HELMo
Haute Ecole
Libre Mosane

Mes identifiants

Toutes les informations entourant vos identifiants HELMo sont reprises ici.

Obtenir mes identifiants lors de mon arrivée à HELMo

Comment obtenir mes identifiants numériques lors de mon arrivée à HELMo?

Pour les nouveaux étudiants

Après la validation de votre inscription et le paiement de votre acompte d'inscription, vous recevrez automatiquement vos identifiants HELMo et Microsoft sur l'adresse e-mail privée que mentionnée lors de votre inscription.

L'envoi des identifiant peut prendre jusqu'à 24h. Si vous payez vos frais d'inscription par virement bancaire, un délai de plusieurs jours peut s'ajouter ; ce délai comprend la réception de votre paiement, son traitement par le service financier et le traitement par le système informatique.

En cas de problème, adressez vous directement au secrétariat de votre institut.

Pour les nouveaux membres du personnel

Après la signature de votre contrat, vous obtiendrez vos identifiants HELMo et Microsoft auprès de la personne relai de votre institut.

Quelle est la durée de validité de mes identifiants HELMo?

Vos identifiants HELMo et Microsoft sont valides tout au long de votre cursus ou de la durée de votre contrat.

Hors circonstance particulière, vos identifiants HELMo et Microsoft **restent valides 6 mois* après la fin de votre cursus ou de votre contrat** afin de vous laisser le temps nécessaire pour récupérer vos données telles que vos fichiers, e-mails et attestations. Passé ce délai, votre compte sera automatiquement et définitivement désactivé ; plusieurs notifications vous parviendront pour vous en avertir.

* Certaines licences spécifiques seront désactivées avec effet immédiat.

Attention aux spams : soyez vigilant, nous ne vous demanderont **jamais** de confirmer quoi que ce soit à propos de votre compte ou d'éviter une prétendue suppression en cliquant sur un lien reçu par e-mail.
En cas de doute sur la légitimité d'un e-mail, vérifiez ou contactez le service informatique.

Mot de passe perdu et problèmes de MFA

Lisez ceci pour éviter le blocage de votre compte après un changement de mot de passe :
Que faut-il faire impérativement après avoir changé de mot de passe HELMo ?

01

02

J'ai perdu mon mot de passe HELMo et/ou Microsoft

Obtenir un nouveau mot de passe en ligne

Pour récupérer un nouveau mot de passe de manière autonome en cas de perte, vous devez renseigner un certain nombre de prérequis.

Prérequis si vous êtes membre du personnel :

- Vous devez posséder un contrat de travail en cours d'exécution afin que votre compte HELMo soit actif.
- Vous devez préalablement avoir renseigné une adresse e-mail privée pour permettre à nos services de vous envoyer un lien éphémère pour la création d'un nouveau mot de passe. Les membres du personnel peuvent renseigner cette donnée auprès du service des ressources humaines.

Prérequis si vous êtes étudiant :

- Vous devez posséder une inscription valide à un cursus HELMo
- Vous devez préalablement avoir renseigné une adresse e-mail privée pour permettre à nos services de vous envoyer un lien éphémère pour la création d'un nouveau mot de passe. Les étudiants peuvent renseigner cette donnée auprès du secrétariat de leur institut.

Procédure de réinitialisation de votre mot de passe :

Si vous rencontrez les prérequis énumérés ci-dessus, en cas de perte de votre mot de passe HELMo ou Microsoft, vous pouvez en définir un nouveau en vous rendant sur cette page : https://mon-espace.helmo.be/MotDePassePerdu/DemandeModifierMotDePasse

Obtenir un nouveau mot de passe en institut

Le helpdesk informatique ne transmet pas de nouveau mot de passe.

Pour obtenir un nouveau mot de passe dans le cas où la récupération de mot de passe en ligne ne fonctionne pas, vous devez rencontrer une personne référente de façon à ce qu'elle puisse vous identifier et procéder au changement de mot de passe.

Les étudiants doivent s'adresser directement au secrétariat de leur institut.

Les membres du personnel peuvent s'adresser à la personne relai sur site.

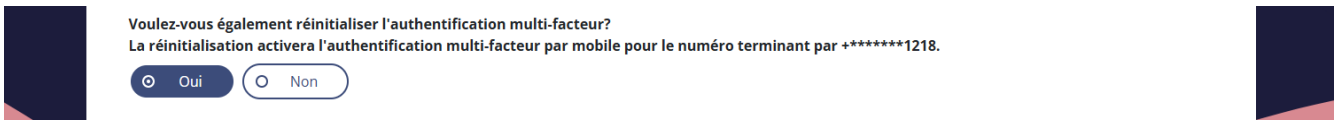
Je souhaite changer mon mot de passe HELMo et/ou Microsoft

Vous avez la possibilité de modifier votre mot de passe HELMo via le bouton "Mot de passe et sécurité" dans votre menu personnel sur la plateforme Mon Espace, soit directement via ce lien : https://mon-espace.helmo.be/ChangementMotDePasse/Employe/Index

J'ai perdu mon moyen d'authentification multi-facteurs (MFA) Microsoft

Si vous perdez l'application ou l'appareil qui vous permet de vous authentifier avec votre compte Microsoft, suivez la procédure **"J'ai perdu mon mot de passe HELMo et/ou Microsoft"** ci-dessus pour débloquer votre compte.

Lors de cette procédure, après la réception de l'e-mail de réinitialisation de votre mot de passe, une option vous permettra de réinitialiser votre MFA :



Par mesure de sécurité, la réinitialisation du mot de passe est obligatoire lors de la réinitialisation du MFA.

Votre MFA sera réinitialisé avec les données que vous avez fournies au secrétariat lors de votre inscription ou au service du personnel lors de la signature de votre contrat. Si ces données ne sont plus à jour, veuillez les contacter.

Mauvais numéro de téléphone lié à mon compte Microsoft

le numéro de téléphone lié a votre compte Microsoft est le numéro que vous avez donné a l'administration de la Haute École lors de votre arrivée. Vous pouvez le consulter sur la page de votre profil dans mon espace.

Si le numéro de téléphone lié au compte Microsoft n'est pas ou plus correct, il est nécessaire de demander de le modifier.

- **Les étudiants** doivent s'adresser directement au secrétariat de leur institut.
- **Les membres du personnel** peuvent s'adresser à la personne relai sur site.

Pour des raisons de sécurité, il est impératif de se présenter physiquement, toute demande de modification de numéro de téléphone par mail ou téléphone sera refusée.

Une fois le numéro modifié, vous pouvez directement réinitialiser votre mot de passe en prenant soins de cocher les deux options suivantes :

    - "Oui" pour la réinitialisation du multi-facteur
    - "Oui" pour la modification du mot de passe Microsoft

Le compte sera alors directement opérationnel, et le code de double authentification sera envoyé au nouveau numéro de téléphone.

Le numéro de téléphone affiché dans le profile peut prendre 24h à se mettre à jour.

Comment configurer l'authentification à facteurs multiples

01 Introduction

L'activation de l'authentification à facteurs multiples (MFA) est une recommandation courante de Microsoft pour la protection des comptes. L'objectif est de rendre encore plus difficile l'usurpation de comptes Microsoft.

Le fonctionnement est simple, lors de la connexion au compte, il faut entrer son adresse mail, son mot de passe et un code unique obtenu par un autre moyen (via une application spécifique sur le smartphone ou via un SMS par exemple). Cette étape supplémentaire n'est pas systématiquement nécessaire : en effet, lorsque vous utilisez vos appareils habituels, la vérification est effectuée une seule fois au début et n'est plus redemandée que tous les 60 jours.

Par contre, la connexion à votre compte Microsoft depuis un nouveau périphérique nécessite la validation en encodant le code supplémentaire obtenu.

Prérequis

La méthode d'authentification supplémentaire que le service informatique vous conseille est l'utilisation d'**une application d'authentification** comme Google Authenticator, Microsoft Authenticator ou Authy.

Si **vous disposez déjà d'une telle application**, vous pouvez passer à l'étape Configuration ci-dessous, nous ajouterons le compte HELMo directement dans votre application préexistante.

Si **vous ne disposez pas de ces applications**, nous vous conseillons d'installer Microsoft Authenticator qui est disponible sur Android (Play Store) et Apple (App Store).

Android

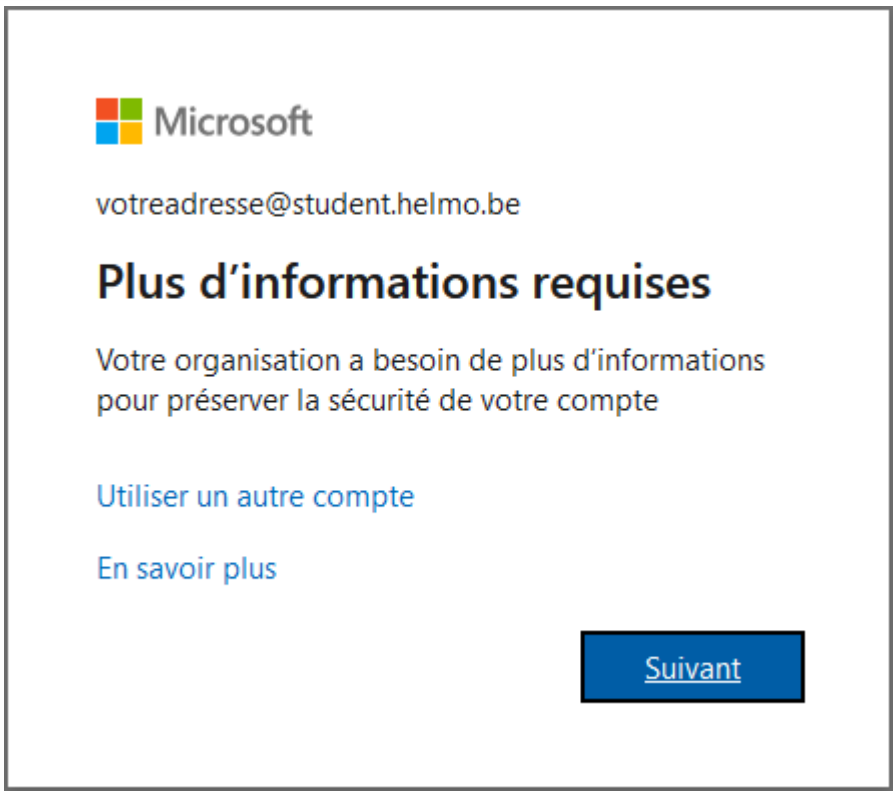
Apple

go.microsoft.com/fwlink/p/?LinkId=722778 go.microsoft.com/fwlink/p/?LinkId=722779

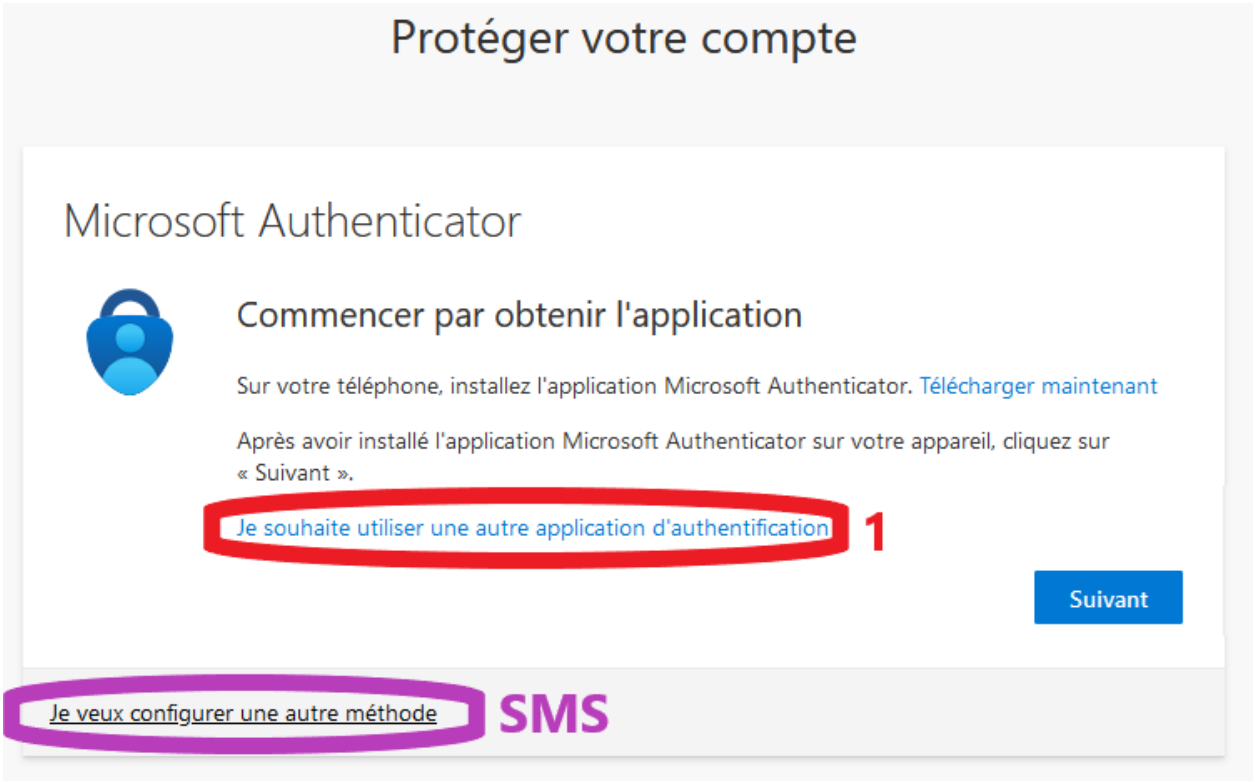
Configuration

Nous procédons aux activations MFA par étape. A un moment donné, la connexion à votre compte Microsoft nécessitera d'accomplir les étapes suivantes :

1. Apparition de la fenêtre suivante :

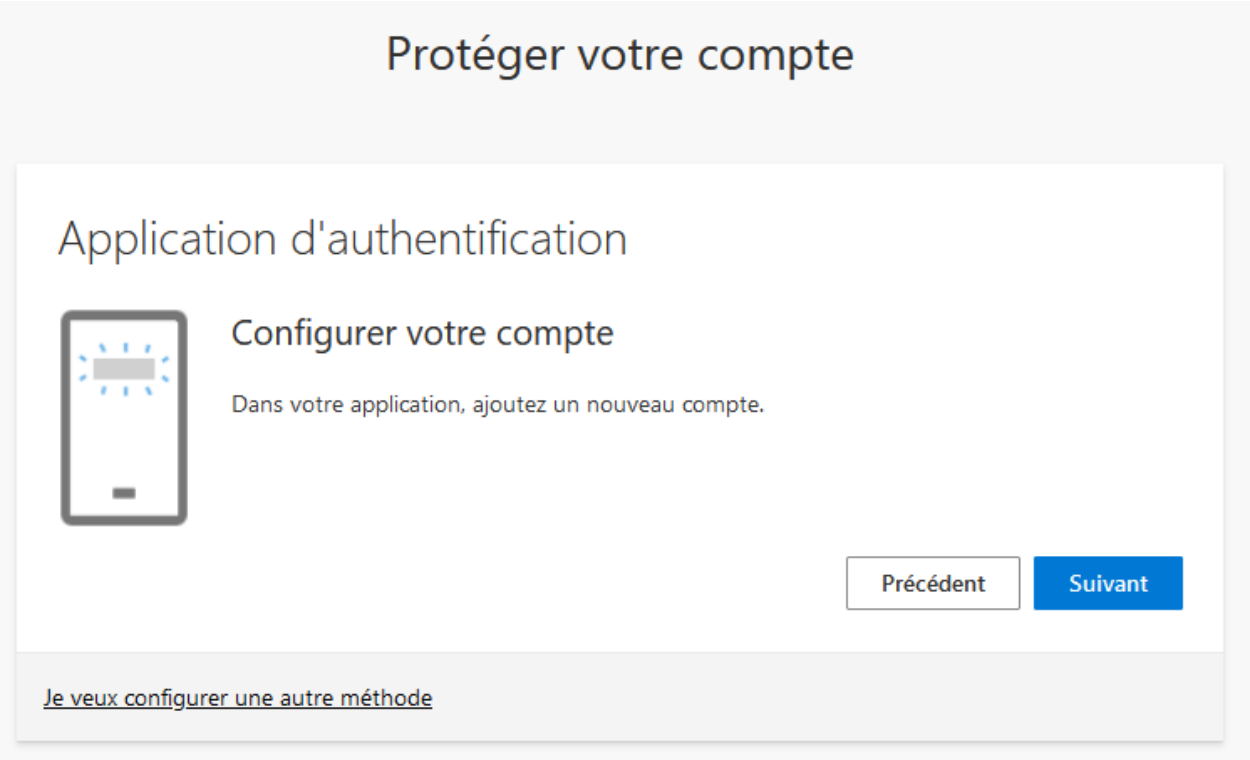


1. En cliquant sur « Suivant », la fenêtre suivante apparaît :



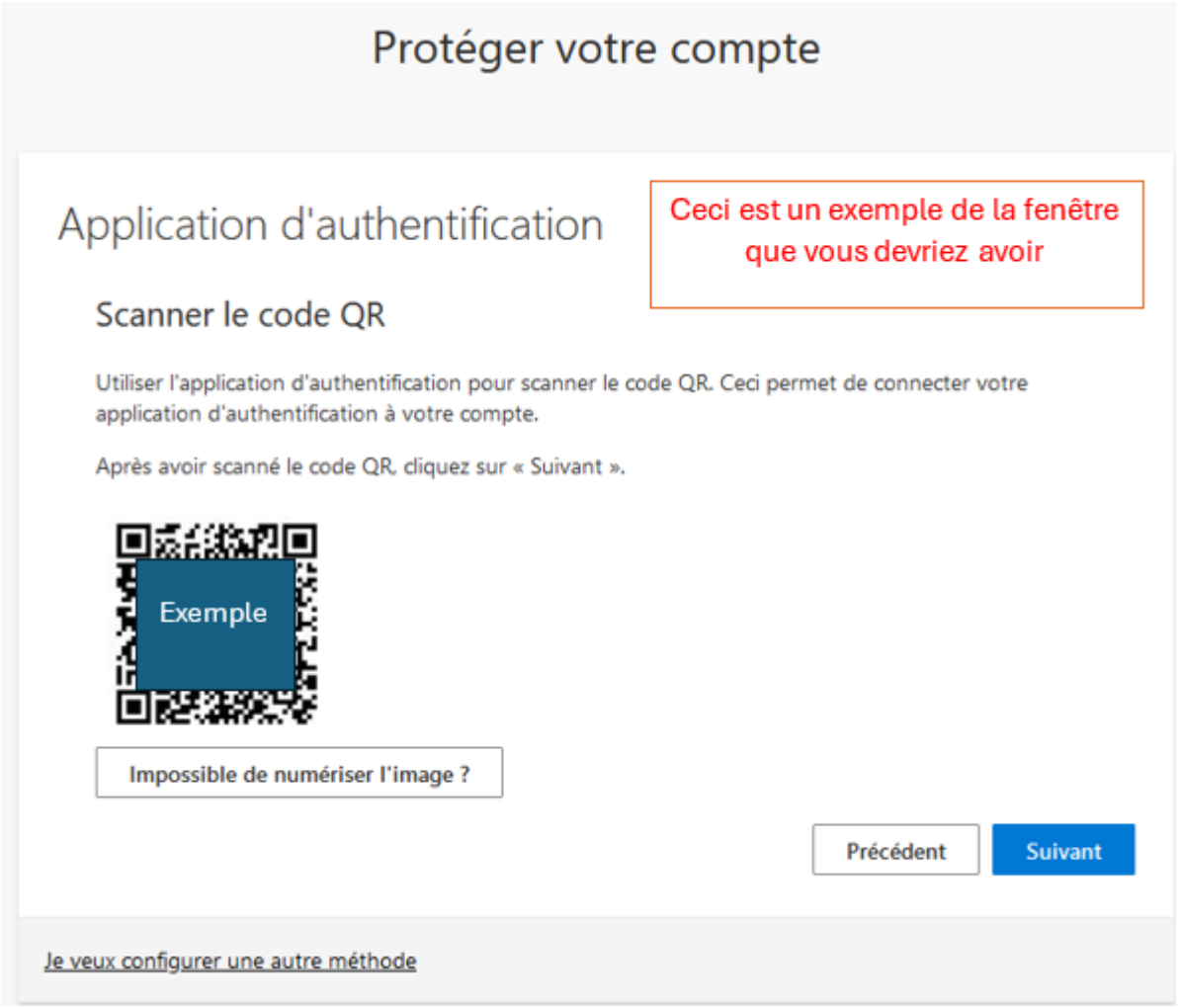
Si vous avez installé une application d'authentification, vous pouvez cliquer sur le lien mentionné « Je souhaite utiliser une autre application d'authentification » (qui fonctionne pour Microsoft Authenticator, Google Authenticator, ...). Si vous ne disposez pas d'un smartphone, il est possible d'encoder votre numéro de téléphone pour recevoir un code par SMS.

1. La fenêtre suivante apparaît alors :



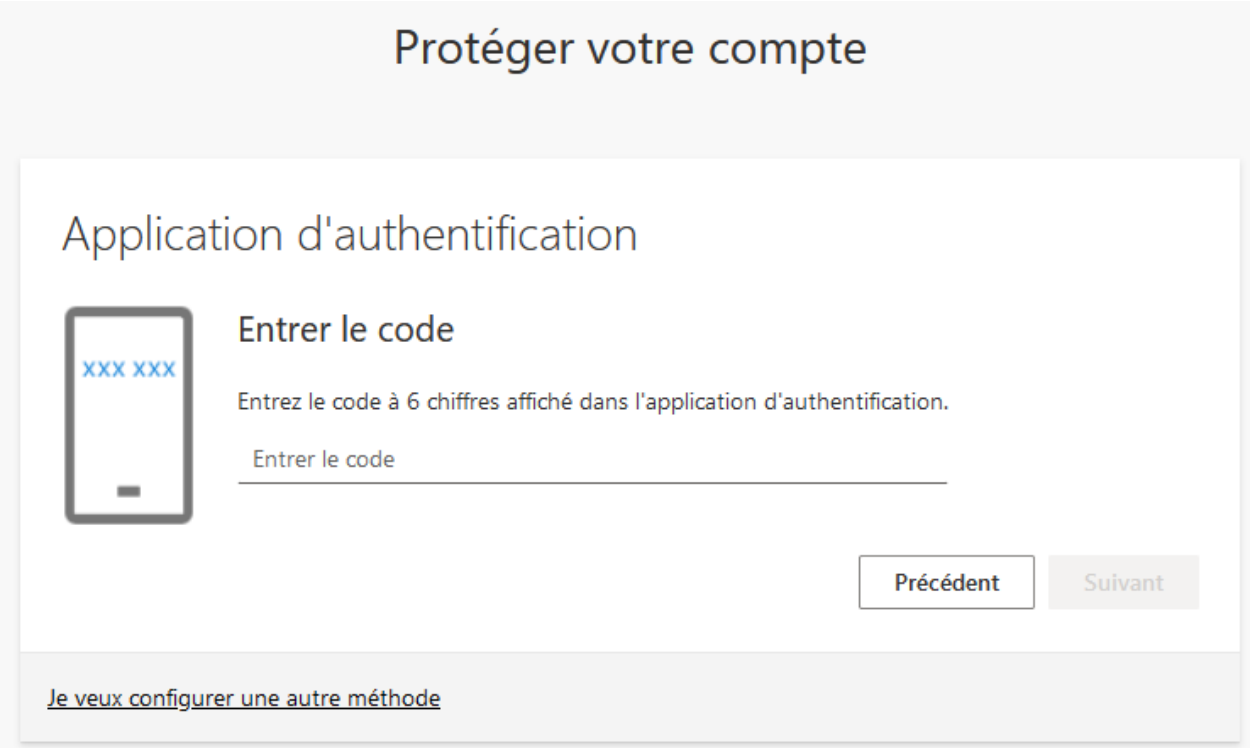
Il faut alors simplement cliquer sur Suivant

1. Le code QR apparaît sur la fenêtre suivante :



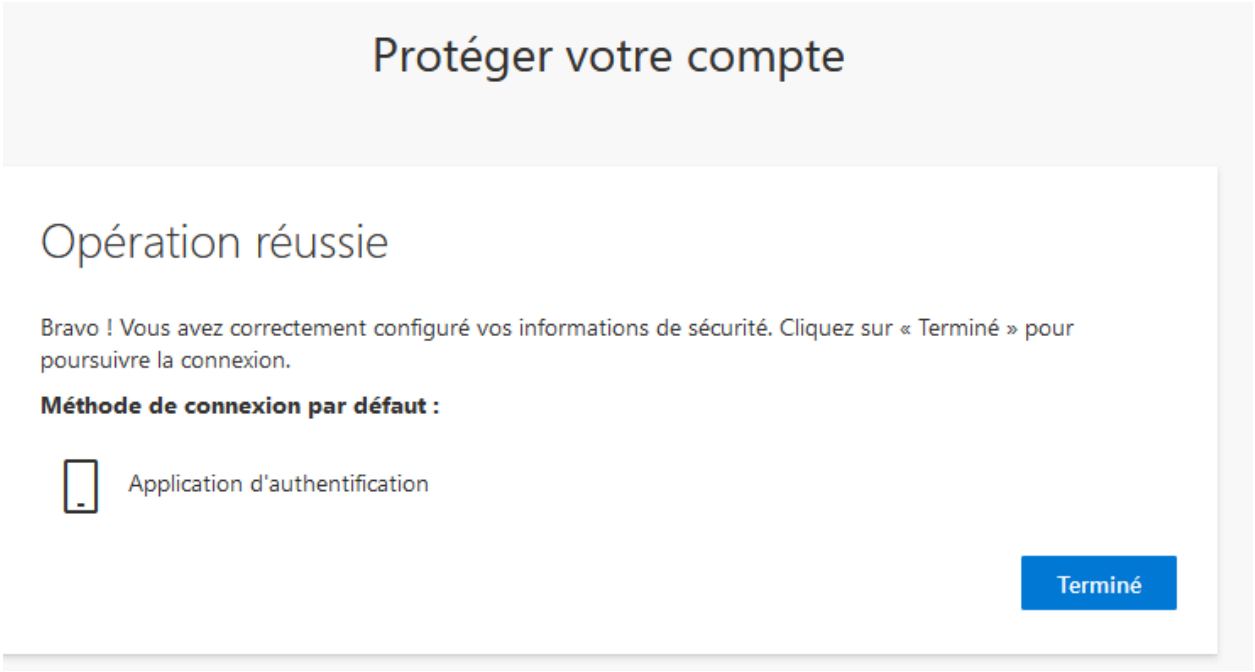
Il faut, ouvrir l'application d'authentification, et dans celle-ci, ajouter un compte (personnel s'il est demandé) et choisir Scanner un code QR. Présentez ensuite l'appareil photo de votre téléphone en regard de ce code. Cela provoquera automatiquement l'ajout du code dans l'application.

1. Etape de validation, la fenêtre suivante apparaît :



Dans votre application d'authentification, si le code de 6 chiffres ne s'affiche pas directement, choisissez le compte ajouté et le code apparaîtra. Il faut entrer le code dans l'interface pour valider le l'installation est bien fonctionnelle.

1. La configuration est alors terminée



Erreurs pendant ou après l'authentification

Retrouvez ici les erreurs d'authentification les plus récurrentes ainsi que les solutions pour les résoudre.

Erreur "Bad Request - Request Too Long" après authentification

Il est possible que vous rencontriez le message d'erreur suivant après l'authentification sur l'une de nos plateforme :

```
Bad Request – Request Too Long
HTTP Error 400. The size of the request headers is too long.
```

Ce message survient lorsque votre cookie de session dépasse la taille maximale autorisée. Cela peut être consécutif d'une mise à jour sur la plateforme ou d'un problème lors du nettoyage des cookies par le navigateur.

Pour corriger ce problème, nous vous recommandons de supprimer les cookies faisant références aux sites HELMo suivants :
- mon-espace.helmo.be
- sso1.helmo.be

Erreur "FatalProfileException" après l'authentification

Il arrive que vous rencontriez le message ci-dessous en tentant de vous authentifier sur une plateforme HELMo. **Ce message indique que votre réseau est configuré pour utiliser plusieurs adresses IP différentes lorsque vous naviguez sur internet.** Cette règle peu commune peut être configurée au niveau de votre fournisseur d'accès, au niveau du réseau de l'établissement dans lequel vous vous trouvez ou encore tout simplement au niveau du périphérique que vous utilisez pour vous connecter.

Par sécurité, notre système d'authentification bloque l'utilisation d'adresses multiples lors du processus d'authentification car elle peut être liée à une attaque informatique. Il est possible qu'un tiers tente d'usurper votre identité en interceptant vos requêtes Web et en les substituant par les siennes.

Pour résoudre le problème, il faut d'abord en identifier la provenance. Commencez par lancer une analyse anti-virus. Essayez ensuite de vous connecter avec un autre périphérique, ou avec le même périphérique depuis un autre réseau. Une fois que vous avez identifié la source du problème, tentez de savoir pourquoi cette règle est configurée et si c'est pertinent dans votre cas. Si ça ne l'est pas, il vaut mieux la désactiver. Dans le cas contraire, il faudra vous connecter à nos services depuis une autre source pour contourner le problème.

Le message d'erreur :

```
opensaml::FatalProfileException
```

```
The system encountered an error at Wed Jun 06 18:02:10 2018
To report this problem, please contact the site administrator at helpdesk@he

Please include the following message in any email:
opensaml::FatalProfileException at (https://www.helmo.be/Shibboleth.sso/SAML

Your client's current address (***.***.***.***) differs from the one used wh
```

Parfois, je peux m'identifier et parfois cela ne fonctionne pas : blocage temporaire du compte

Pour des raisons de sécurité, nos systèmes bloquent automatiquement les comptes des utilisateurs lorsque plusieurs tentatives de connexion (au wifi, VPN, ou site HELMo) avec un mauvais mot de passe surviennent.

Les règles appliquées sont les suivantes : si j'effectue **5** tentatives de connexion infructueuses dans une période de **10** minutes, mon compte **sera bloqué automatiquement pour plusieurs minutes**.

Les conséquences du blocage sont :

- impossibilité de me connecter au Wifi.
- impossibilité de me connecter à Learn,
- impossibilité de me connecter à HELMo Connect,
- impossibilité d'utiliser l'application HELMo,
- impossibilité de me connecter en VPN (si une telle connexion est fournie par mon institut),

Attention si vous avez changé votre mot de passe HELMo :

Que faut-il faire impérativement après avoir changé de mot de passe HELMo ?

01

02

Que faut-il faire impérativement après avoir changé de mot de passe HELMo ?

Attention : si vous avez changé votre mot de passe HELMo il est impératif de lire ceci pour éviter le blocage de votre compte !

Pour des raisons de sécurité, nos systèmes bloquent automatiquement les comptes des utilisateurs lorsque plusieurs tentatives de connexion (au Wifi, VPN, ou site HELMo) avec un mauvais mot de passe surviennent.

Les règles appliquées sont les suivantes : si j'effectue **5** tentatives de connexion infructueuses dans une période de **10** minutes, mon compte **sera bloqué automatiquement pour plusieurs minutes**.

Les conséquences du blocage sont :

- impossibilité de me connecter au Wifi.
- impossibilité de me connecter à Learn,
- impossibilité de me connecter à HELMo Connect,
- impossibilité d'utiliser l'application HELMo,
- impossibilité de me connecter en VPN (si une telle connexion est fournie par mon institut),

Si vous avez modifié votre mot de passe et qu'un portable (téléphone ou ordinateur) tente de se connecter automatiquement avec l'ancien mot de passe, **il est probablement la cause du blocage de votre compte**.

Il faut, dans ce cas, réinitialiser les profils Wifi sur vos appareils mobiles (téléphone et portable). Si vous utilisez l'application HELMo, il faut également se reconnecter.

- Pour supprimer le **profil wifi sous Windows**, vous pouvez consulter la vidéo suivante.
- Pour supprimer le **profil wifi sous MacOS**, vous pouvez consulter la vidéo suivante.
- Pour supprimer le **profil wifi sous Android**, vous pouvez consulter la vidéo suivante.

Garder mes identifiants en sécurité

Des conseils pour garder vos identifiants en sécurité et réagir de façon adéquate en cas de piratage.

Identifiez les sites Web frauduleux

Les tentatives de vol de vos informations personnelles sont nombreuses. Que ce soit par e-mail ou via d'autres canaux, il est important de pouvoir différencier rapidement les sites Web légitimes des sites Web frauduleux.

La règle de base est de ne **jamais entrer votre mot de passe HELMo si ces conditions ne sont pas toutes rencontrées :**

- L'adresse de la page Web se termine exactement par **".helmo.be" ou"login.microsoftonline.com"**
  exemples: sso1.helmo.be, www.helmo.be, learn.helmo.be, webmail.helmo.be...
- La page Web utilise **https** et non http et possède un certificat https valide au nom de la Haute Ecole

Une importante quantité de liens frauduleux transitent par messages SPAM, il est important d'apprendre à reconnaitre et se prémunir des tentatives d'hameçonnage pour garder vos identifiants en sécurité.

Si vous pensez avoir entré votre mot de passe sur un site frauduleux veuillez changer votre mot de passe sans tarder.

Utilisez un gestionnaire de mot de passe éprouvé

Nous utilisons tous de nombreux services en ligne : messagerie, banque, réseaux sociaux, outils professionnels... Pour garantir la sécurité de vos comptes, il est essentiel de suivre ces **bonnes pratiques** :

- Générez un mot de passe **long, complexe et unique** pour chaque service
- Changez régulièrement vos mots de passe les plus sensibles
- Changez immédiatement un mot de passe dont vous suspectez qu'il pourrait être compromis

Utiliser un gestionnaire de mot de passe est essentiel pour suivre les meilleurs pratiques de sécurité sans compliquer les choses. Ces logiciels vous permettent de générer, organiser et stocker vos mots de passes, certains prennent aussi en charge l'authentification multifacteur.

Avec un gestionnaire de mots de passe, vos identifiants sont stockés dans un conteneur sécurisé, lui-même protégé par une combinaison de moyens forts (certificat, mot de passe,...).

Comment choisir un gestionnaire de mots de passe ?

Parmi les solutions les plus réputées, **KeePass** est un logiciel gratuit, open-source et certifié par de nombreuses organisations sérieuses. Il vous permet de :

- Générer des mots de passe complexes et aléatoires
- Les stocker de manière sécurisée dans un coffre-fort chiffré
- Y accéder facilement à l'aide d'un mot de passe maître unique

Il existe de nombreuses solutions similaires à KeePass. Préférez toujours une solution open-source certifiée.

Utilisez l'authentification multifacteur partout

Les mots de passe, même solides, ne suffisent plus à garantir une sécurité complète. En cas de fuite, vos comptes peuvent être exposés. C'est pourquoi il est essentiel d'activer l'**authentification multifacteur (MFA)** dès que possible.

Qu'est-ce que le MFA ?

L'authentification multifacteur ajoute une étape supplémentaire à la connexion. En plus de votre mot de passe, vous devrez valider votre identité via un **code temporaire** reçu par SMS, email, ou généré par une application comme **Microsoft Authenticator**, **Google Authenticator**, ou **Authy**.

Pourquoi l'utiliser ?

- Si votre mot de passe est volé, un pirate **ne pourra pas accéder** à votre compte sans le second facteur.
- Le MFA bloque **la majorité des tentatives de piratage**, même en cas de mot de passe compromis.
- De nombreux services en ligne proposent cette option gratuitement.

Où l'activer ?

Activez le MFA **partout où c'est possible** : messagerie, réseaux sociaux, comptes professionnels, plateformes de cloud, banques, etc. Cela ne prend que quelques minutes, mais peut vous éviter de gros problèmes. A HELMo, l'authentification multifacteur est obligatoire et activée par défaut.

Vérifiez la fiabilité de vos mots de passe

Il existe toujours un risque que les plateformes sur lesquelles vous possédez un compte subissent un vol de données suite à une attaque informatique. Ce risque n'épargne pas les plateformes les plus connues comme Adobe ou Dropbox.

Lorsqu'un attaquant parvient à voler des données confidentielles, il pourra tenter de les vendre sur des sites illégaux. Après un certain temps, ces données feront surface sur d'autres sites et deviendront accessibles facilement pour qui sait où chercher.

Il est possible que votre adresse e-mail HELMo et/ou privée figure à votre insu dans une base de données volée, accessible aux pirates, au côté de votre mot de passe ou d'autres informations personnelles.

Il existe un moyen simple de vérifier si votre compte est toujours sûr. **En effet, plusieurs plateformes centralisent les bases de données frauduleuses disponibles en ligne et vous permettent d'y rechercher votre adresse e-mail et/ou votre mot de passe**. Elles permettent aussi de recevoir une alerte dans le cas où votre adresse e-mail apparaît dans une nouvelle base de données volée. Nous vous recommandons de vous inscrire à ces notifications afin de ne plus avoir à y penser par après.

Parmi ces plateformes nous pouvons en citer deux principales:
https://haveibeenpwned.com/
https://monitor.firefox.com/

Si vous retrouvez votre adresse e-mail HELMo ou privée sur une de ces plateformes, il est important de changer votre mot de passe partout où il est utilisé.

Nous vous recommandons l'utilisation d'un mot de passe fort, éventuellement gardé dans un gestionnaire de mots de passes sûr et reconnu. Veillez à ne pas réutiliser le même mot de passe partout, surtout entre les comptes privés et professionnels. Enfin, il est vivement recommandé d'activer la double authentification partout où elle est disponible. Ceci constitue une sécurité supplémentaire en cas de vol de votre mot de passe.

Sécurisez vos appareils

Un ordinateur, qu'il soit sous Windows ou MacOS X **doit être protégé par une solution de sécurité**. Il existe bon nombre de solutions de sécurité qui sont disponibles. Certaines sont proposées gratuitement tandis que d'autres sont payantes. Notez que Windows 10 est, par défaut, équipé de Windows Defender, la solution de sécurité proposée par Microsoft.

Comment choisir une solution de sécurité ? Référez-vous toujours aux comparatifs sérieux publiés. Par exemple, les comparatifs suivants analysent en profondeur les différentes solutions de sécurité : Av-Test, Av-Comparatives ou SELabs.

Ainsi, parmi les solutions gratuites, épinglons:

- Avast / AVG
- Avira
- Bitdefender Free

- Kaspersky Free
- Panda Free

Si **vous disposez déjà d'un antivirus installé**, il n'est pas possible d'en installer un deuxième (ils risquent de ralentir fortement la machine et d'entrer en conflit). Cependant, vous pouvez toujours vérifier votre machine par un antivirus en-ligne. Ceux-ci permettent de vérifier, en utilisant un autre antivirus, que votre ordinateur ne contient pas de malware. Voici quelques antivirus en-ligne disponibles:

- F-Secure Online Virus Scanner
- TrendMicro HouseCall - Free Online Security Scan
- ESET Online Malware Detection

N'hésitez pas à vérifier que votre ordinateur est toujours bien protégé.

Personnes relais

Qui contacter en cas de problème avec vos identifiants?

Personnes relais des étudiants

Les secrétariats sont les points de contact des étudiants dans la gestion de leurs identifiants.

Personnes relais des membres du personnel

Si vous êtes membre du personnel, les personnes relais des membres du personnel peuvent, selon votre département, vous assister dans la gestion de vos identifiants.