte (il s'agit du caractère « + » en haut à droite) et sélectionnez « Compte professionnel ou scolaire », puis « Scanner un code QR ».

9. L'application va vous demander une autorisation pour utiliser la caméra. Vous pouvez y consentir de façon permanente ou pour cette fois seulement, si l'option vous est offerte. Cette permission n'est requise que pour analyser le code QR.

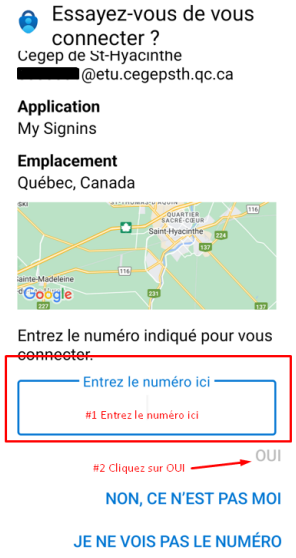
10. Placez votre téléphone intelligent devant le code QR qui s'affiche à votre écran et numérisez-le. Votre compte Cégep de Saint-Hyacinthe s'ajoutera dans l'application mobile et il vous sera indiqué que l'opération a réussi. Si vous n'y arrivez pas, réessayez. Si vos tentatives sont infructueuses, vous pouvez appuyer sur « Impossible de numériser l'image » à l'écran de l'ordinateur. Des instructions vous seront données pour utiliser un code chiffré, lequel permet également l'enregistrement de votre compte sur votre appareil mobile.

11. Sur votre ordinateur, cliquez sur le bouton « Suivant ».

12. Vous verrez un écran comme celui-ci à l'ordinateur, où un code à 2 chiffres sera indiqué (*il est important de ne pas trop attendre de passer à la prochaine étape, puisque le délai de validité du code est court)* :

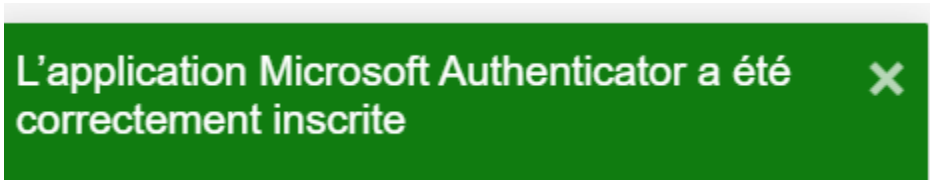


13. Simultanément, sur votre appareil mobile, une notification apparaîtra à l'écran, où vous pourrez entrer le code en question, pour ensuite appuyer sur « OUI »:

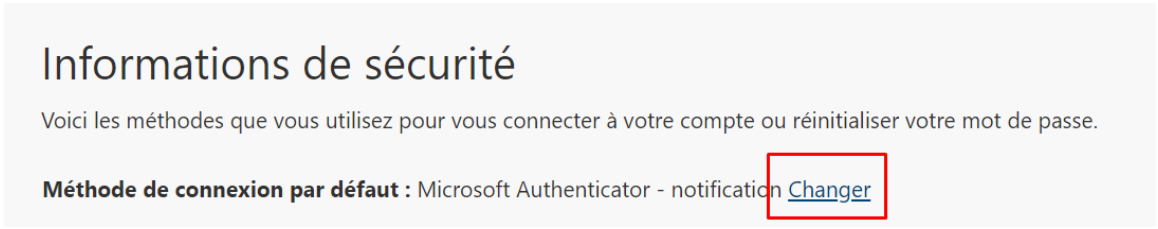


14. Vous verrez ensuite cet écran à votre ordinateur où vous devez cliquer sur « Suivant » :

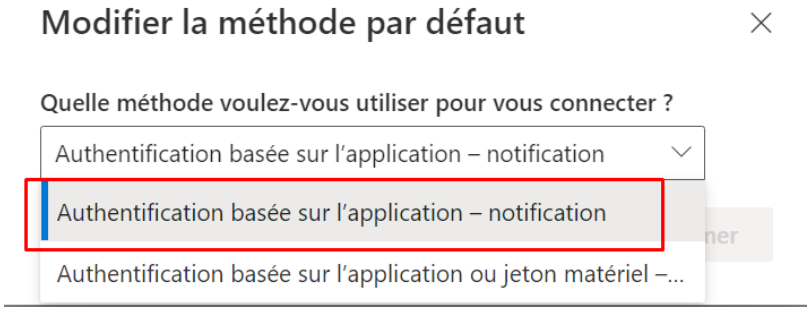
15. Si l'opération ne fonctionne pas, il faut recommencer du début, quitte à effacer le nouveau lien créé avec l'appareil en se connectant au https://mysignins.microsoft.com/security-info. Sinon, vous verrez alors cette notification à l'écran de l'ordinateur (*il se peut que vous soyez rapidement déconnecté et reconnecté par la suite, et qu'un autre écran indique le processus a été complété avec succès – c'est normal!)*:



16. Pour terminer, il faut ensuite s'assurer que la « Méthode de connexion par défaut **»** soit bien telle qu'elle est montrée ci-dessous (« Microsoft Authenticator – notification », sans quoi il faut la modifier en cliquant sur « Changer » (toujours à l'écran offert ici : https://mysignins.microsoft.com/security-info):



17. Cliquez ensuite sur la liste déroulante qui apparaît à l'écran, puis sélectionnez « Authentification basée sur l'application – notification », puis cliquez sur « Confirmer »:



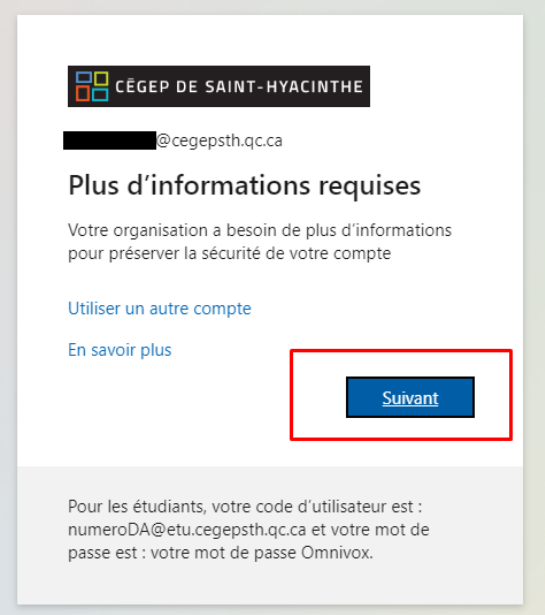
18. Voilà, vous obtiendrez désormais des notifications sur votre appareil mobile lors de connexion avec votre compte requérant votre deuxième facteur! Vous pourrez désormais constater d'où provient la connexion géographiquement approximative, en plus de constater l'identité de l'application qui est à l'origine de la connexion (*à noter que le résultat n'est pas toujours parfait)*.

    Si toutefois une connexion n'a pas été initiée à votre initiative et qu'ainsi vous n'avez pas accès au code à deux chiffres demandé par votre appareil mobile, **cela peut signifier que quelqu'un d'autre connaît le mot de passe de votre compte « cégep ».** Il faut alors

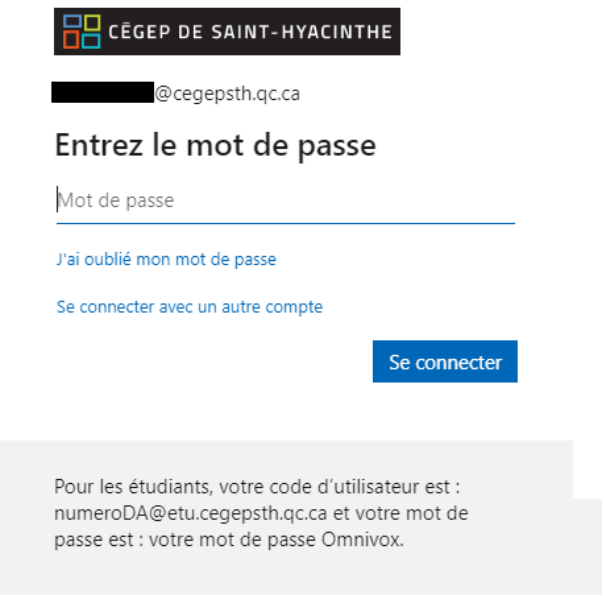
répondre « NON CE N'EST PAS MOI » à l'écran de votre appareil mobile, puis appuyer ensuite sur l'option pour le signaler aux administrateurs. Vous serez éventuellement contacté par le CAT, mais dans l'intervalle **il est très important de rapidement changer le mot de passe de votre compte « cégep », à l'ordinateur**.

Téléphone (excluant le téléphone fixe du bureau)

1. Démarrez un navigateur (Chrome, Edge, etc.) et connectez-vous à https://aka.ms/mfasetup. Vous devriez voir cet écran suivant. Si c'est le cas, vous pouvez cliquer sur « Suivant » (sinon vous pouvez passer à la prochaine étape) :

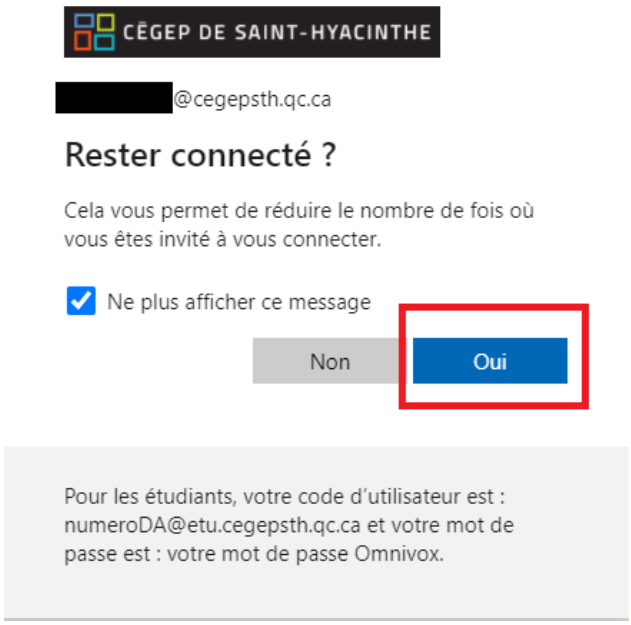


2. Vous pouvez ensuite entrer votre mot de passe :



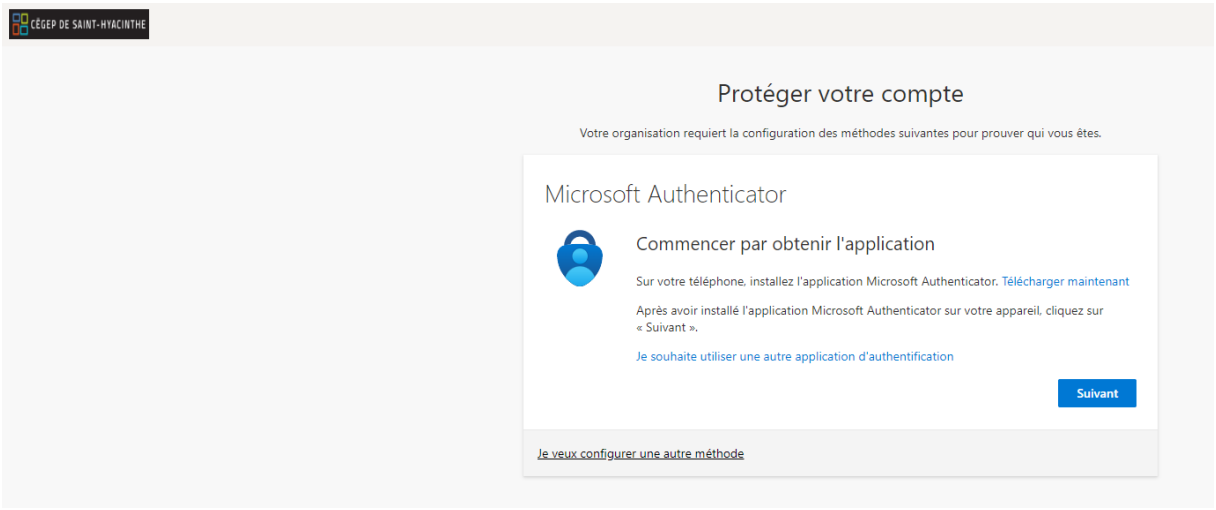
3. Il est probable que l'écran suivant vous soit proposé, pour lequel nous vous recommandons fortement de cliquer sur « Oui », en plus de cocher l'option « Ne plus afficher ce message » **si et seulement si vous êtes sur un appareil de confiance**

(exemple : votre portable du Cégep) :

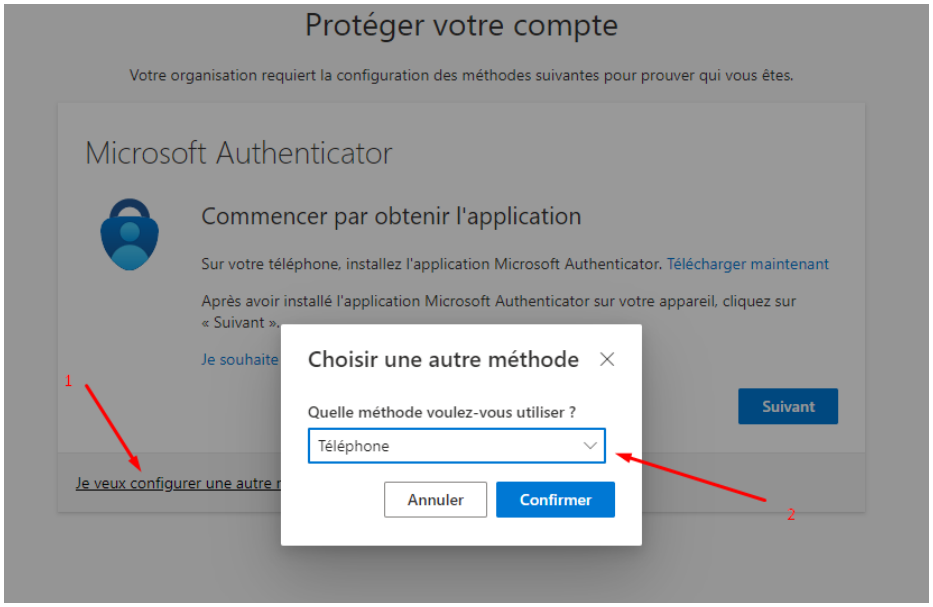


Il ne faut surtout pas cliquer sur « Oui » si l'appareil est public, tel un ordinateur à la bibliothèque! Il est important de comprendre qu'il pourrait être très facile de s'approprier votre compte si vous quittez le poste sans fermer votre session d'ordinateur!

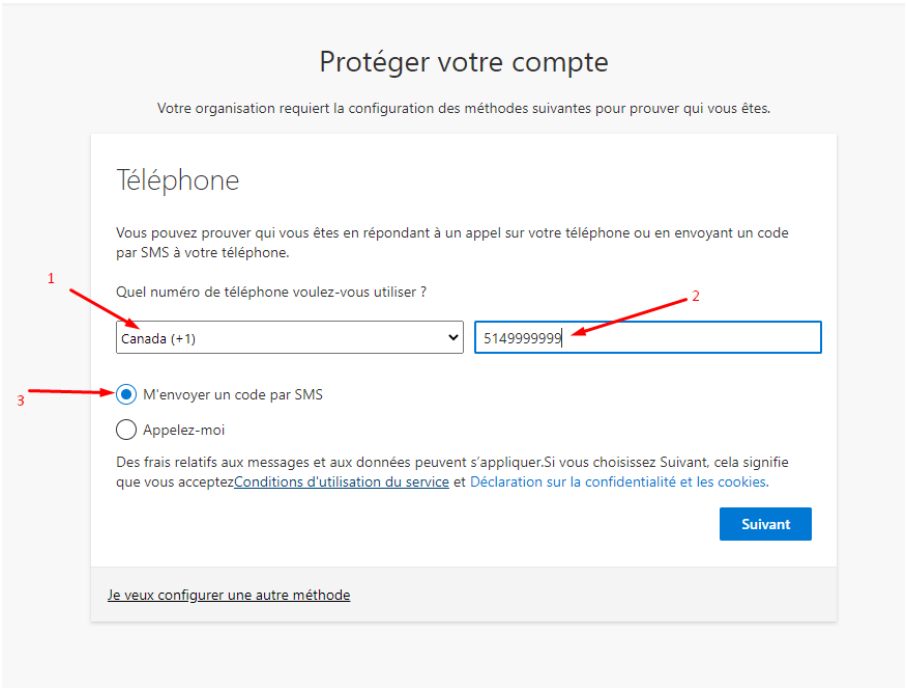
4. Vous verrez ensuite cet écran :



5. Cliquez sur « Je veux configurer une autre méthode » (1), puis sélectionnez « Téléphone » (2). Cliquez ensuite sur « Confirmer »:

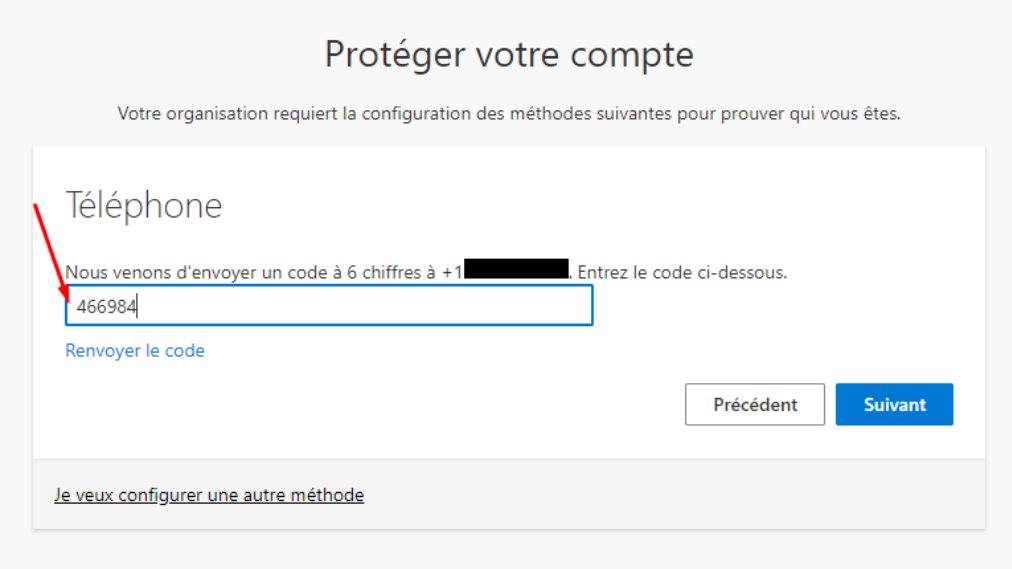


6. Sélectionnez comme pays l'option du « Canada (+1) » (1), puis entrez votre numéro de téléphone sans tiret comme montré ci-dessous (2). S'il s'agit d'un téléphone mobile, nous vous recommandons de sélectionner l'option « M'envoyer un code par SMS » (3). Si toutefois il s'agit d'un numéro provenant d'une ligne fixe, vous devrez sélectionner l'option « Appelez-moi » (4). Lorsque vous avez entré toutes ces informations, vous pouvez cliquer sur « Suivant ».



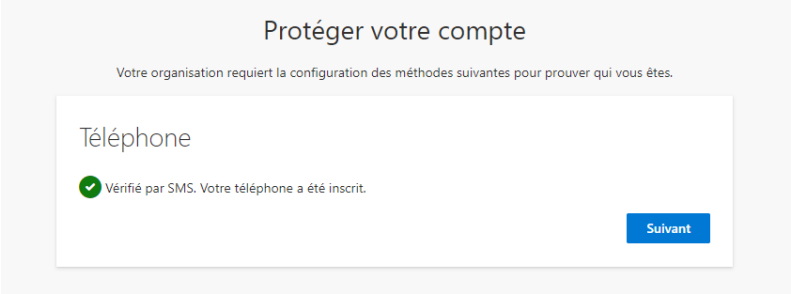
7. Si vous avez sélectionné **l'appel téléphonique** à l'étape précédente, il vous sera demandé lors de l'appel d'appuyer sur # (dièse). Vous pourrez de cette manière prouver qu'il s'agit bien de vous et raccrocher quand on vous indiquera de le faire. Vous pourrez alors cliquer sur « Suivant » à votre écran d'ordinateur, puis sur « Terminer », ce qui conclura votre inscription à ce facteur.

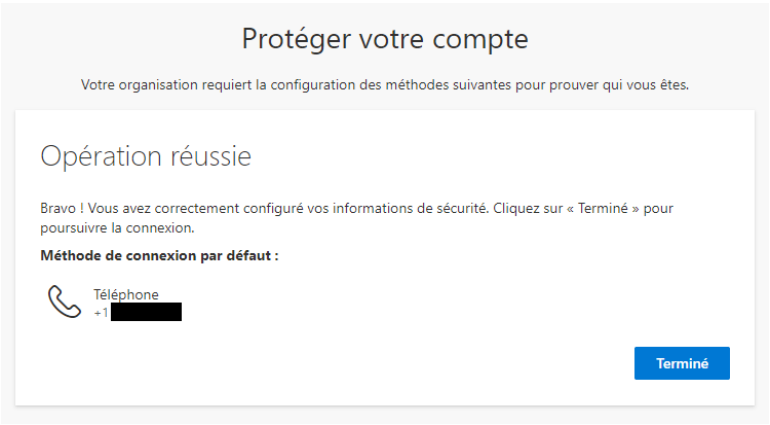
   Si vous avez sélectionné **le code par SMS (texto)**, il vous sera demandé d'entrer le code que vous avez reçu sur votre téléphone mobile à l'écran, comme suit (il faut faire relativement vite, le code unique n'étant valide que quelques minutes, sans quoi il sera indiqué de refaire l'envoi d'un autre code):



   Vous pouvez ensuite cliquer sur « Suivant ».

8. Vous verrez alors ces 2 écrans, ou vous pourrez cliquer sur « Suivant » et « Terminé ». Vous pouvez aussi fermer la page qui suit, puisque votre enregistrement aura été complété avec succès. À noter qu'à chaque connexion où le second facteur vous sera demandé, il vous sera possible de choisir de recevoir un texto ou un appel téléphonique.

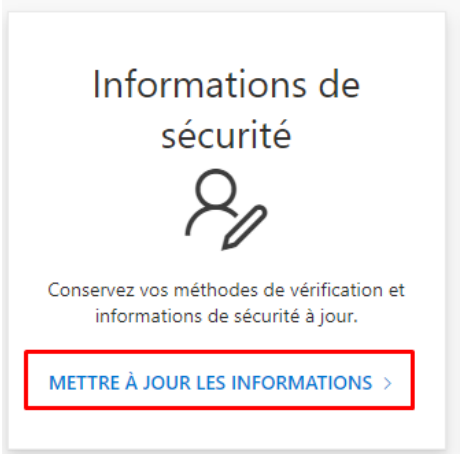


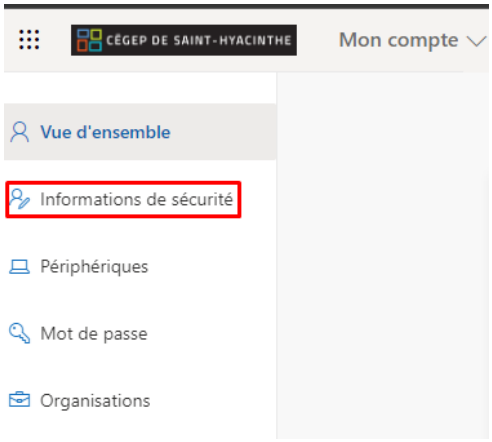

Protéger votre compte
Votre organisation requiert la configuration des méthodes suivantes pour prouver qui vous êtes.
Opération réussie
Bravo ! Vous avez correctement configuré vos informations de sécurité. Cliquez sur « Terminé » pour poursuivre la connexion.
Méthode de connexion par défaut :
Téléphone
+1 [redacted]
Terminé

Téléphone fixe du bureau (avec extension)

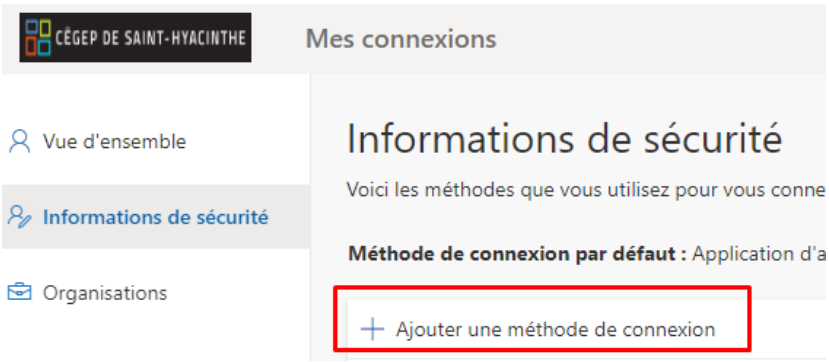
1. Démarrez un navigateur (Chrome, Edge, etc.) et connectez-vous à https://myaccount.microsoft.com

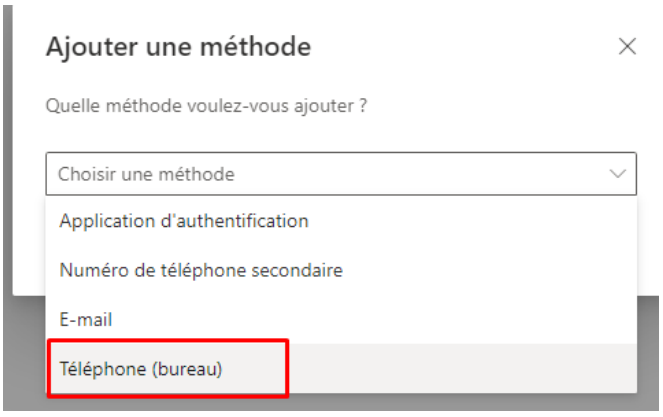
2. Cliquez sur « Mettre à jour les informations » ou sur « Informations de sécurité » dans la colonne de gauche :

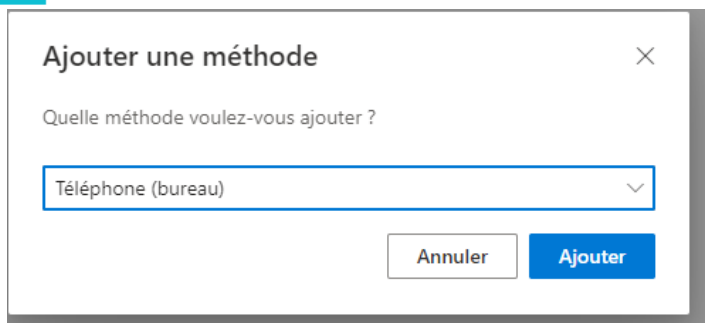




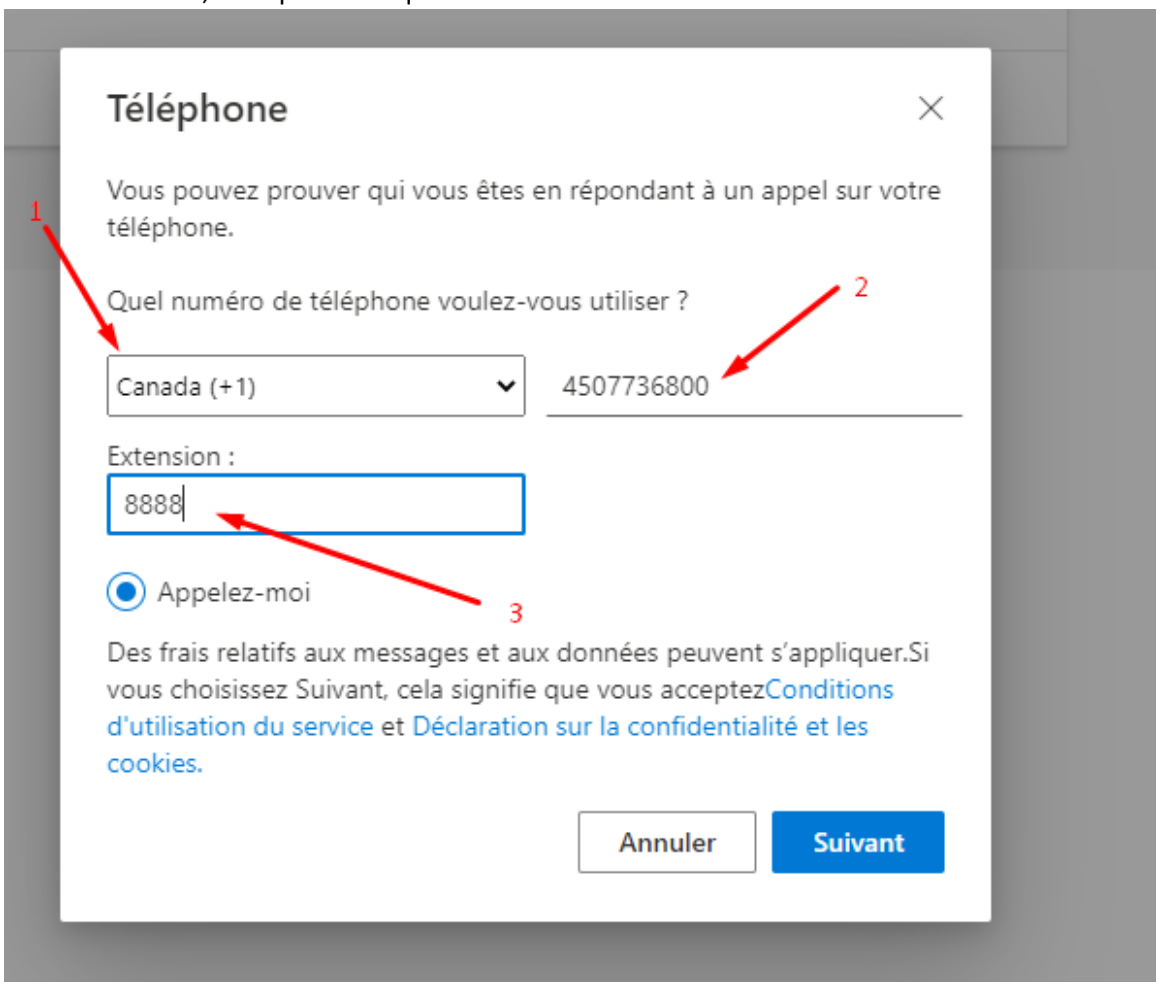
3. Cliquez sur « Ajouter une méthode de connexion », puis sélectionnez « Téléphone (bureau) », puis cliquez sur « Ajouter » :







4. Sélectionnez comme pays l'option du « Canada (+1) » (1), puis entrez le numéro de téléphone du Cégep comme montré ci-dessous (2). Tapez ensuite votre extension téléphonique de 4 chiffres dans la case « Extension » (3). Lorsque vous avez entré toutes ces informations, vous pouvez cliquer sur « Suivant ».



5. Votre téléphone sonnera peu de temps après. Lors de l'appel, il vous sera d'appuyer sur # (dièse). Vous pourrez de cette manière prouver qu'il s'agit bien de vous et raccrocher quand on vous indiquera de le faire. Vous pourrez alors cliquer sur « Suivant » à votre écran d'ordinateur, puis sur « Terminer », ce qui conclura votre inscription à ce facteur.

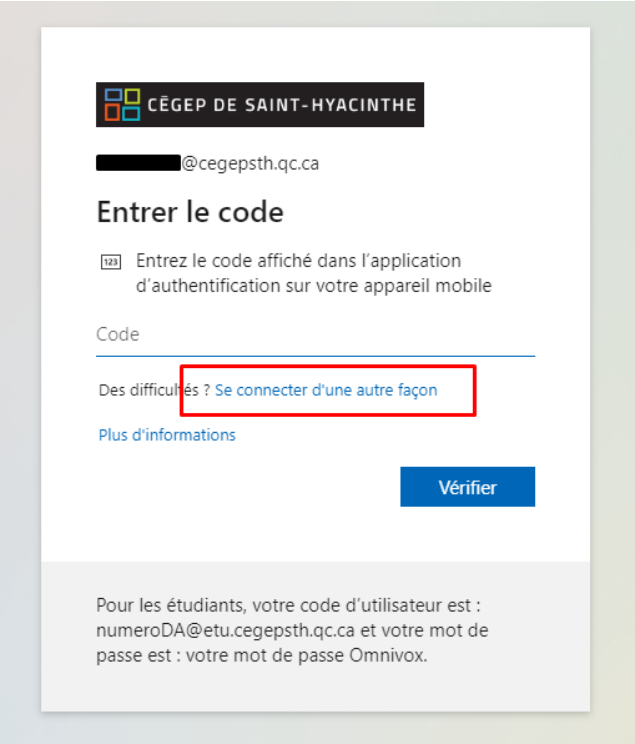
CĒGEP DE SAINT-HYACINTHE

Comment modifier ses informations d'authentification à deux facteurs

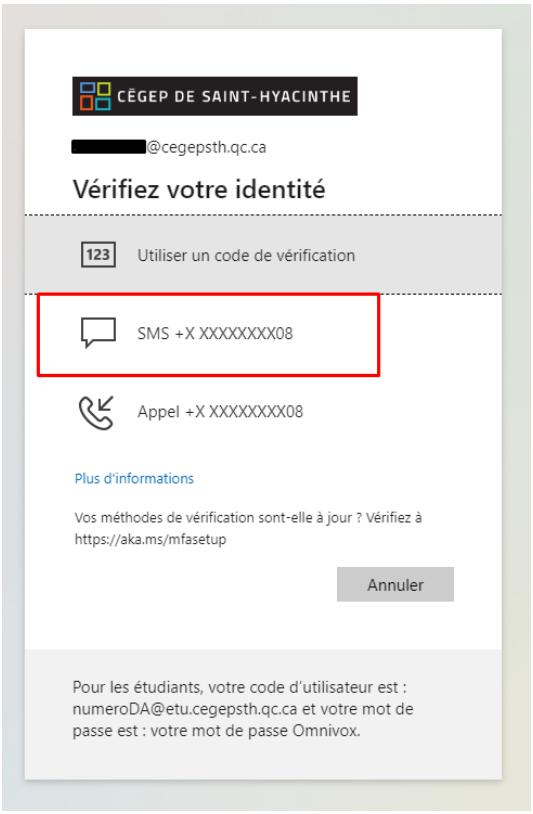
Note importante : si vous décidez de renoncer à votre jeton physique, il est très important de le rapporter au CAT (local B-2230)! Seul le CAT peut modifier les paramètres relatifs au jeton.

19. Démarrez un navigateur (Chrome, Edge, etc.) et connectez-vous à https://myaccount.microsoft.com

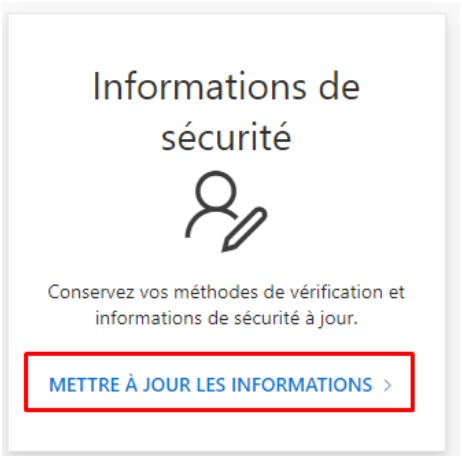
20. (OPTIONNEL) Il est possible qu'il vous soit demandé votre deuxième facteur et que vous ne l'ayez pas en votre possession (exemple : vous avec changé de cellulaire et ne pouvez donc pas utiliser *Microsoft Authenticator* sur votre ancien téléphone). Si vous avez conservé le même numéro de téléphone et que vous l'aviez configuré comme un de vos *deuxièmes facteurs*, vous pourrez vous en tirer sans faire appel au CAT en cliquant sur « Se connecter d'une autre façon » :

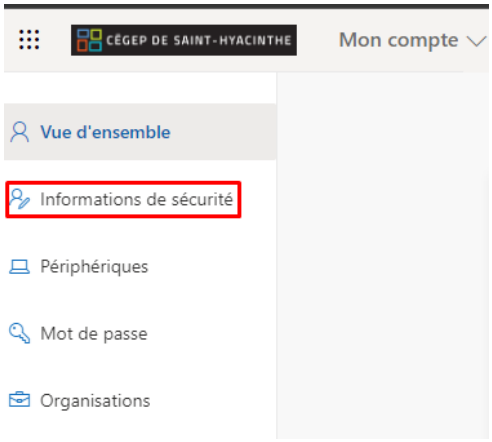


21. Il vous faudra ensuite sélectionner l'option SMS (ou « Appel », ou une autre option qui fonctionne toujours pour vous) et suivre les indications à l'écran :

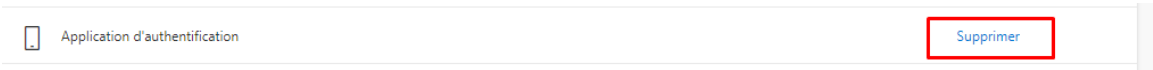


22. Cliquez sur « Mettre à jour les informations » ou sur « Informations de sécurité » dans la colonne de gauche :



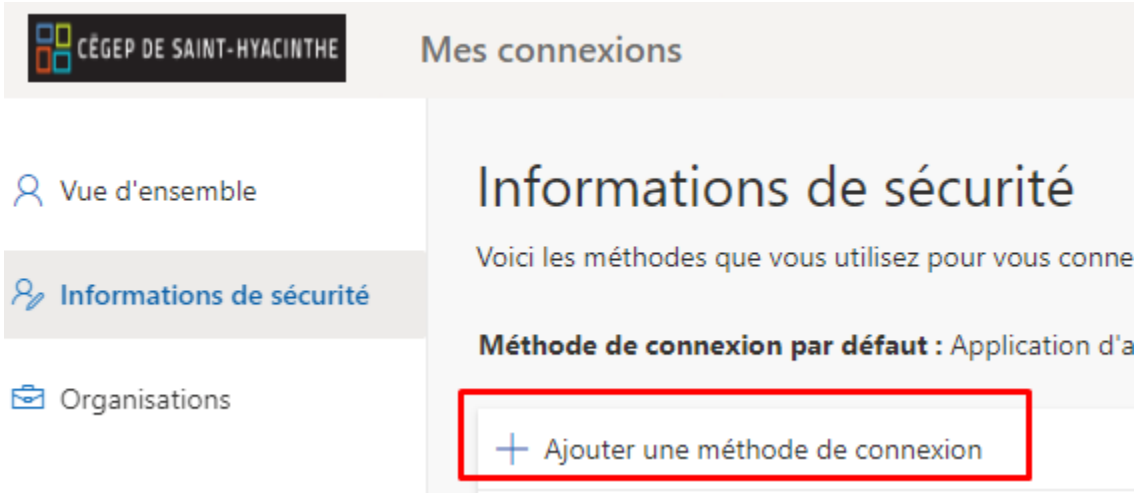


23. Pour **la suppression d'un facteur existant** cliquez sur « Supprimer » vis-à-vis le facteur en question (exemple ci-dessous : pour supprimer le lien avec l'*Authenticator* de votre ancien téléphone):

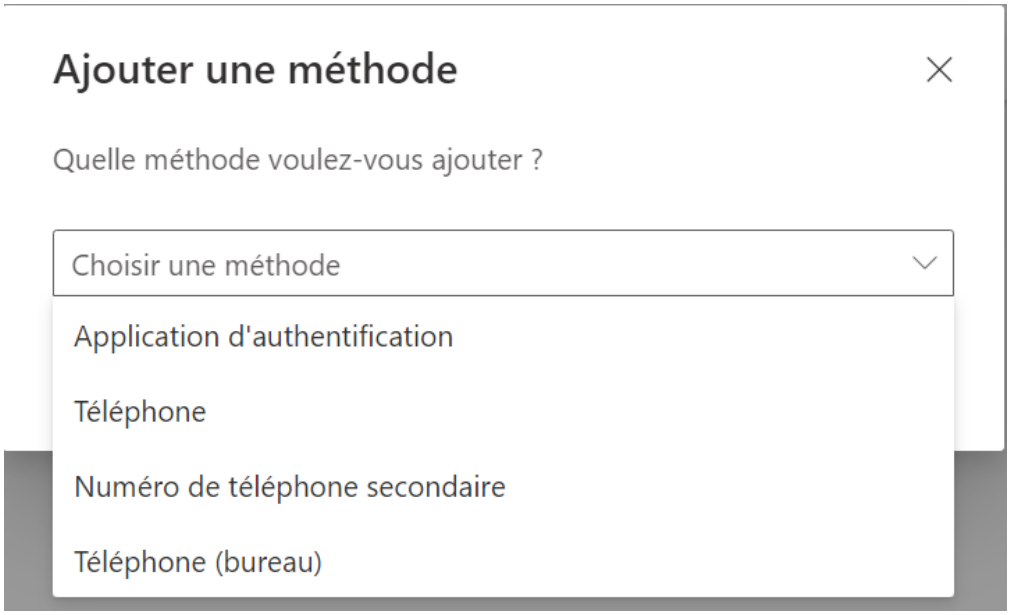


Ensuite, sur votre appareil mobile (cellulaire ou tablette) où est installé « Microsoft Authenticator, il faut supprimer le lien avec votre compte en ouvrant l'application, puis en appuyant sur la ligne « Cegep de Saint-Hyacinthe » qui montre également votre courriel du Cégep. Il faut aller appuyer sur la petite roue dentelée en haut à droite de l'écran, puis appuyer sur « Supprimer le compte » ou « Remove Account ». À l'écran qui suit, vous devez cliquer encore sur l'option « Supprimer le compte » ou « Remove Account ».

24. Pour **l'ajout d'un facteur supplémentaire**, cliquez sur « Ajouter une méthode de connexion », puis suivez les étapes à l'écran :

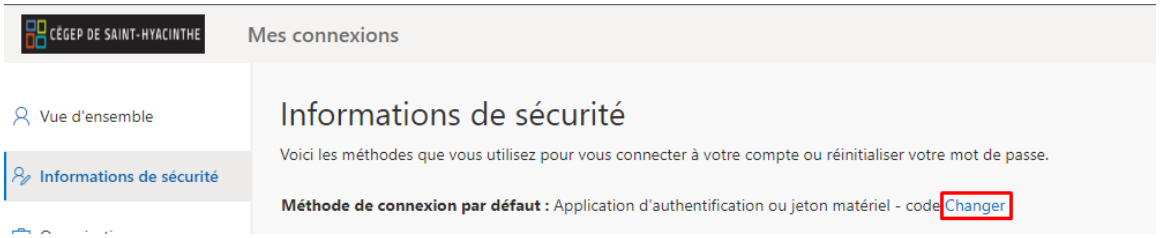


Vous pouvez ensuite sélectionner celui qui vous convient *(nous vous recommandons fortement « Application d'authentification » si vous ne l'utilisez pas déjà, soit une application à installer sur votre téléphone du nom de « Microsoft Authenticator »):*

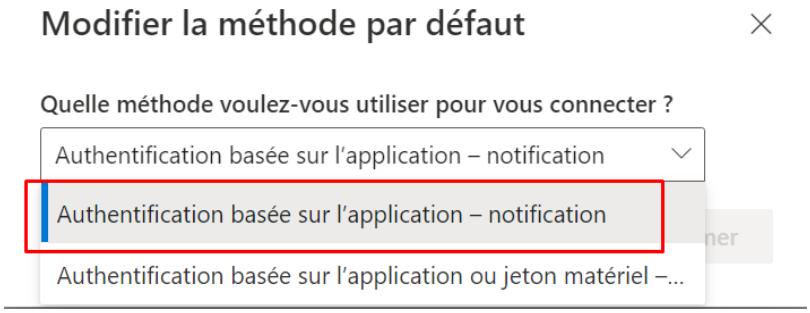


Pour plus de détails concernant l'inscription d'un facteur en particulier, référez-vous à cette section du guide.

25. Si vous souhaitez plutôt **modifier votre deuxième facteur principal** (*il est préférable de posséder au moins deux facteurs de double authentification pour le dysfonctionnement éventuel de l'un*) :

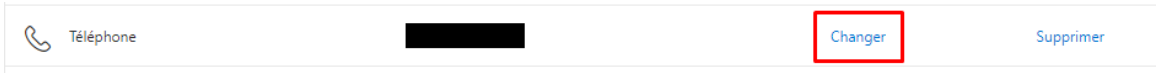


Cliquez ensuite sur la liste déroulante qui apparaît à l'écran, puis sélectionnez le facteur souhaité (la capture d'écran ci-dessous montre un exemple), puis cliquez ensuite sur « Confirmer »:



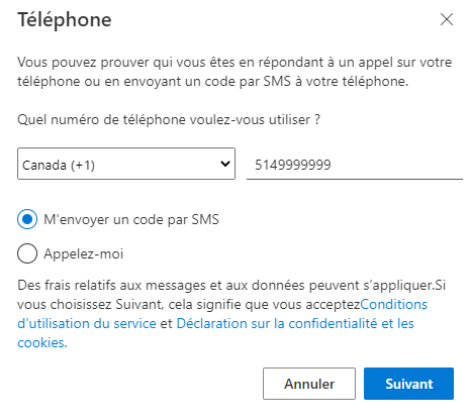
Pour ceux qui ont configuré « Microsoft Authenticator », nous vous recommandons fortement de sélectionner « Authentication basée sur l'application – notification », puisque cela vous permettra de voir une carte géographique avec la provenance approximative de chacune de vos connexions nécessitant le 2è facteur, en plus du nom de l'application à partir de laquelle vous tentez de vous connecter. *Sinon, il est possible de choisir « **Authentication basée sur l'application ou jeton matériel – code** » si c'est la seule option offerte (c'est le cas pour les jetons physiques), qui est très valable et sécuritaire également, mais qui n'offre pas autant de fonctionnalités que l'autre.*

26. Pour **modifier un numéro de téléphone**, cliquez sur « Changer » vis-à-vis le facteur en question :

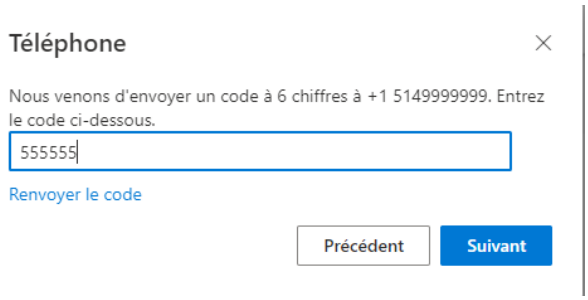


Vous pouvez ensuite entrer le nouveau numéro de téléphone, puis procéder à une vérification du numéro en sélectionnant l'envoi d'un texto (« M'envoyer un code par SMS ») ou par un appel téléphonique robotisé (« Appelez-moi »). Vous pouvez ensuite

cliquer sur « Suivant » :



Dans le cas de l'option du texto, un code unique de 6 chiffres vous sera demandé. Vous pouvez l'entrez comme suit et cliquez sur « Suivant » :



CÉGEP DE SAINT-HYACINTHE

Comment se procurer un nouveau jeton matériel?

ATTENTION! LE JETON PHYSIQUE EST OFFERT AUX EMPLOYÉS SEULEMENT et ne l'est pas pour les retraités, entraîneurs sportifs et étudiants.

Pour des raisons évidentes, il n'est pas possible de se procurer un jeton sans devoir passer au Cégep.

Songez-vous à vous convertir à l'utilisation d'un appareil mobile? Si oui, référez-vous à cette section!

Également, veuillez noter que les jetons physiques ne sont pas offerts aux entraîneurs sportifs et aux retraités.

- ✓ Créer un billet de demande de soutien informatique (https://abovecrm.cegepsth.qc.ca/abovecrm_info/PortailAboveCRM.asp) afin de fixer rendez-vous avec le CAT en indiquant vos disponibilités, ou par téléphone au 450-773-6800, poste 2198, ce qui nous permettra de configurer le jeton à l'avance et de vous contacter lorsqu'il sera prêt.

- ✓ Vous pouvez sinon vous présenter sans rendez-vous au B-2230 pendant les heures habituelles de service pour l'obtention d'un nouveau jeton. Vous devez prévoir des délais supplémentaires.