Équipe des outils de collaboration du CISSSBSL

GUIDE POUR LA CONFIGURATION DE L'AUTHENTIFICATION MULTIFACTEUR

Mise en contexte

Depuis l'arrivée d'Office 365, il est nécessaire d'ajouter une couche de sécurité supplémentaire à votre compte, en plus de votre mot de passe et de vos questions de sécurité, à l'aide de l'une des trois différentes méthodes d'authentification.

Dès qu'une connexion à votre compte sera effectuée à partir de n'importe quel appareil qui n'est pas connecté au réseau du CISSSBSL (appareil cellulaire ou appareil personnel), une demande d'authentification vous sera envoyée et vous devez l'approuver ou non. Si vous ne l'approuvez pas, le compte sera verrouillé, cliquez **ici** pour les détails (*ou voir la page 13*). Nous vous expliquerons comment configurer une méthode d'authentification à **l'intérieur du CISSSBSL** (*ou voir page 2*) et **à la maison** (*ou voir page 4).*

Des demandes d'authentification vous seront demandées de façon aléatoire, sur chaque appareils utilisés pour les connexions à l'extérieur du CISSSBSL.

VEUILLEZ NOTER qu'une authentification vous sera demandée À CHAQUE FOIS que vous accéderez aux endroits suivants de votre compte de messagerie électronique, et ce, MÊME À L'INTÉRIEUR DU CISSSBSL :

-La section "Informations de sécurité";

-La modification du mot de passe;

-Le système peut également faire des validations ponctuelles, à l'intérieur du CISSSBSL, donc assurez-vous que, dans la mesure du possible, la méthode choisie puisse être utilisée lorsque vous êtes dans les installations du CISSSBSL. **Exemple. :** Privilégier l'appareil cellulaire (que vous avez toujours avec vous) à la tablette personnelle (qui reste à la maison).

Si vous recevez des demandes fréquentes d'authentification à l'intérieur du CISSSBSL, alors que vous n'avez tenté de faire aucune des actions mentionnées précédemment, veuillez communiquer avec l'équipe de soutien aux outils de collaboration en composant le : 1 844 400-2433, option 2.

IMPORTANT

-Il est recommandé d'utiliser le navigateur Microsoft Edge ou Google Chrome pour configurer l'authentification multifacteur sur votre compte ;

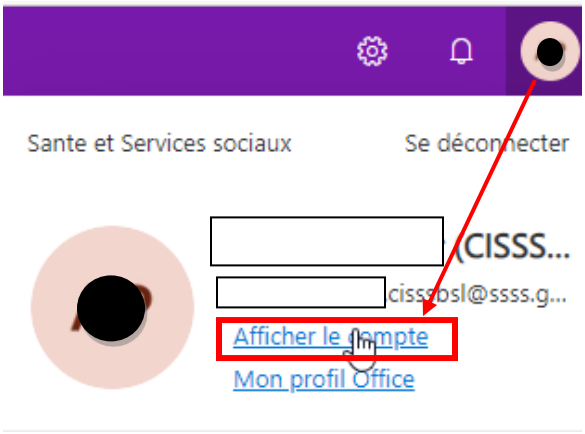
-Vous devez configurer l'authentification multifacteur à partir d'un poste de travail et non sur un appareil mobile (cellulaire, tablette), mais vous aurez probablement besoin d'un de ces 2 appareils pour compléter la configuration;

-Vous ne devrez faire aucune pause durant la configuration, sans quoi vous devrez recommencer le processus. Si cela se produit, vous devrez fermer la fenêtre de navigateur web et recommencer la configuration (voir l'image suivante comme exemple du message d'erreur reçu).

-Vous pouvez, en tout temps, modifier la méthode d'authentification choisie cliquez **ici** pour savoir comment faire (*ou voir la page 14*).

CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR À L'INTÉRIEUR DU RÉSEAU DE LA SANTÉ

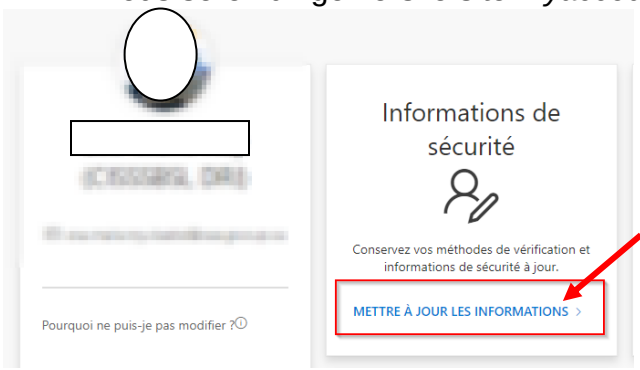
Vous pouvez configurer une méthode authentification à partir de votre compte Outlook **à l'intérieur** du réseau de la santé. La façon de faire est la suivante :



Se connecter à son compte de messagerie électronique Outlook du CISSSBL.

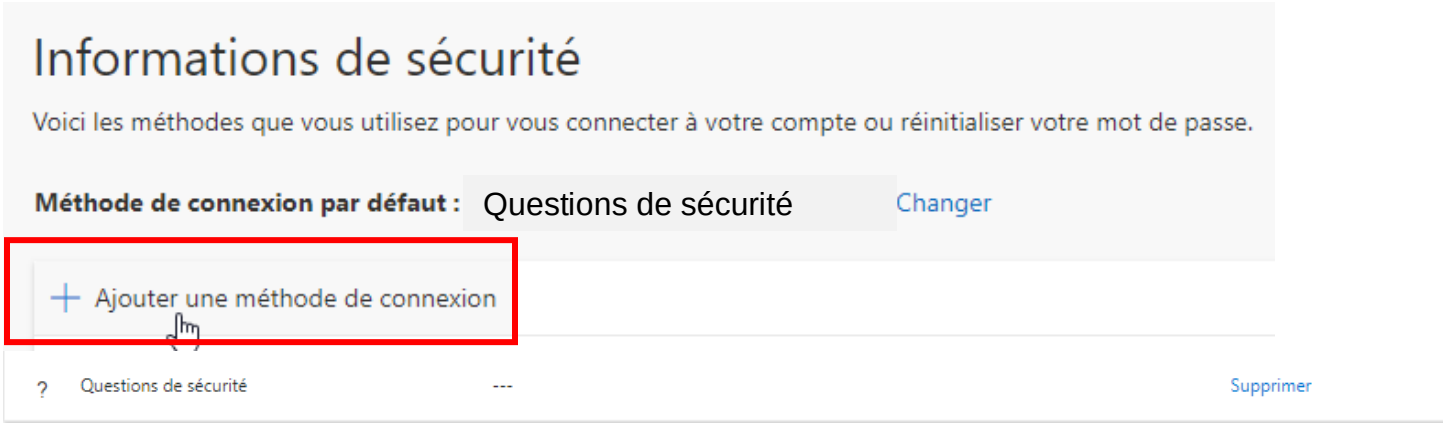
Cliquer sur la pastille contenant vos initiales ou votre photo et sélectionner l'option **« Afficher le compte »**, dans le menu qui s'affichera.

Vous serez dirigé vers le site *myaccount.microsoft.com*.



Pour ajouter l'authentification multifacteur, cliquer sur **« Mettre à jour les informations »** dans la tuile « Informations de sécurité ».

Vous serez dirigez vers la section **« Informations de sécurité »** Pour configurer la méthode d'authentification souhaitée, cliquez sur **« Ajouter une méthode »** et choisir l'option désirée dans le menu déroulant :



Bien que vous possédiez déjà un mot de passe et que vos questions de sécurité sont configurées, vous devez tout de même ajouter une seconde méthode d'authentification.

Voici les trois méthodes d'authentification multifacteur qui s'offrent à vous :

Par SMS (Texto) : Un code est envoyé par SMS sur votre mobile. Vous devez le saisir pour compléter la connexion à votre compte. Vous devez nous contacter si vous changer de numéro et pour modifier votre méthode. (*Méthode simple à utiliser).*

Cliquer ici ou voir la **page 6** pour la configuration.

Téléphone fixe : Un appel téléphonique vous est acheminé et devez confirmer la connexion en suivant les instructions. (*Méthode peu pratique si besoin de mobilité. Elle nécessite d'être présent physiquement près de l'appareil. Donc s'il s'agit du téléphone du domicile et qu'une demande d'authentification à lieu à l'intérieur du CISSSBSL, vous devrez nous appeler pour obtenir de l'aide).*

Cliquer ici ou voir la **page 8**; pour la configuration.

****ATTENTION** - Il est impossible de configurer l'option d'appel téléphonique sur ligne fixe à la maison, à l'intérieur du CISSSBSL, puisque vous devez être présent pour recevoir l'appel de confirmation.**

Application pour appareil mobile : Vous devez installer l'application *Microsoft Authenticator* sur votre appareil mobile. Une demande d'autorisation est envoyée à l'application que vous aurez installée sur votre appareil et vous devez confirmer le tout pour compléter la connexion à votre compte de messagerie. *Vous devez nous contacter si vous changer d'appareil puisque cette méthode est liée à celui-ci. Cette méthode* ***est recommandée aux utilisateurs expérimentés****.*

****Cette méthode d'authentification peut être utilisée sans connexion internet ou réseau cellulaire**.**

Pour utilisateurs expérimentés, cliquer ici ou voir la **page 10**, pour la configuration.

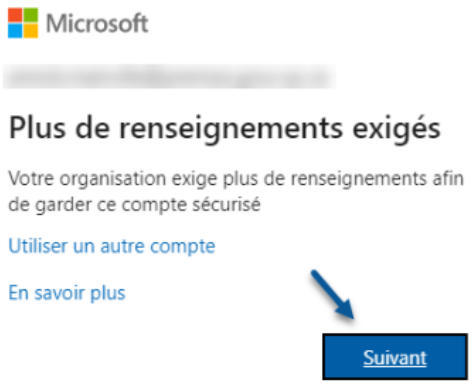
CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR À L'EXTÉRIEUR DU RÉSEAU DE LA SANTÉ

ÉTAPE 1

À l'aide d'un ordinateur et du navigateur **Google Chrome** ou **Microsoft Edge,** se rendre à l'adresse suivante : outlook.office.com.

Lors de votre première connexion à votre compte Outlook, à l'extérieur de l'établissement, vous serez invité à configurer des paramètres supplémentaires avant ou après avoir inscrit votre mot de passe pour vous connecter.

Cette fenêtre apparaîtra et vous devrez cliquer sur **« Suivant »** :



ÉTAPE 2

Bien que vous possédiez déjà un mot de passe et que vos questions de sécurité sont configurées, vous devez tout de même ajouter une seconde méthode d'authentification. Voici les trois méthodes d'authentification multifacteur qui s'offrent à vous :

Par SMS (Texto) : Un code est envoyé par SMS sur votre appareil mobile. Vous devez le saisir pour compléter la connexion à votre compte. *Vous devrez nous contacter si vous changer de numéro et pour modifier votre méthode.* (*Méthode simple à utiliser).*

Cliquer ici ou voir la **page 6** pour la configuration.

Téléphone fixe : Vous recevez un appel téléphonique et devez confirmer la connexion. S'il s'agit du téléphone du domicile et qu'une demande d'authentification a lieu à l'intérieur du CISSSBSL, vous devrez nous appeler pour obtenir de l'aide. (*Méthode peu pratique si besoin de mobilité. Elle nécessite d'être présent physiquement près de l'appareil).*

Cliquer ici ou voir la **page 8**; pour la configuration.

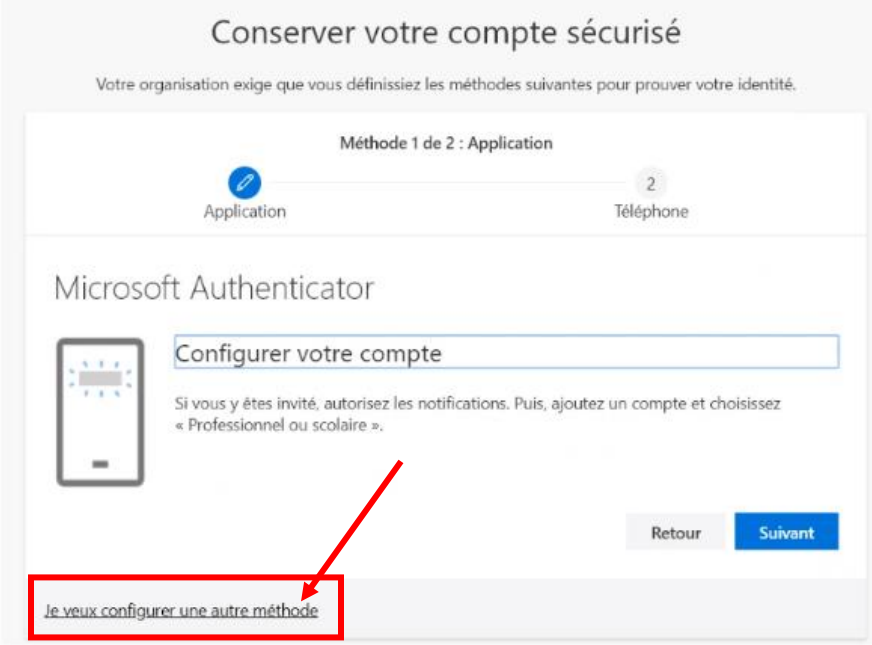
Application pour appareil mobile : Vous devez installer l'application *Microsoft Authenticator* sur votre appareil mobile. Une demande d'autorisation est envoyée à l'application que vous aurez installée sur votre appareil et vous devez confirmer le tout pour compléter la connexion à votre compte de messagerie. Vous devez nous contacter si vous changer d'appareil puisque cette méthode est liée à celui-ci. *(Cette méthode est recommandée aux **utilisateurs expérimentés)**.*

****Cette méthode d'authentification peut être utilisée sans connexion internet ou réseau cellulaire**.**

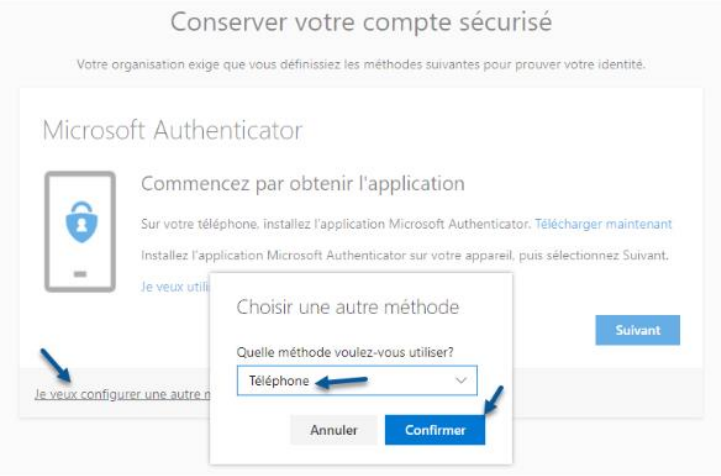
Cliquer ici ou voir la page 10, pour la configuration

COMMENCER LA CONFIGURATION :

Par défaut, le système vous offre l'authentification par l'application *Microsoft Authenticator.* Pour configurer une autre méthode, cliquez sur **« Je veux configurer une autre méthode »**.



CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR PAR SMS (TEXTO)



-Cliquer sur **« Je veux configurer une autre méthode »**.

-Dans la fenêtre qui apparaît, sélectionner **Téléphone**, puis cliquez sur **Confirmer**.

-S'assurer de sélectionner **Canada**, comme pays puisque c'est États-Unis qui est proposé par défaut.

-Inscrire les 10 chiffres de votre numéro de téléphone mobile, sans trait d'union, ni espace.

-Sélectionnez **« Envoyez-moi un code par texto ».**

-Cliquez sur **Suivant**.

À ce moment, vous recevrez un code par SMS (Texto).

-Entrez le code reçu par (Texto).

-Cliquez sur **Suivant**.

Le système confirmera que votre appareil cellulaire a bien été configuré au compte.

Cliquer sur **« Suivant »** pour poursuivre.

Cliquez sur **Terminé**.

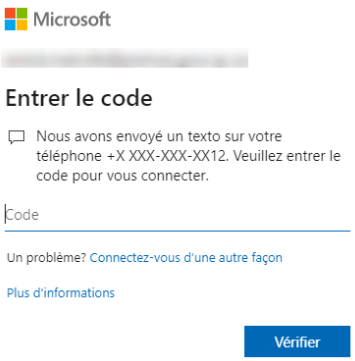
Après la configuration, lorsque qu'une demande d'authentification vous sera envoyée, une fenêtre s'affichera à l'écran vous demandant de choisir si vous souhaitez recevoir **un appel** ou **un texto.** Vous devrez cliquer sur l'option que vous souhaitez utiliser pour que le système vous envoie une demande.

ATTENTION le code reçu n'est valable que quelques minutes.

Notez qu'il est possible, lorsque le signal cellulaire est faible à l'endroit où vous vous trouvez, que receviez pas le code demandé, que vous demandiez à en recevoir un autre et que le premier demandé finisse par être acheminé plusieurs minutes plus tard. Si vous n'arrivez pas à recevoir les codes, vous pouvez essayer d'activer et désactiver le mode avion ou, si ça le fonctionne pas, demander à recevoir un appel pour confirmer votre connexion.

Option « Texto » : Vous recevrez un code par message texte que vous devrez inscrire à l'écran :

**** Notez qu'il peut y avoir des frais supplémentaires si les textos sont restreints dans votre forfait mobile.****

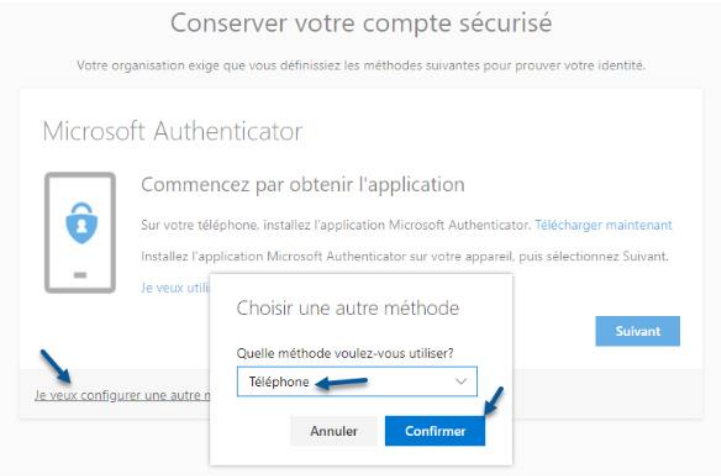


-Entrez le code reçu du mobile dans l'espace désigné;

-Cliquez sur **Vérifier**.

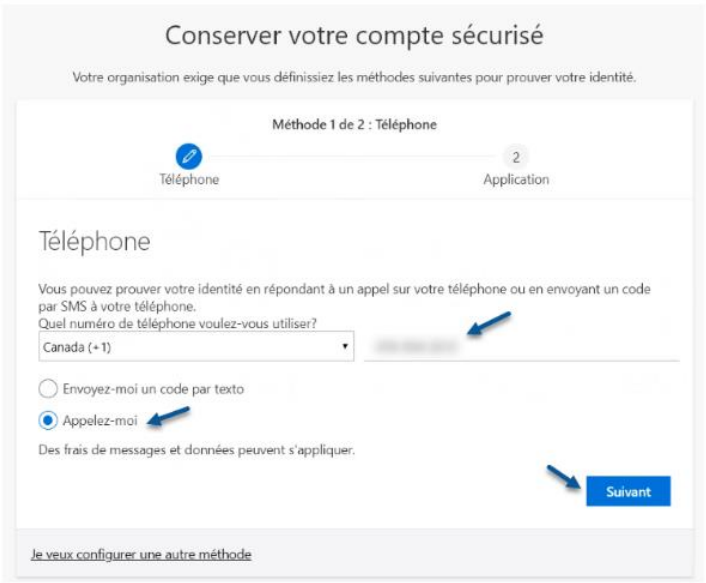
Option « Appel » : Vous recevrez un appel téléphonique enregistré de la part de Microsoft, qui vous demandera de confirmer la demande d'authentification en appuyant sur la touche dièse/carré **#,** et l'accès à votre compte sera accordé.

CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR PAR APPEL TÉLÉPHONIQUE (MOBILE OU FIXE)



-Cliquer sur **« Je veux configurer une autre méthode »**.

-Dans la fenêtre qui apparaît, sélectionner **Téléphone**, puis cliquez sur **Confirmer**.



-S'assurer de sélectionner **Canada**, comme pays puisque c'est États-Unis qui est proposé par défaut;

-Inscrire les 10 chiffres de votre numéro de téléphone, sans trait d'union, ni espac;.

-Sélectionnez **« Appelez-moi »;**

-Cliquez sur **Suivant**.

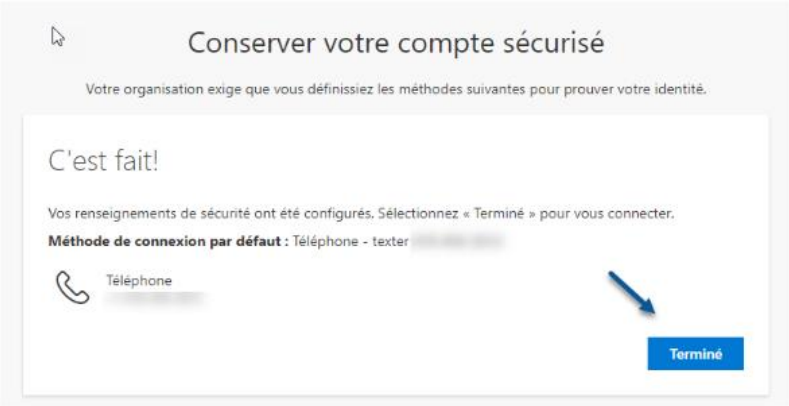
Vous recevrez un appel de Microsoft au numéro que vous avez indiqué. Répondez et suivez les instructions.

On vous demandera de confirmer avec la touche dièse/carré **#,** et ceci validera la configuration.

Le système confirmera que votre appareil cellulaire a bien été configuré au compte.

Cliquer sur **« Suivant »** pour poursuivre.

Cliquez sur **Terminé**.



Après la configuration, lorsque qu'une demande d'authentification vous sera envoyée, une fenêtre s'affichera à l'écran, vous demandant de choisir si vous souhaitez recevoir **un appel** ou **un texto**. Vous devrez cliquer sur **« appel »** :

Vous recevrez un appel téléphonique enregistré de la part de Microsoft, qui vous demandera de confirmer la demande d'authentification en appuyant sur le carré # et l'accès à votre compte vous sera accordé.

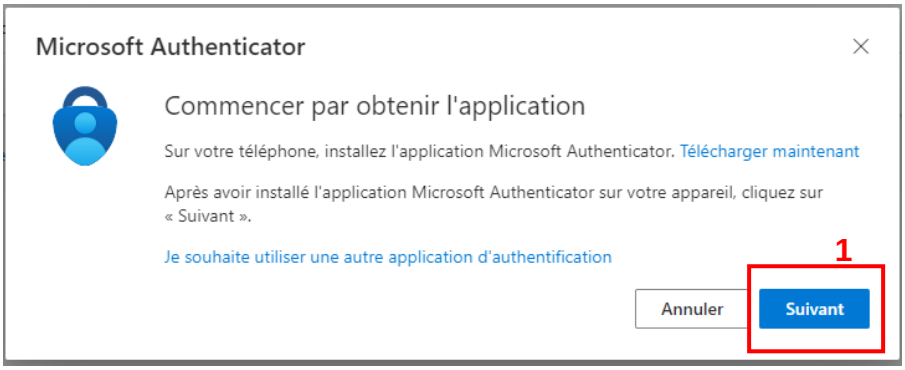
**** Notez qu'il peut y avoir des frais d'interurbains selon votre forfait de téléphonie.****

CONFIGURER L'AUTHENTIFICATION MULTIFACTEUR À PARTIR DE L'APPLICATION AUTHENTICATOR SUR UN APPAREIL MOBILE

Par défaut, on vous offre l'authentification par l'application *Microsoft Authenticator.* Par contre, **nous recommandons son utilisation *aux utilisateurs expérimentés.***

****Il est important de suivre les étapes dans l'ordre et sans pause. Nous vous suggérons donc de lire complétement la marche à suivre avant de procéder à la configuration de cette méthode.****

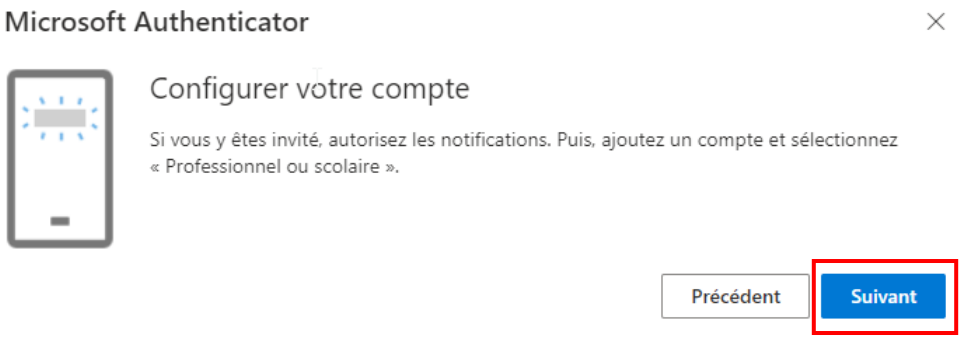
- Le système vous demandera de télécharger **sur votre appareil mobile** l'application *Microsoft Authenticator* par le biais de *l'App Store* ou de *Google Play Store;*



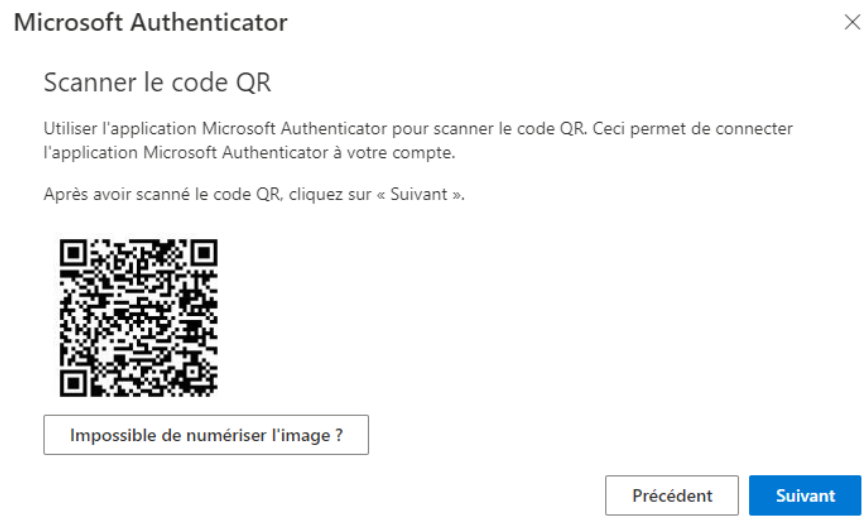
Une fois l'application installée et ouverte sur votre appareil mobile : **Cliquez sur 1- « Suivant » sur le poste de travail** avant de continuer. Une nouvelle fenêtre apparaîtra à l'écran vous demandant de poursuivre la configuration sur l'appareil.

Sur l'appareil mobile : Au démarrage de l'application, « Microsoft respecte votre vie privée », vous devez sélectionner **« J'accepte »**

Sur le poste de travail : Cliquer ensuite sur **« Suivant »** dans la fenêtre présente à l'écran (*voir image précédente*), sur le poste de travail.

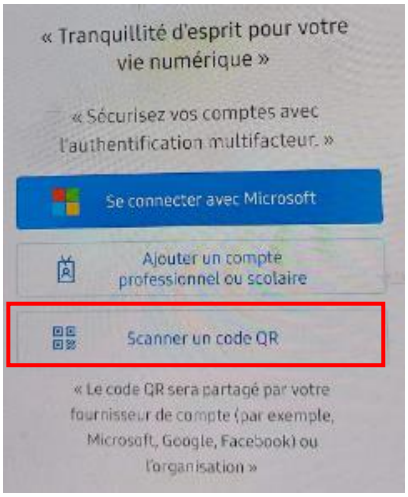


Une fenêtre apparaîtra vous demandant de scanner un code QR.



Sur l'appareil mobile :

-Choisir l'option « Scanner un code QR »

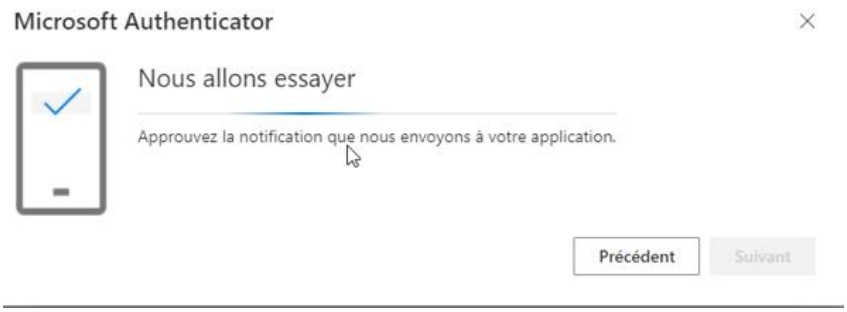


-Vous devrez ensuite autoriser l'application à prendre des photos et à enregistrer des vidéos en choisissant l'option : « Lorsque vous utiliser l'application ».

Dirigez la caméra de votre appareil mobile vers le code QR présent à l'écran de votre poste de travail.

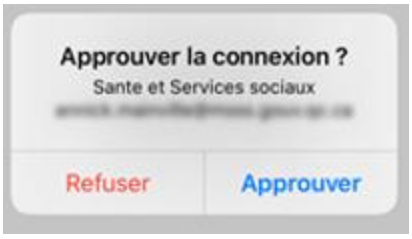
Dès que le code sera scanné avec succès, vous aurez une confirmation sur votre appareil mobile que votre compte à bien été ajouté et pourrez appuyer sur le bouton « Et voilà » qui sera affiché à l'écran.

Poste de travail : Une fenêtre apparaîtra à l'écran vous disant que le système va essayer d'envoyer une demande d'authentification à l'application que vous venez d'installer sur votre appareil mobile.



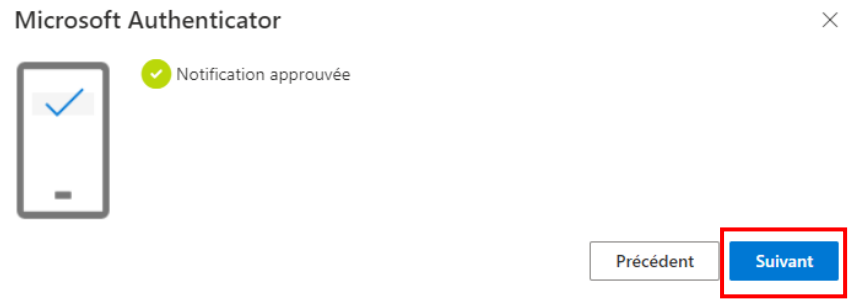
Sur l'appareil mobile :

Vous serez invité à approuver ou refuser la demande, vous devrez donc choisir **« Approuver ».**



Sur le poste de travail :

Cette fenêtre s'affichera pour confirmer que la configuration s'est complétée avec succès.



Vous pouvez cliquer sur suivant pour terminer l'opération.

Les demandes d'authentifications futures se passeront de la même façon. Une notification s'affichera à l'écran du poste de travail vous avisant qu'une demande a été envoyée à votre application. Vous devrez **« Approuver »** la demande sur votre appareil mobile et aurez ensuite accès à votre compte de messagerie électronique.

VOUS AVEZ REÇU UNE DEMANDE D'AUTHENTIFICATION NON SOLLICITÉE

Vous devez **REFUSER** la demande d'authentification si :

- Vous n'avez **PAS** tenté de vous connecter à votre compte ;

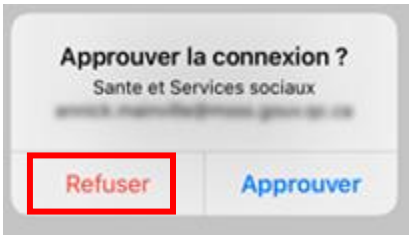
- Vous n'avez **PAS** tenté de modifier votre mot de passe Outlook ;

- Vous n'avez **PAS** tenté d'utiliser TEAMS **ou** d'ouvrir un document Office 365 dans l'application installée sur votre poste de travail.

Si vous avez reçu un texto : Ne répondez pas au texto.

Si vous avez reçu un appel de Microsoft : Raccrochez sans faire le dièse/carré #.

Si vous avez reçu une demande de l'application *Microsoft Authenticator* : Appuyez sur **Refuser** à la demande d'approbation reçue sur votre appareil mobile.



PAR CONTRE, le fait de cliquer **Refuser** une demande d'approbation de connexion, fera apparaître un message vous informant que votre compte a été bloqué et c'est tout à fait **normal**.

Ceci déclenche le processus de compte compromis au Ministère et la prise en charge est rapide.

Notez que dans le cas des codes par texto, si vous n'en recevez pas et demandez à en recevoir un autre, que le premier demandé finisse par être acheminé plusieurs minutes plus tard. Il ne s'agirait donc pas d'une demande « non sollicitée », mais plutôt d'un retard d'acheminement. Cela arrive parfois si le signal cellulaire est plus faible à l'endroit où vous vous trouvez.

Si vous recevez une demande d'authentification **NON sollicitée,** communiquez avec l'équipe des outils de collaboration du CISSSBSL en composant le : 1 844 400-2433, option 2

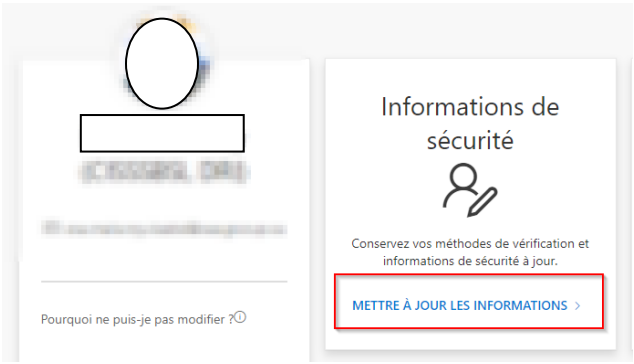
COMMENT MODIFIER LA METHODE D'AUTHENTIFICATION

Vous pouvez configurer votre authentification à partir de votre compte Outlook **à l'intérieur** du réseau de la santé. La procédure est la suivante :

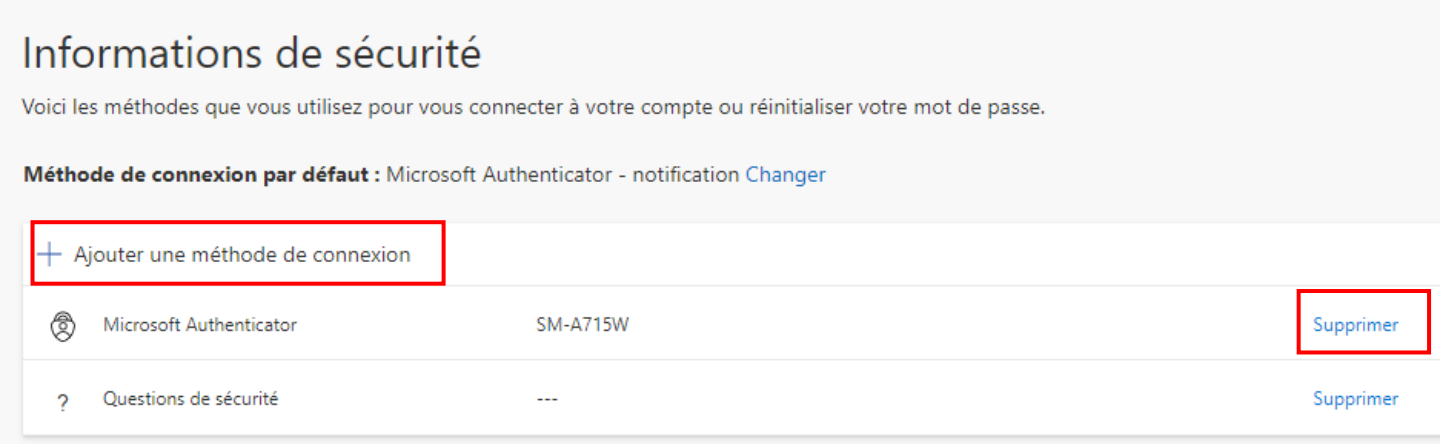
Connectez-vous normalement avec votre compte de messagerie électronique Outlook;

Dans le menu de droite se trouvant sous la pastille contenant vos initiales, sélectionnez « Afficher le compte ».

Vous serez dirigé vers le site *myaccount.microsoft.com*. Pour ajouter l'authentification multifacteur, vous devez cliquer sur **« Mettre à jour les informations »** dans la case « Informations de sécurité ».



Dans la fenêtre **« Informations de sécurité »**, vous verrez normalement que vos questions de sécurité sont considérées comme méthode de connexion par défaut;



Commencer par supprimer la méthode que vous ne souhaitez plus utiliser et ensuite cliquer sur « + Ajouter une méthode de connexion » pour choisir une nouvelle méthode.

ATTENTION si vous supprimez la **méthode « Microsoft Authenticator », n'oubliez pas de supprimer également l'application de votre appareil mobile AVANT** de configurer une nouvelle méthode.