Si vous avez besoin d'assistance, veuillez créer une requête ici

Configuration de validation en deux étapes

Qu'est-ce que la validation en deux étapes ?

La validation ou l'authentification en deux étapes ou à deux facteurs (authentification forte) est un procédé qui fait appel à deux étapes de vérification pour sécuriser l'accès à un profil d'usager, permettant ainsi de se protéger contre les accès non autorisés et bloque les tentatives de connexions inhabituelles. La validation en deux étapes peut, par exemple, être utilisée si on accède à un compte courriel, à des applications, à des espaces de stockage de données, ou aux comptes de réseaux sociaux. *La validation en deux étapes est aussi communément connue sous 2FA (Two-Factor Authentication), MFA (Multi-Factor Authentication) ou AMF (Authentification Multifactorielle).*

Pourquoi utiliser la validation en deux étapes?

Le montant d'acteurs malveillants, les campagnes d'hameçonnage et les cyberattaques continuent à augmenter de manière constante et deviennent de plus en plus sophistiqués. Il est donc de plus en plus difficile d'assurer un niveau de sécurité adéquat avec l'utilisation d'un mot de passe complexe. En activant une deuxième méthode de validation en deux étapes, il est beaucoup plus difficile (voir presque impossible) qu'un attaquant puisse accéder à votre compte et aux renseignements, même avec votre mot de passe.

La validation en deux étapes est utile à tous membres du personnel qui accède à des renseignements sensibles, qui se branche à partir d'endroits comme un hotspot wifi non sécurisé, ou lorsqu'une présence usurpée sur les réseaux sociaux pourrait être dommageable.

Fonctionnement avec la validation en deux étapes.

Avec la validation en deux étapes activées, chaque nouvelle connexion va demander une deuxième authentification pour s'assurer que la tentative d'authentification provient de vous.

Pour des appareils de travail qui sont utilisés quotidiennement, Microsoft et Google leur donnent un haut niveau de confiance, donc la validation en deux étapes n'est pas nécessaire à chaque connexion.

Exigences pour activer la validation en deux étapes.

Pour activer la validation en deux étapes, il faut au minimum un téléphone cellulaire avec un numéro actif. L'application Microsoft Authenticator est capable de générer des codes de sécurité même s'il n'a pas de signal cellulaire.

La deuxième option est un texto SMS où il faut simplement fournir un numéro de téléphone pour recevoir les codes de validation.

La troisième option qui utilise, elle aussi, l'application Microsoft Authenticator peut envoyer une invite Microsoft. Vous n'avez qu'à sélectionner oui sur votre cellulaire lorsqu'il sera affiché. Mais, cette option exige la configuration de votre compte du conseil scolaire dans les logiciels Microsoft Authenticator et votre appareil doit posséder un code pour débarrer l'écran.

Comment activer la validation ?

La validation à deux étapes protège votre compte et les données ainsi que plusieurs des applications web offertes par le CSDCEO par exemple Aspen, eBase, portail d'employé et d'autres qui s'ajouteront dans le futur.

Il y a plusieurs façons d'ajouter l'AMF à votre compte

- Utilisé le Déroulement d'activation (recommander)
- Utilisé l'inscription manuelle

Déroulement d'activation Authentification multifactorielle (AMF)

Cette méthode vous apporte directement au processus d'inscription AMF.

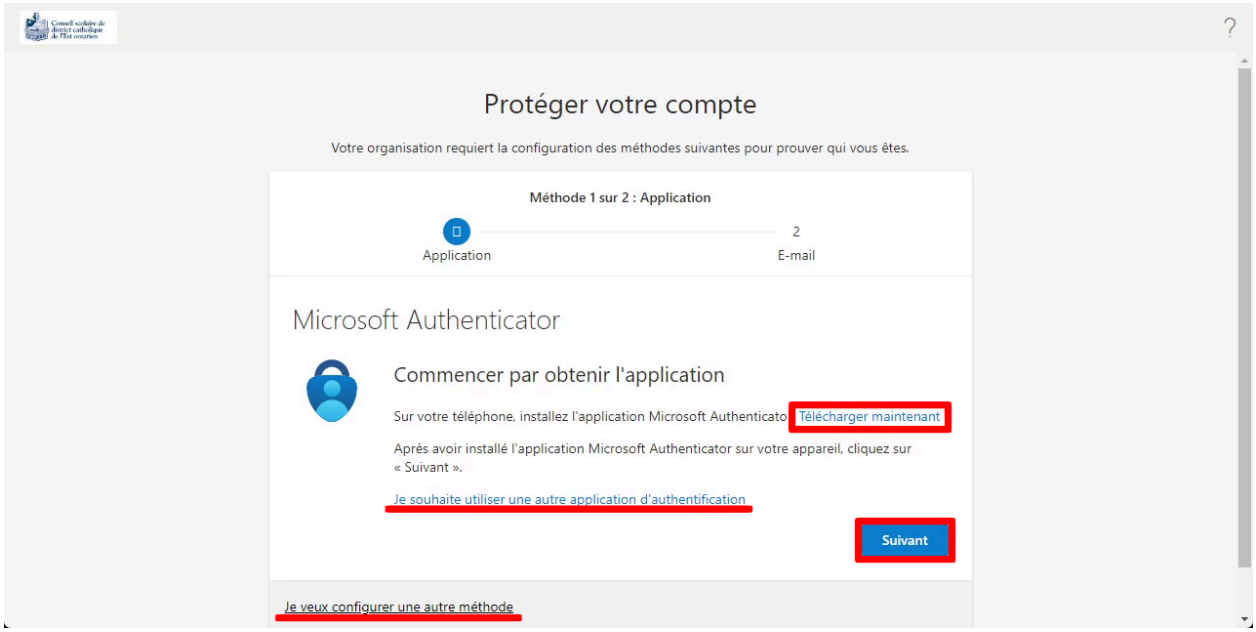
1. Cliquez sur ce lien https://aka.ms/mfasetup pour commencer votre inscription ou vous serrez apporter automatiquement lors d'une authentification Google ou WEB.
   Notez que si vous avez déjà fait l'inscription, vous serez apportés au portail de gestion de votre compte Microsoft.
2. Après vous avoir authentifié, vous serez dirigés à la première étape.

3. Vous pourrez choisir la méthode désirée soit l'application de Microsoft Authenticator qui est fortement recommandé pour sa sécurité et fonctionnalités additionnelles ou par SMS sur votre téléphone portable.

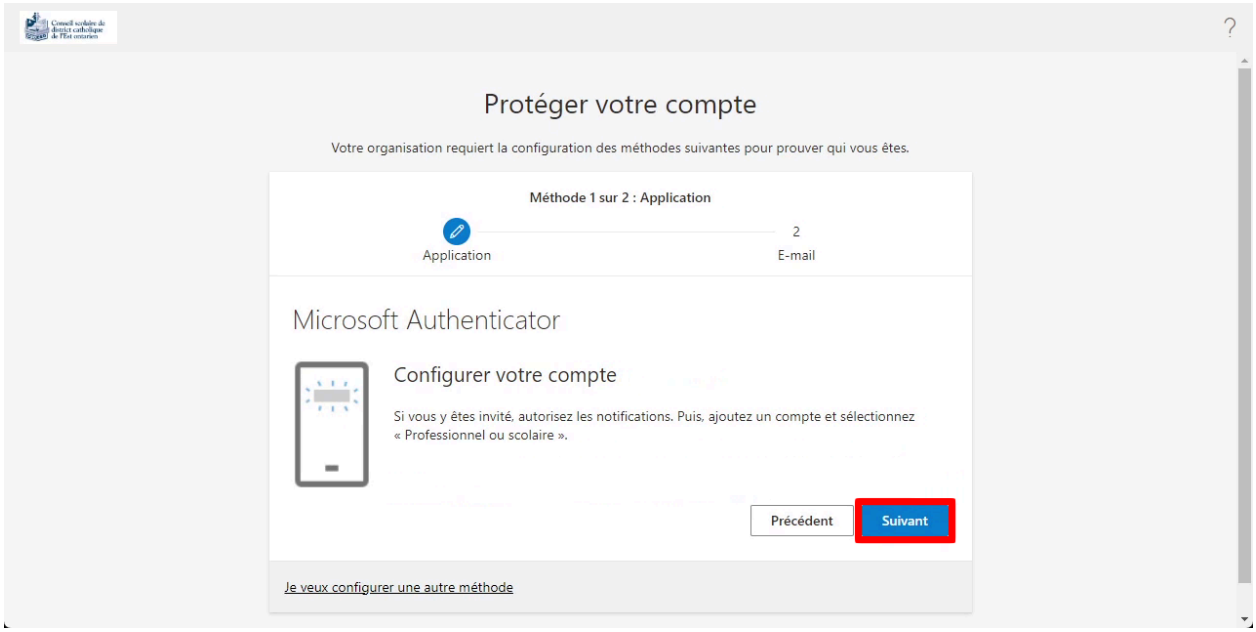
4. Choisir la méthode d'inscription
    - Application Microsoft Authenticator
    - Texto SMS

Application Microsoft Authenticator

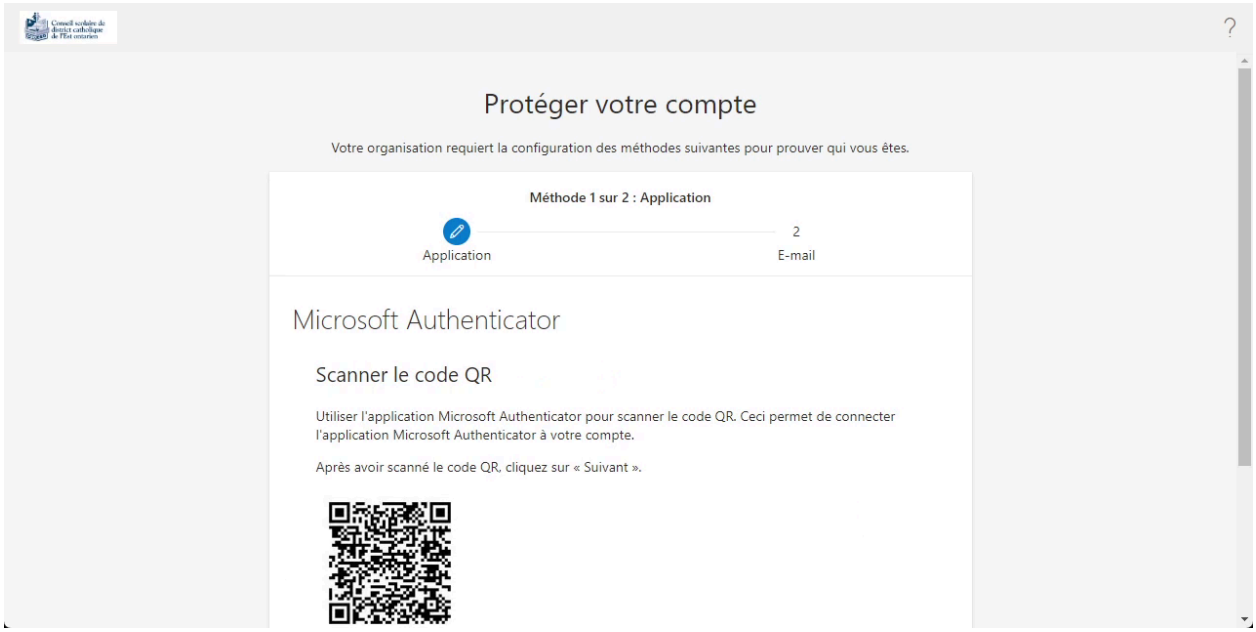
1. **La première étape** sera la configuration d'authentification à deux facteurs. Nous vous suggérons la plus sécuritaire, Microsoft Authenticator qui est l'option par défaut.
    - Cliquez **Télécharger maintenant** pour être redirigé pour l'installation du logiciel par code QR sur votre cellulaire. Une fois l'application installée, cliquez sur le bouton suivant.
    - Si vous utilisez déjà un générateur de code comme Google Authenticator, vous pouvez cliquer « **Je souhaite utiliser une autre application d'authentification** ».
    - Vous pouvez aussi choisir parmi d'autres méthodes comme un texto SMS à votre téléphone en cliquant sur « **Je veux configurer une autre méthode** ».



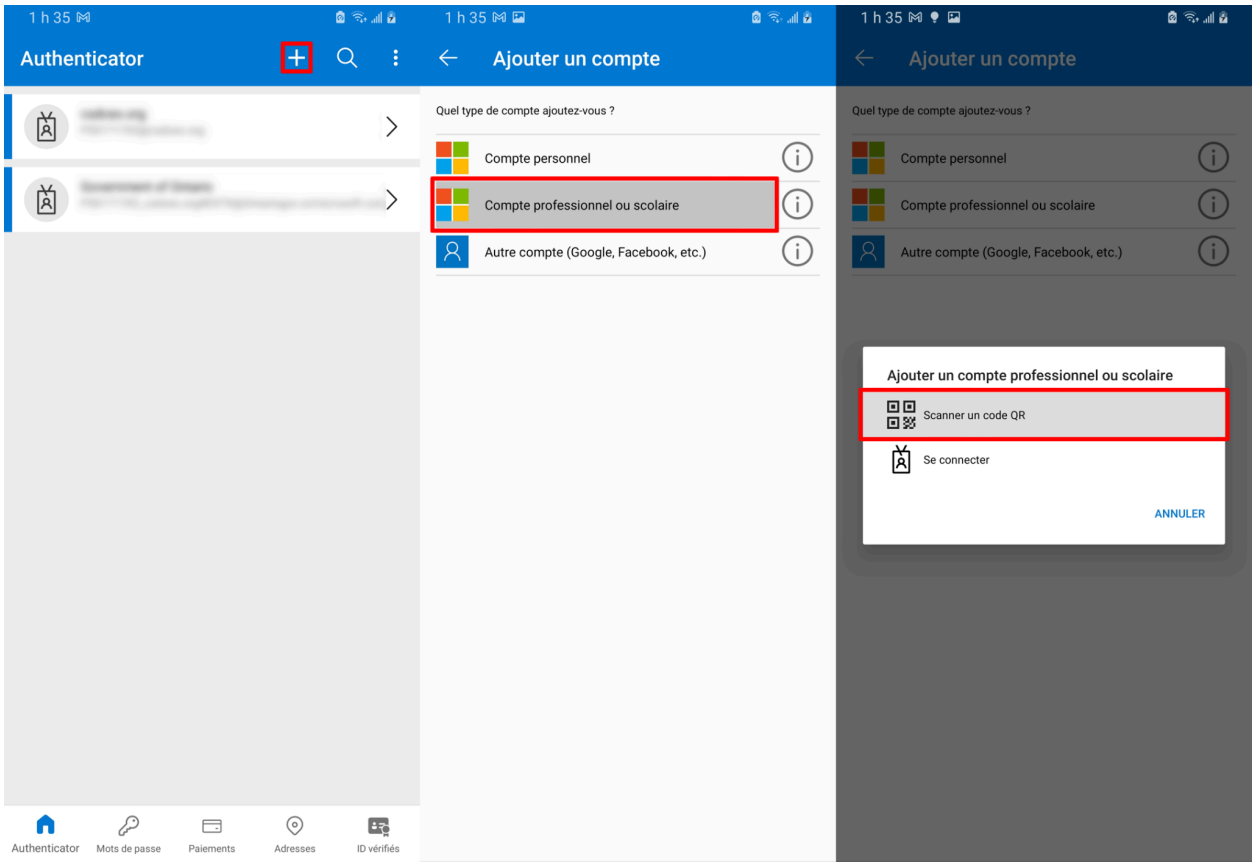
2. Après avoir installé Microsoft Authenticator sur votre cellulaire, cliquez sur Suivant.



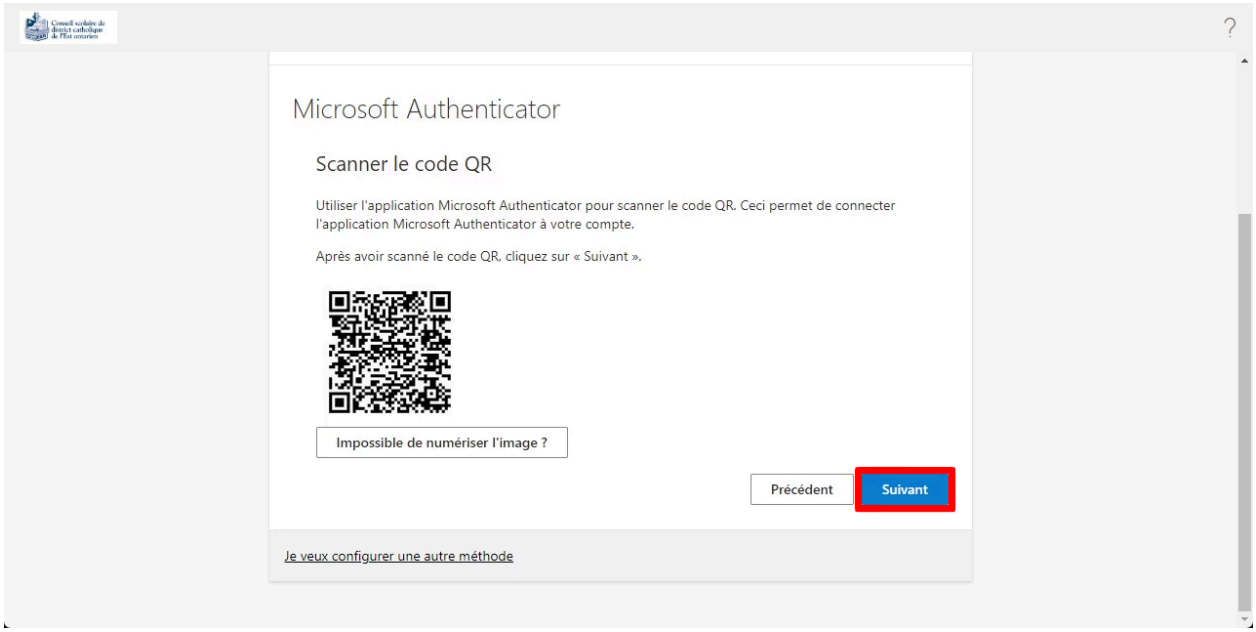
3. Maintenant que vous avez un code QR à l'écran, il faut l'ajouter dans l'application Microsoft Authenticator sur votre cellulaire.



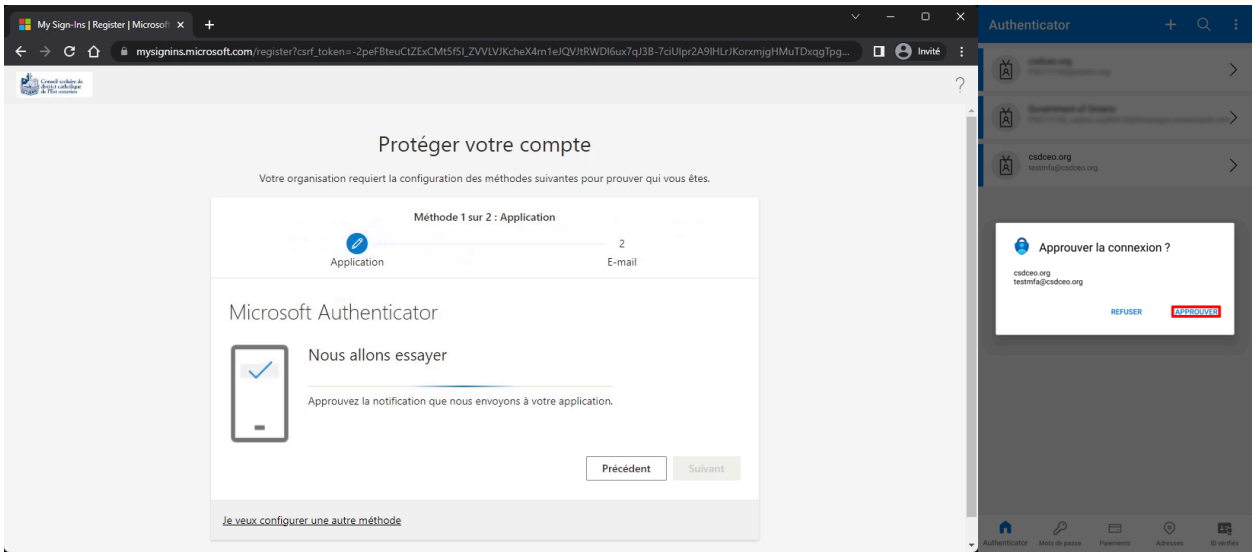
4. Dans l'application Microsoft Authenticator de votre cellulaire, suivez les étapes suivantes :
    - Cliquez sur le **+** pour ajouter un nouveau compte.
    - Sélectionnez **Compte professionnel ou scolaire**.
    - Cliquez sur **Scanner un code QR**. (Assurer vous de choisir cette option)
    - Capturez le code QR sur votre écran (comme indiqué à l'image précédente).



5. Après avoir capturé le code QR cliquez sur Suivant.

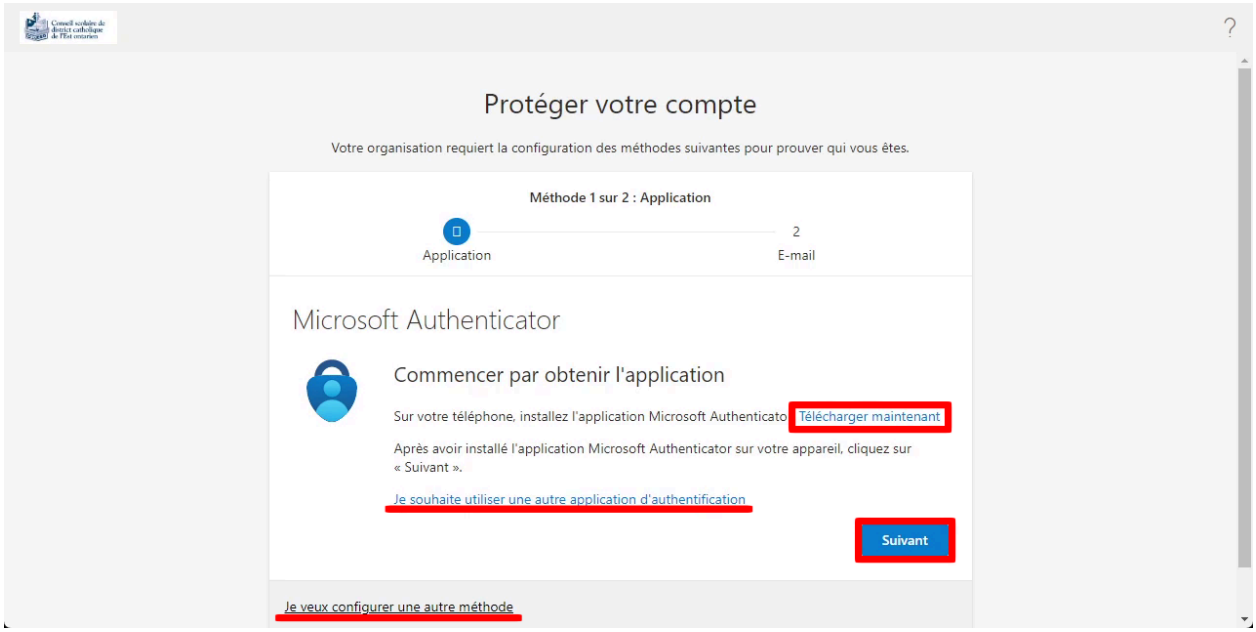


6. Une demande va être envoyée à votre cellulaire donc, cliquez sur **Approuver**.



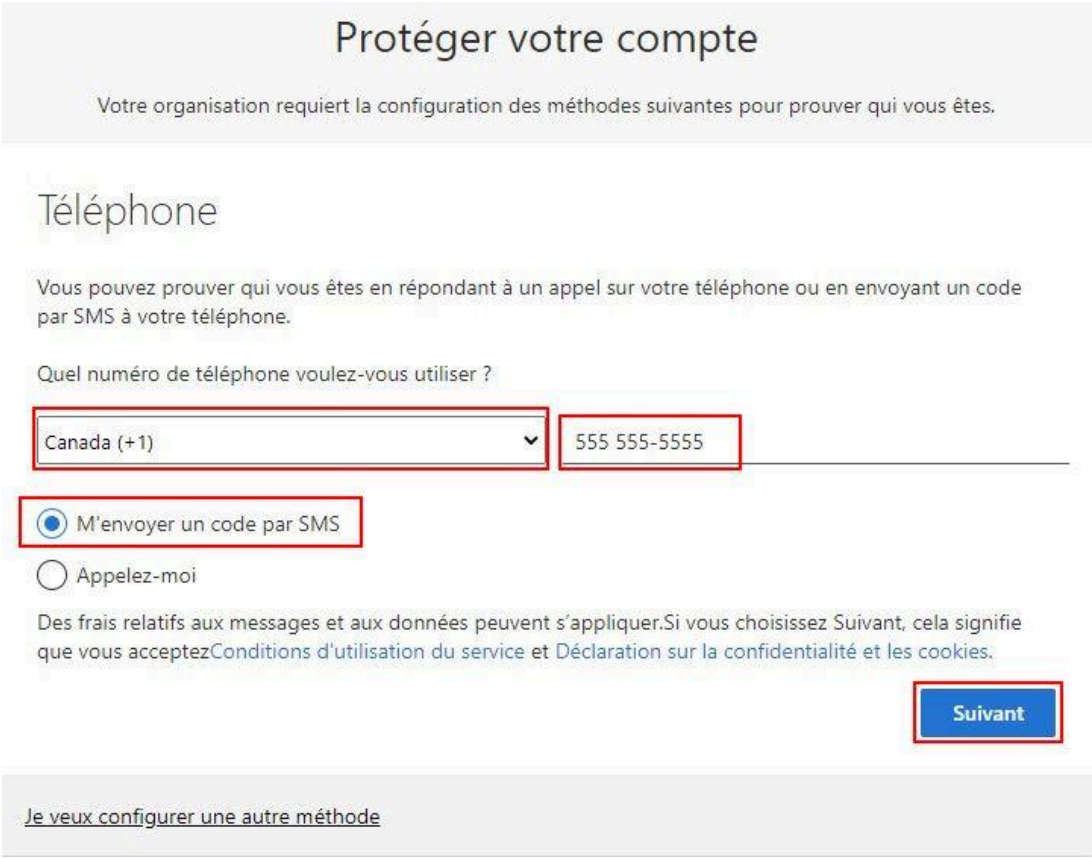
Texto SMS

1. Suite à vous authentifier vous
2. Si vous voulez l'inscription par texto SMS, sélectionnez l'option **je veux configurer une autre méthode.**

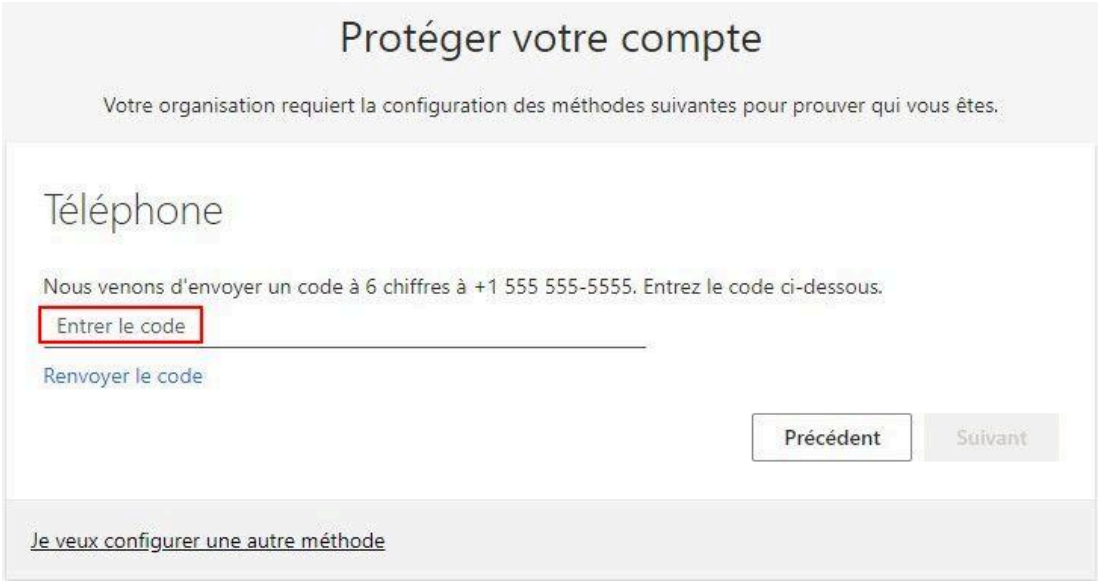


3. Choisir du menu déroulant Téléphone

4. Choisir Canada, mettre votre numéro de cellulaire et choisissez de l'option M'envoyer un code par SMS et cliquer sur le bouton suivant.

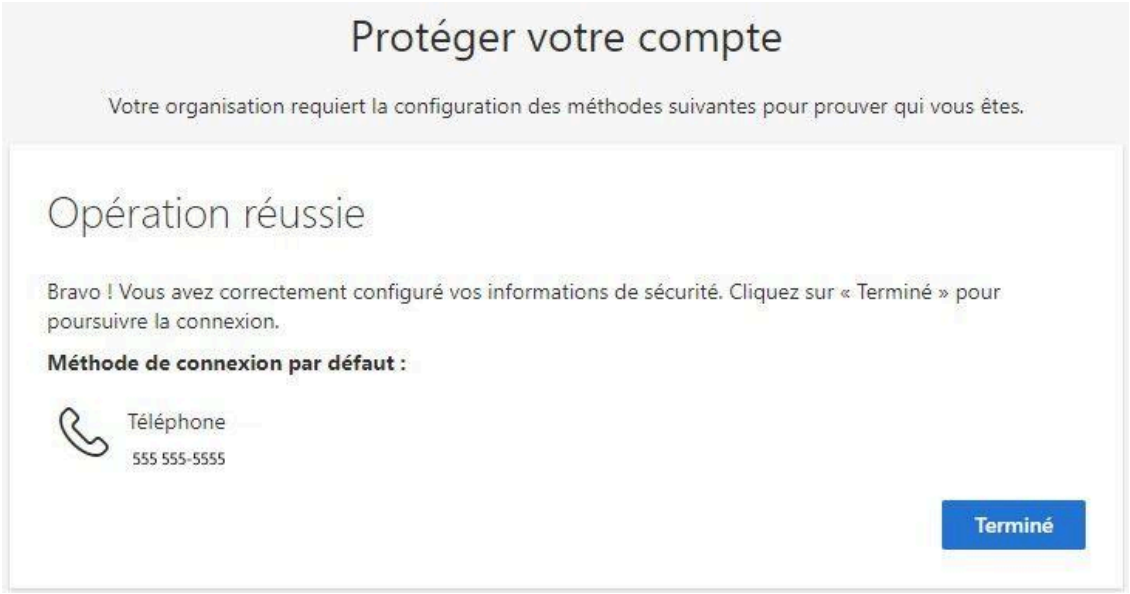


5. Vous devriez recevoir SMS, insérer le code de 6 chiffres et cliquer sur suivant.



6. Une validation que le code entré est bon vous sera afficher.

7. Félicitation, ceci complète votre inscription AMF. À partir de maintenant, certains services vous demanderont une deuxième validation quand il sera nécessaire.



Clé USB de sécurité

La configuration de la clé sécurité USB contient plusieurs étapes de plus et est un peu plus complexe. Suivez cette procédure après avoir reçu votre clef USB de sécurité.

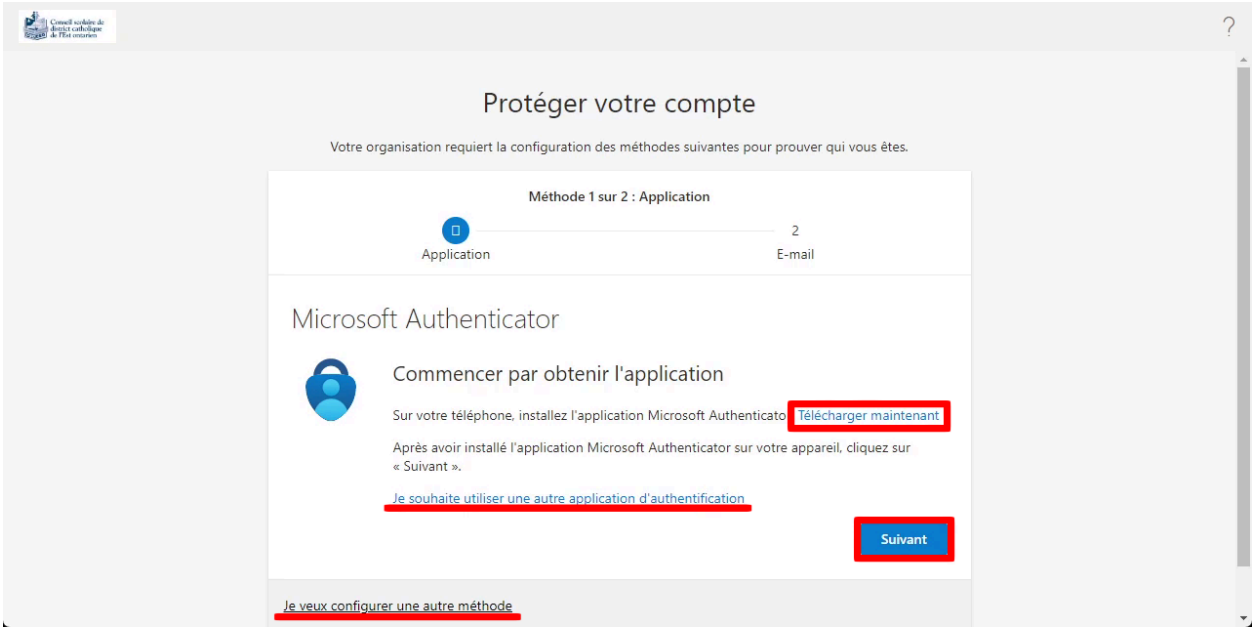
Nous avons remarqué qu'il n'y a pas d'option pour ajouter votre clé de sécurité lors de l'activation de l'authentification multifactorielle. Ceci est parce qu'il doit y avoir une autre méthode de disponible avant que la clé puisse être enregistrée.

Il y a deux options de disponible,

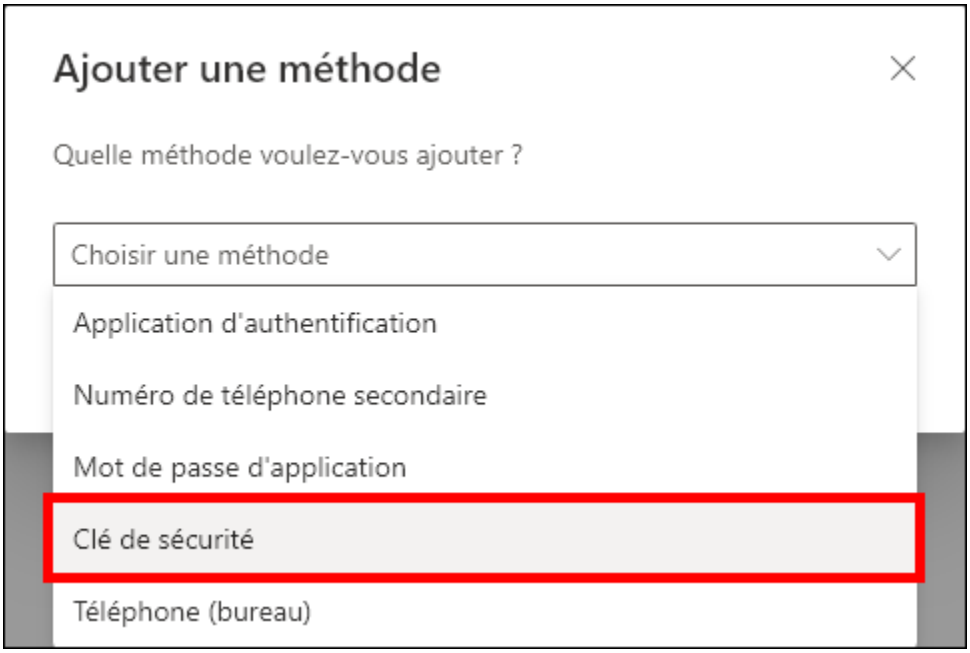
1. Vous pouvez utiliser la méthode SMS ou vocal de votre téléphone et ensuite enregistrer votre clé de sécurité, mettre la clé comme méthode par défaut et quand le tout est terminé, enlever votre téléphone.

2. Prendre un rendez-vous en utilisant le formulaire '**Oublié mon mot de passe**' nous allons vous fournir un mot de passe temporaire pour être en mesure d'enregistrer votre clé.

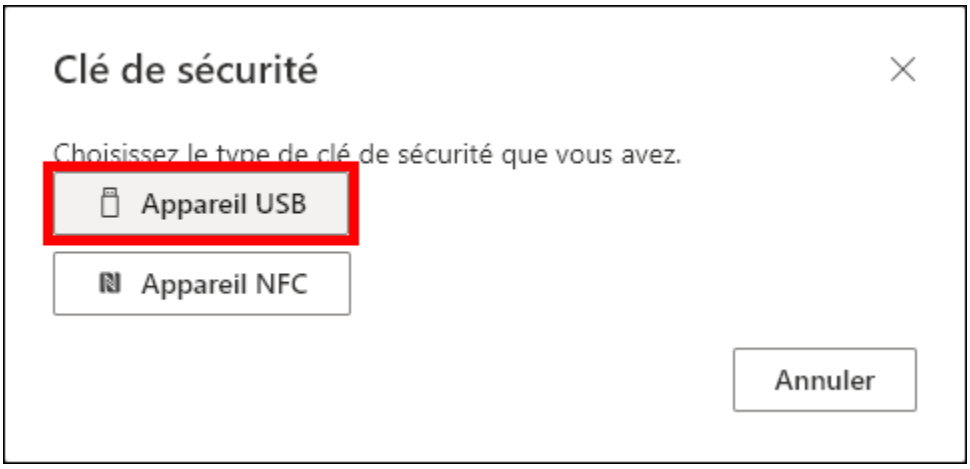
1. Aller à l'adresse https://aka.ms/mfasetup. Il est possible qu'il vous demande de vous authentifier.
2. Sélectionnez l'option. Je **veux configurer une autre méthode** au bas de la page.



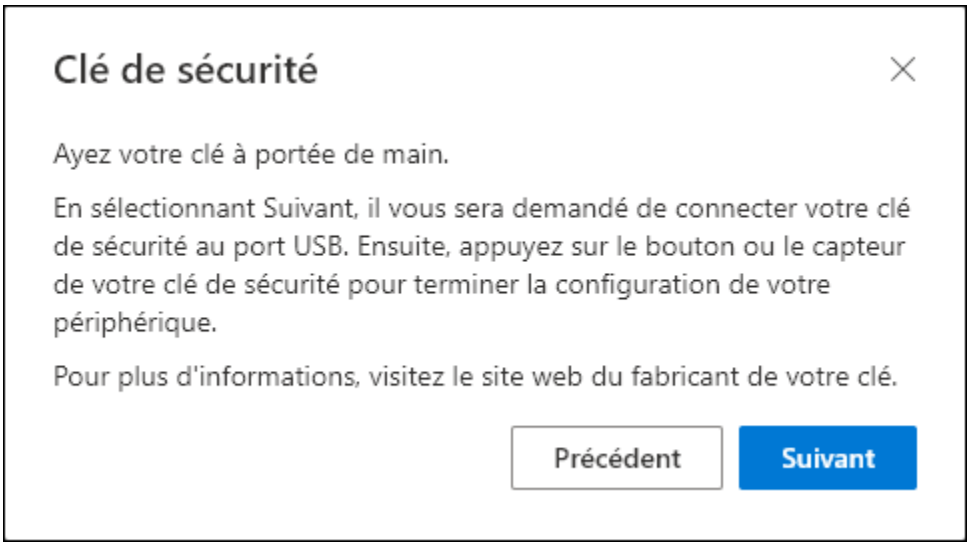
3. Sélectionnez **Clé de sécurité,** ensuite cliquez sur **Suivant**.


Ajouter une méthode
Quelle méthode voulez-vous ajouter ?
Choisir une méthode
Application d'authentification
Numéro de téléphone secondaire
Mot de passe d'application
Clé de sécurité
Téléphone (bureau)

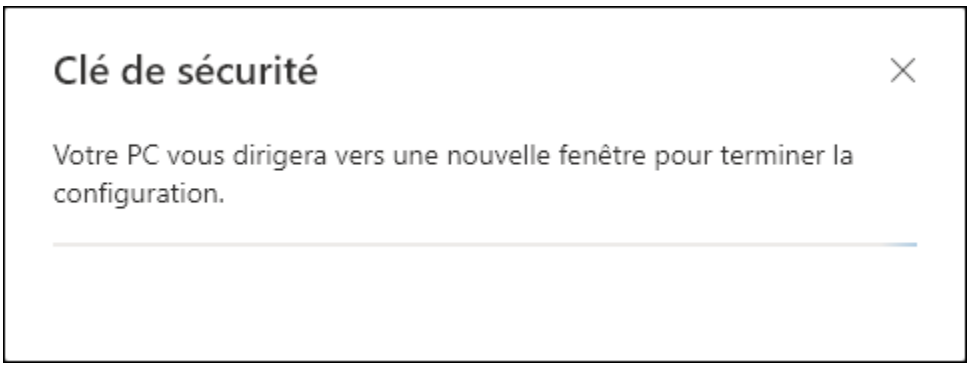
4. Cliquez sur **Appareil USB**.



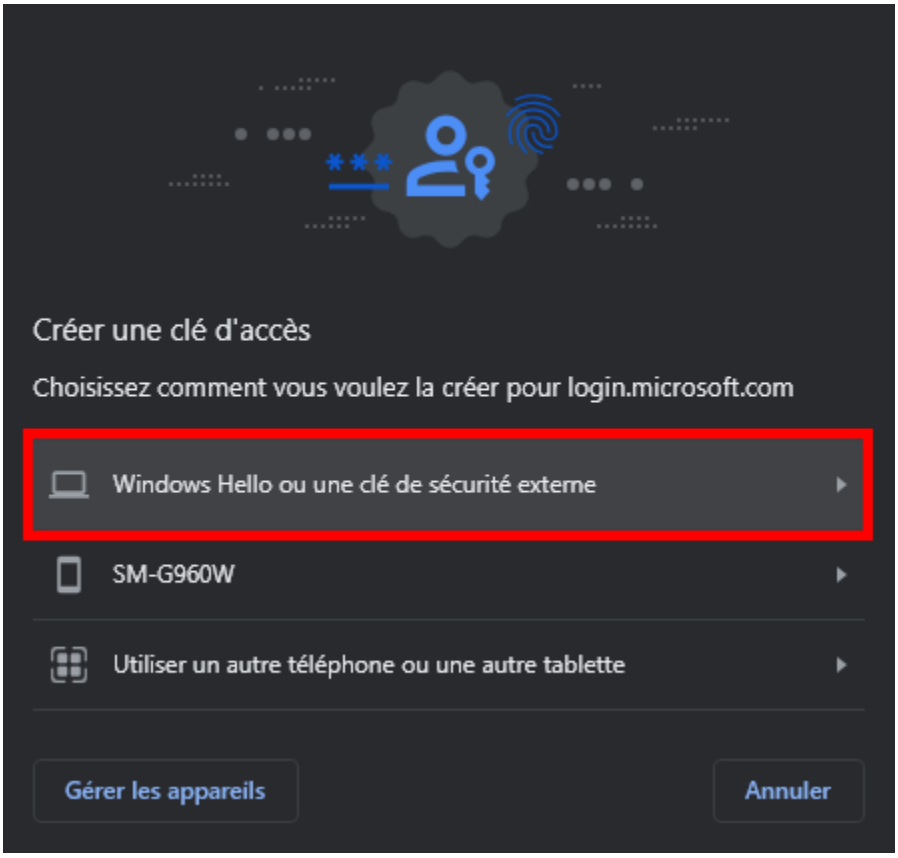
5. Cette fenêtre vous informe que la prochaine étape va commencer la configuration de votre clé USB. Cliquez sur **Suivant** pour continuer.



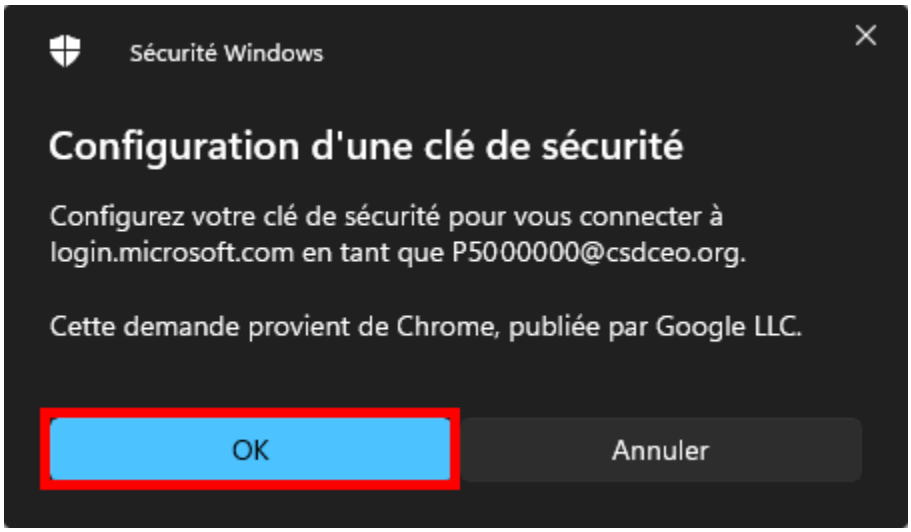
6. Attendez quelques instants pendant que la configuration débute.



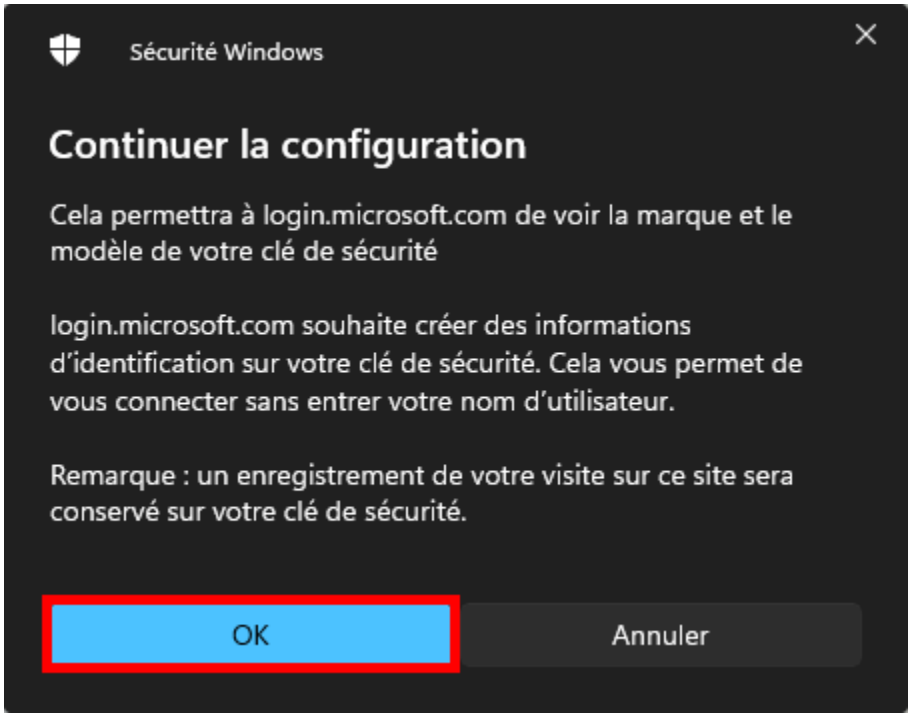
7. Google Chrome va montrer la fenêtre suivante, sélectionnez **Windows Hello ou une clé de sécurité externe** pour configurer votre clé de sécurité.



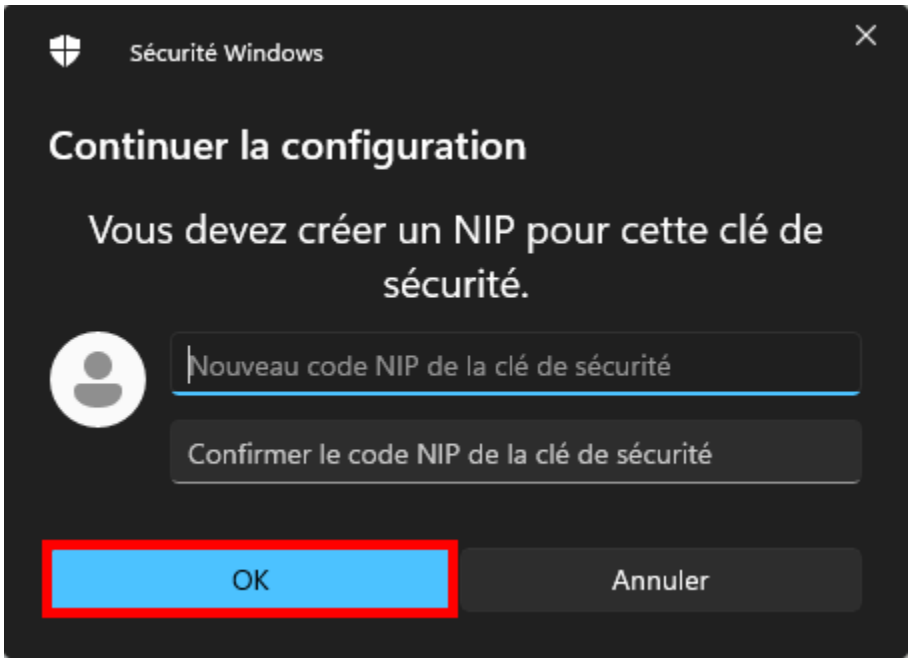
8. Windows va maintenant demander permission pour permettre Chrome d'utiliser votre clé de sécurité, cliquez sur **OK** pour permettre ceci.



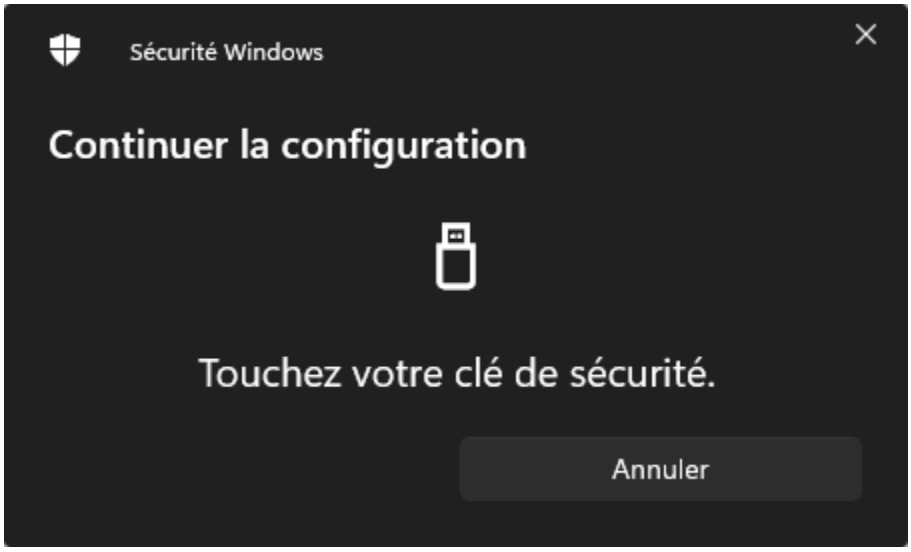
9. Windows vous avertit que le site web spécifié va avoir accès à votre clé de sécurité. Assurez-vous que le site est bien celui de microsoft.com ensuite, cliquez sur **OK**.



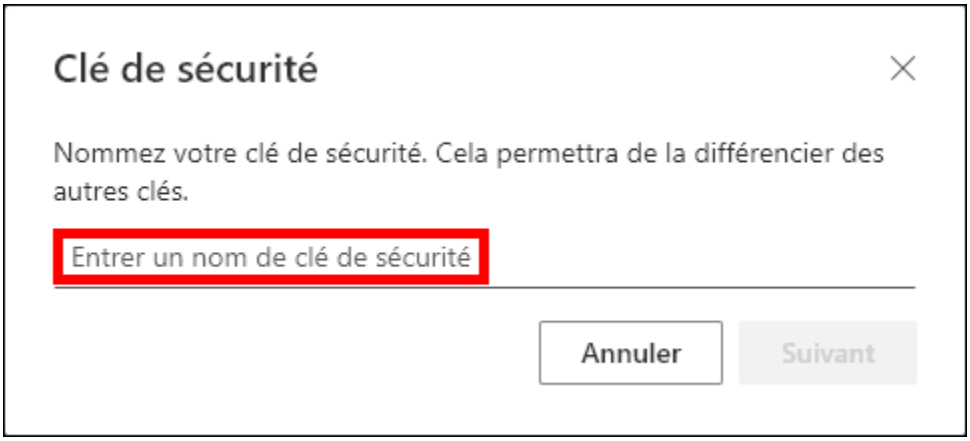
10. Créez un NIP pour sécuriser votre clé. **ATTENTION : Ce NIP est nécessaire pour utiliser la clé, donc il est important de ne pas oublier ce code**.



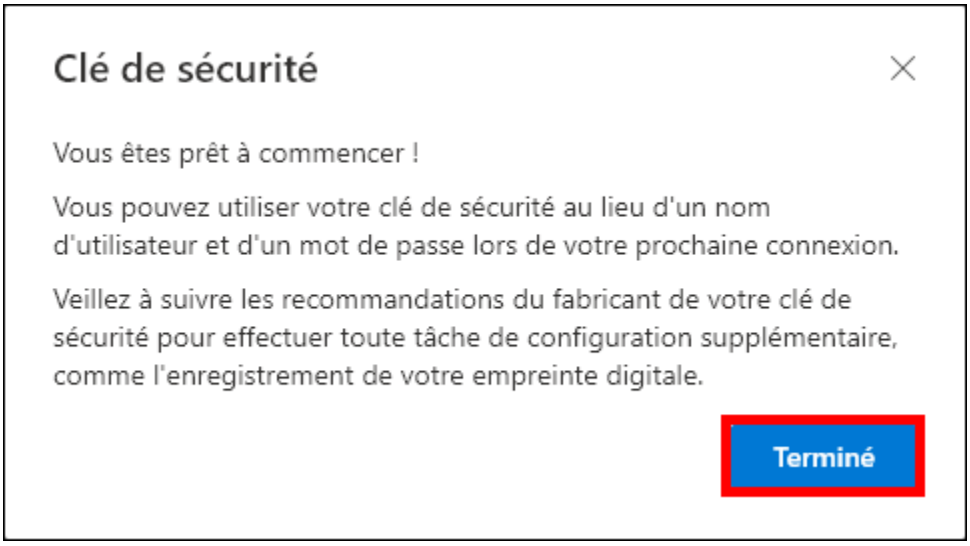
11. Après avoir créé un NIP, il devrait y avoir une lumière qui clignote sur votre clé de sécurité. Appuyez sur le bouton ou le rond doré pour permettre accès à Microsoft.



12. Donnez un nom pour identifier votre clé et ensuite, cliquez **Suivant**.



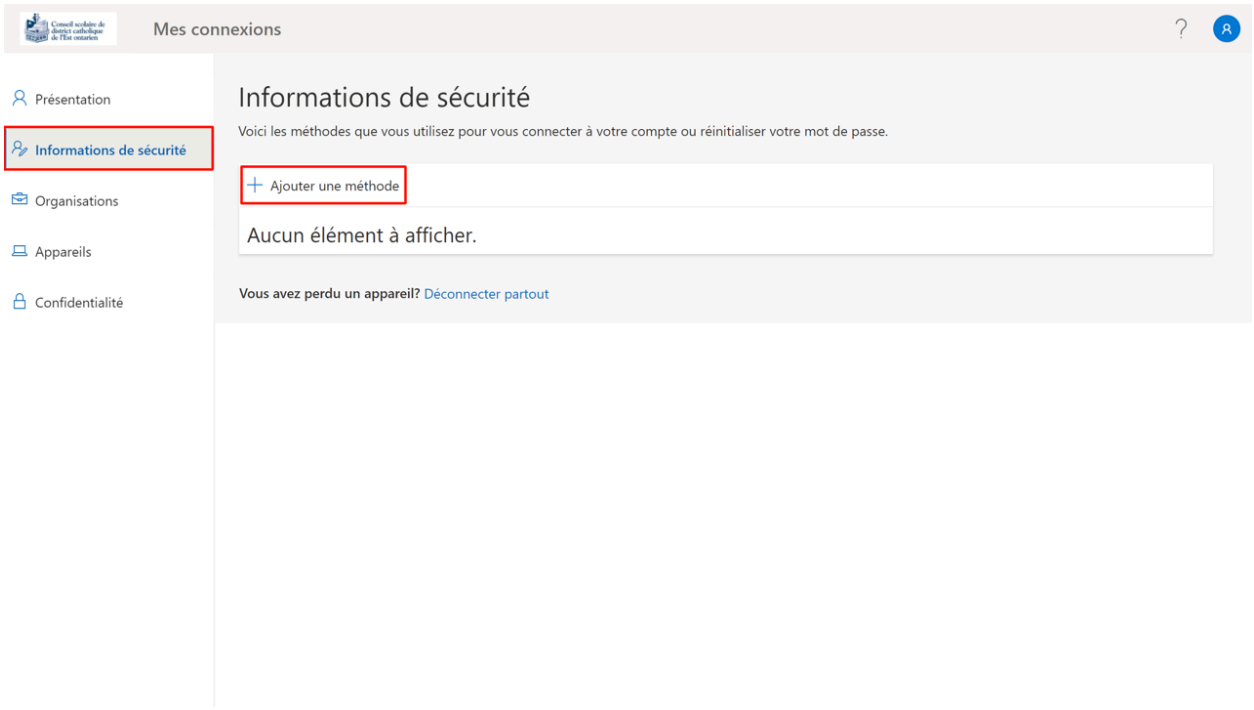
13. Vous avez maintenant la confirmation que la clé est configurée. Cliquez sur **Terminé** et vous pouvez à présent fermer la fenêtre ou configurer une autre méthode d'authentification.



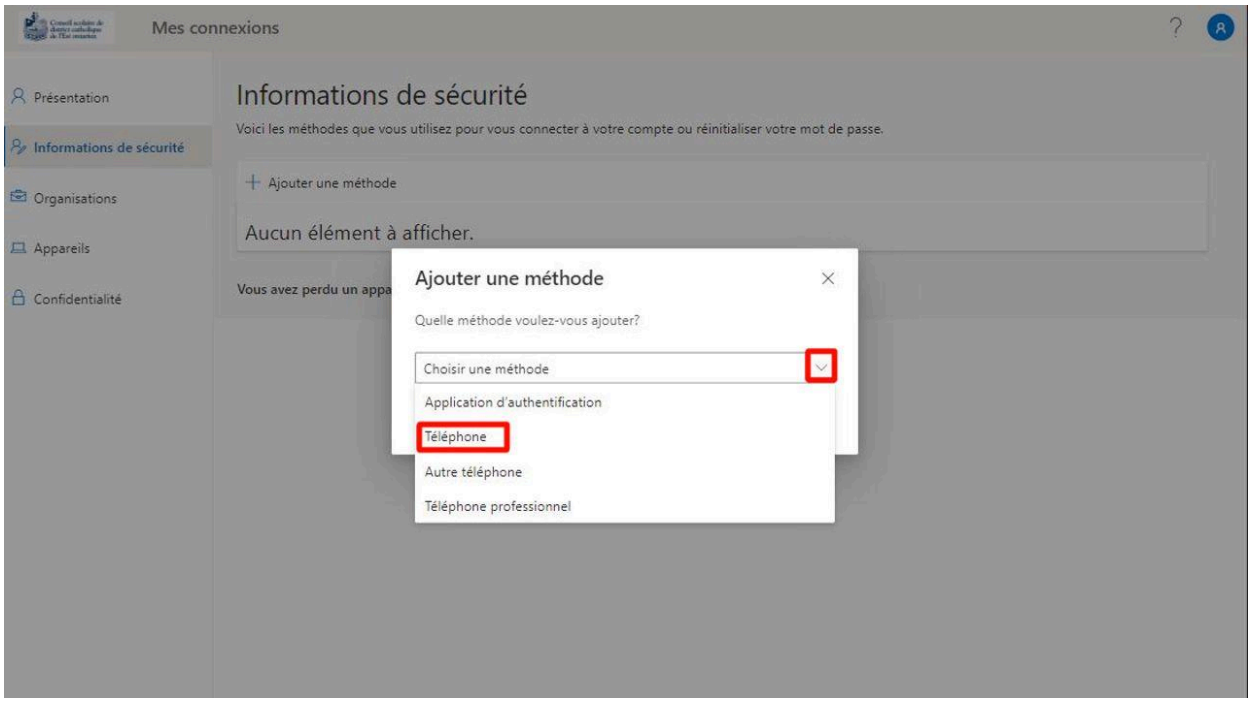
Ajout manuel et gestion des méthodes à utiliser

Pour gérer ces préférences de sécurité, soit pour ajouter ou révoquer des méthodes de vérification à 2 étapes, suivez les étapes suivantes.

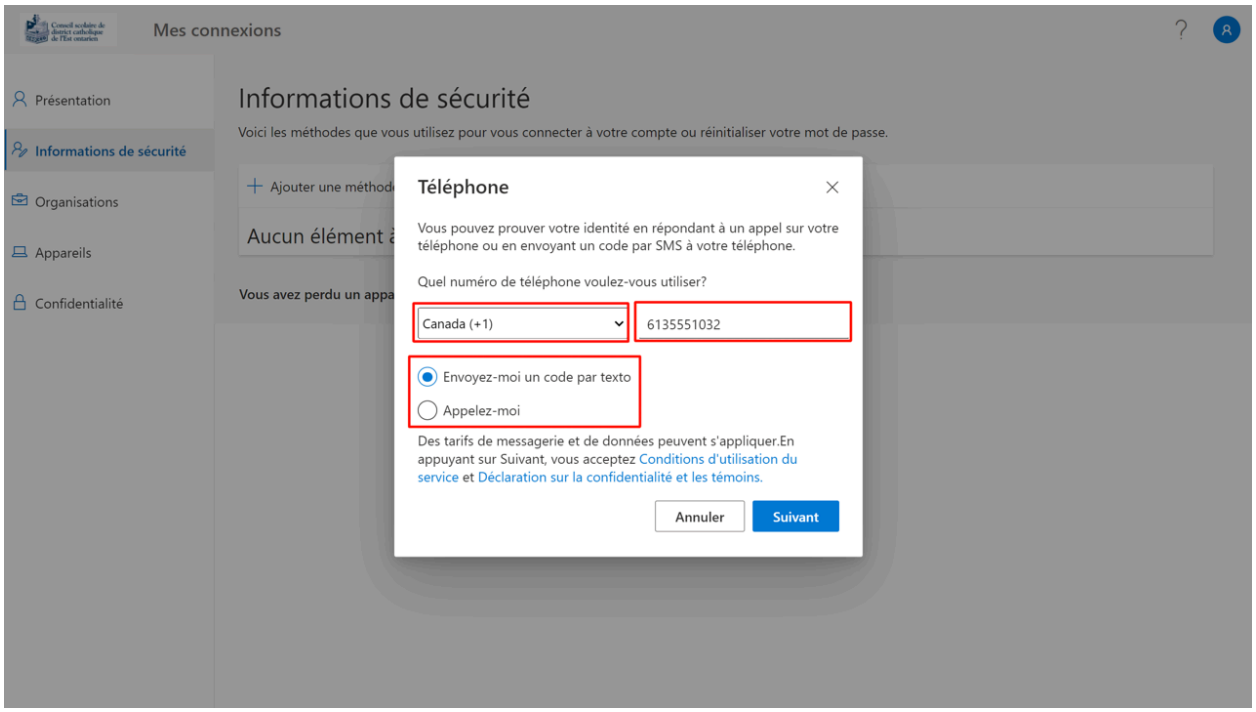
1. Cliquer sur ce lien https://mysignins.microsoft.com/security-info pour se rendre à la configuration d'authentification multifacteur de Microsoft.
   Note : Si vous n'êtes pas déjà connecté, vous devrez vous authentifier en utilisant votre compte Active Directory qui est le même que pour l'ordinateur (P0000000@csdceo.org).
2. Sélectionner Informations de sécurité et ensuite Ajouter une méthode


Mes connexions
Présentation
Informations de sécurité
Organisations
Appareils
Confidentialité
Informations de sécurité
Voici les méthodes que vous utilisez pour vous connecter à votre compte ou réinitialiser votre mot de passe.
Ajouter une méthode
Aucun élément à afficher.
Vous avez perdu un appareil? Déconnecter partout

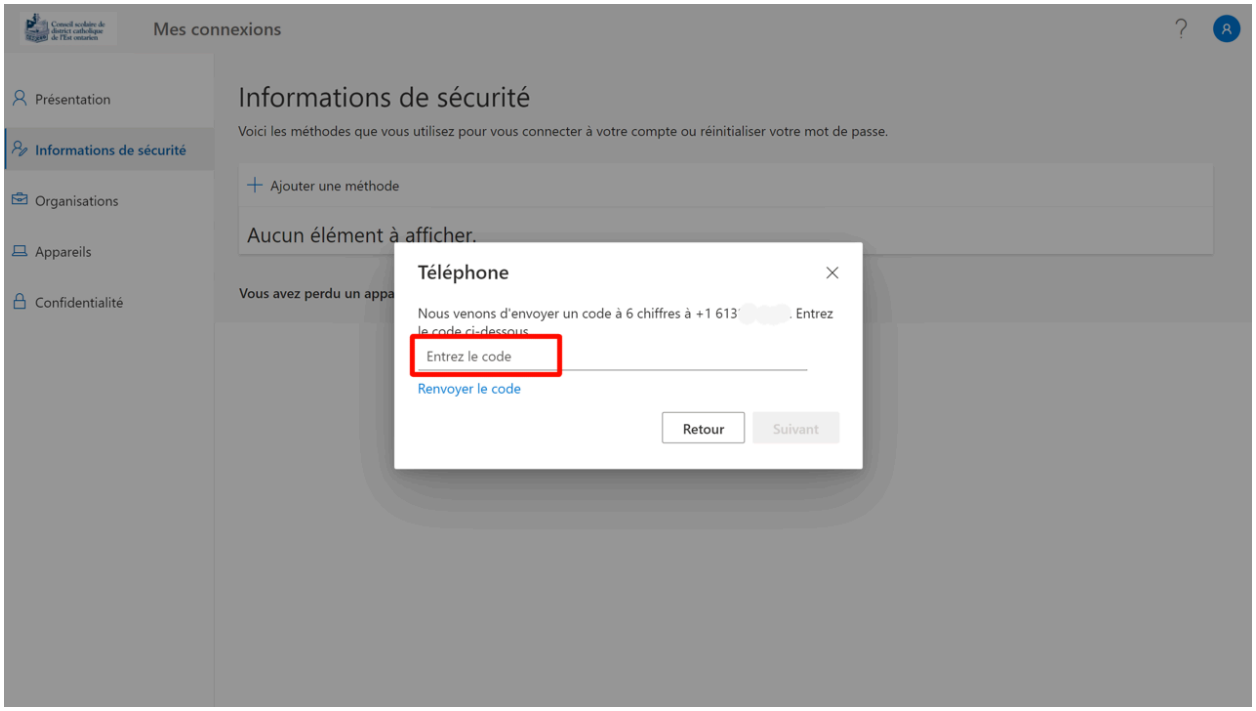
3. Sélectionner la petite flèche et choisir Téléphone ensuite cliquer sur ajouter



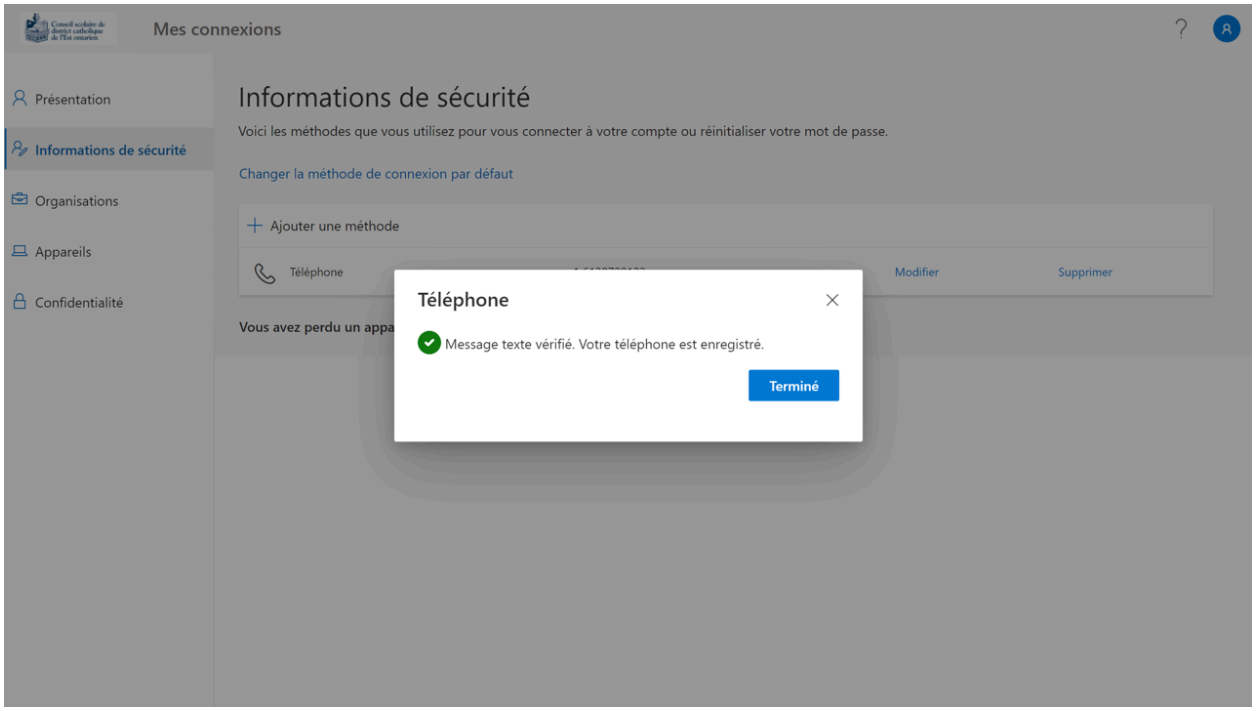
4. Sélectionner Canada et ensuite entrer votre numéro de téléphone.



5. Entrer le code reçu à votre téléphone et ensuite appuyer sur suivant.



6. Si vous avez entré le code correctement, vous aurez un message avec un coche vert. Ceci termine votre connexion deux étapes pour votre compte Active Directory.



À partir de maintenant, vous aurez à valider votre identité en utilisant la méthode choisie.

1. Quand vous utiliserez un nouvel appareil.
2. Quand ça fait longtemps que vous n’avez pas utilisé votre appareil principal.
3. De temps en temps, juste pour confirmer que c’est bel et bien vous qui utilisez réellement l'appareil.

Foire aux questions

- Je dois changer mon cellulaire et j'utilise l'application Microsoft Authenticator :
    - Vous devez sauvegarder les données et les récupérer sur votre nouveau cellulaire. Vous pouvez vous fier à ce guide Sauvegarder et récupérer Authenticator sur un nouvel appareil.
- Je dois changer de # de téléphone et j'utilise l'authentification via texte
    - Dès que vous connaissez le nouveau numéro de téléphone, une requête doit être faite au service TI pour le modifier à votre compte.
- J'ai perdu ma clé AMF
    - Vous devez vous rendre au portail, cliquez « Problème de connexion »,
- J'ai oublié mon NIP pour ma carte AMF
    - Vous devez faire une requête au service TI pour qu'ils vous aident à effacer votre clé et créer un nouveau NIP
- J'ai besoin d'une nouvelle clé AMF
    - Vous devez vous rendre au portail, cliquez « Problème de connexion »,
- J'utilise l'authentification avec l'application Microsoft Authenticator et je ne reçois pas de code
    - Selon le type et l'âge du cellulaire, parfois, l'application n'envoie pas le code. Si ceci vous arrive, vous devez démarrer l'application sur votre cellulaire et dans la section csdceo.org. Vous pourrez y voir un code à usage unique.
- Ma clé AMF n'est pas détectée par l'ordinateur.
    - Certaines clés peuvent être branchées des deux côtés. Il faut avoir le côté, avec le bouton, vers le haut.
    - Si votre clé est sur le bon sens, vous pouvez tenter de brancher à un autre port USB de l'ordinateur.
- Pourquoi me demandez-vous d'inscrire mon courriel personnel.
    - Aucune communication ne sera faite à cet endroit par le service TI. Cette demande est pour vous faciliter la tâche, lorsque vous avez oublié votre mot de passe. Il vous sera possible de récupérer votre compte et votre mot de passe via cette adresse courriel personnel et ainsi, éviter des délais de réponse.
- Pourquoi me demandez-vous d'utiliser mon cellulaire personnel ?
    - Ce sont des nouvelles exigences de sécurité demande des assureurs et vérificateurs, le service TI se devait de mettre en place l'authentification multiple facteur pour éviter que quelqu'un, qui a été capable de trouver votre code, puisse se brancher à votre compte.
    - On offre la possibilité d'utiliser une clé AMF, mais on recommande d'utiliser le cellulaire pour éviter des délais si vous avez oublié votre clé AMF ou si elle est brisée. De plus, il est moins probable de perdre ou d'oublier son cellulaire.