HELMo
Haute Ecole
Libre Mosane

Guide d'utilisation des outils numériques

Ce livre couvre les procédures d'utilisation ses plateformes et services numériques disponibles à HELMo.

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.

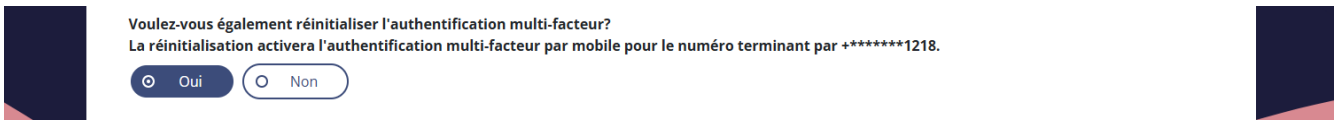
Je souhaite changer mon mot de passe HELMo et/ou Microsoft

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

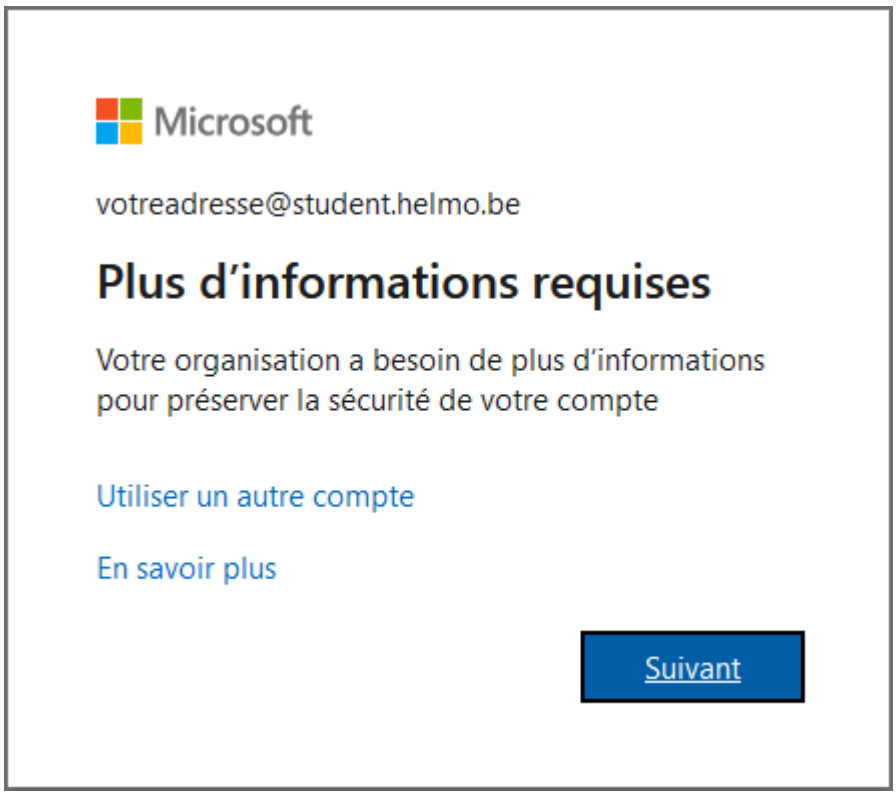
Apple

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

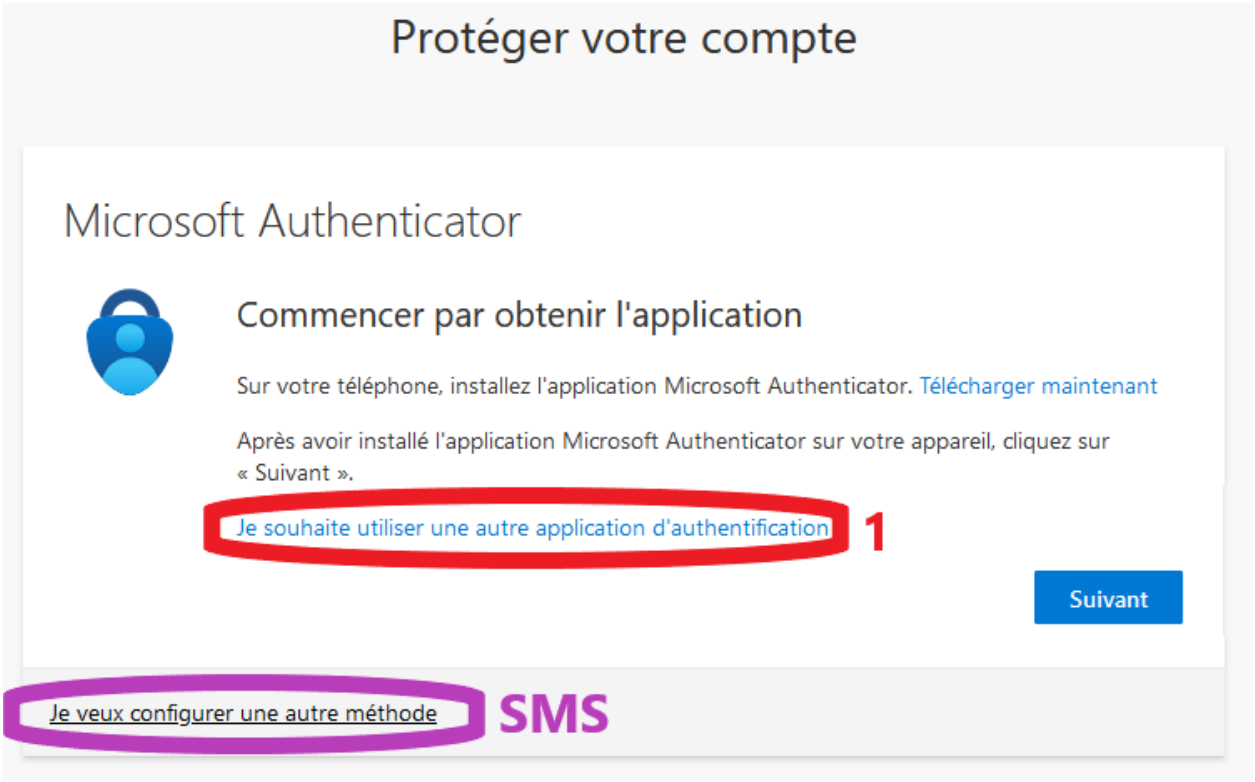
Configuration

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 :

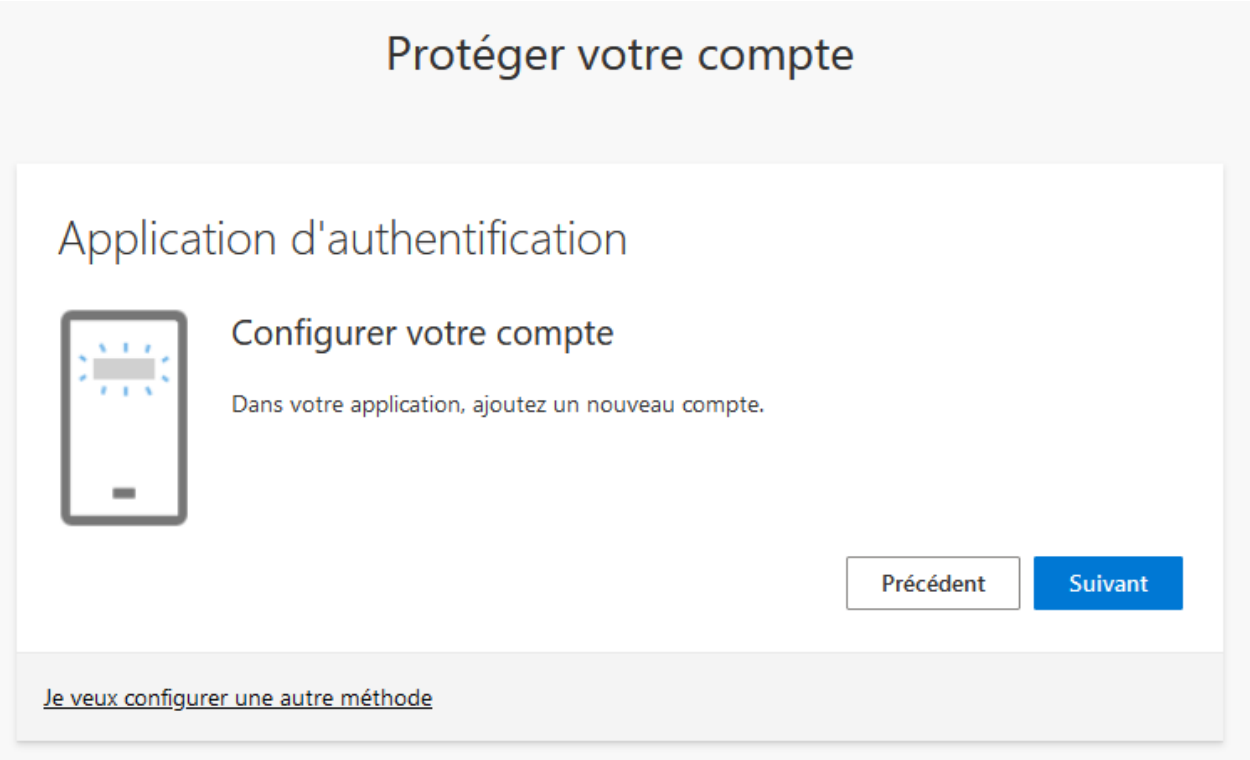


1. En cliquant sur « Suivant », la fenêtre suivante apparaît :



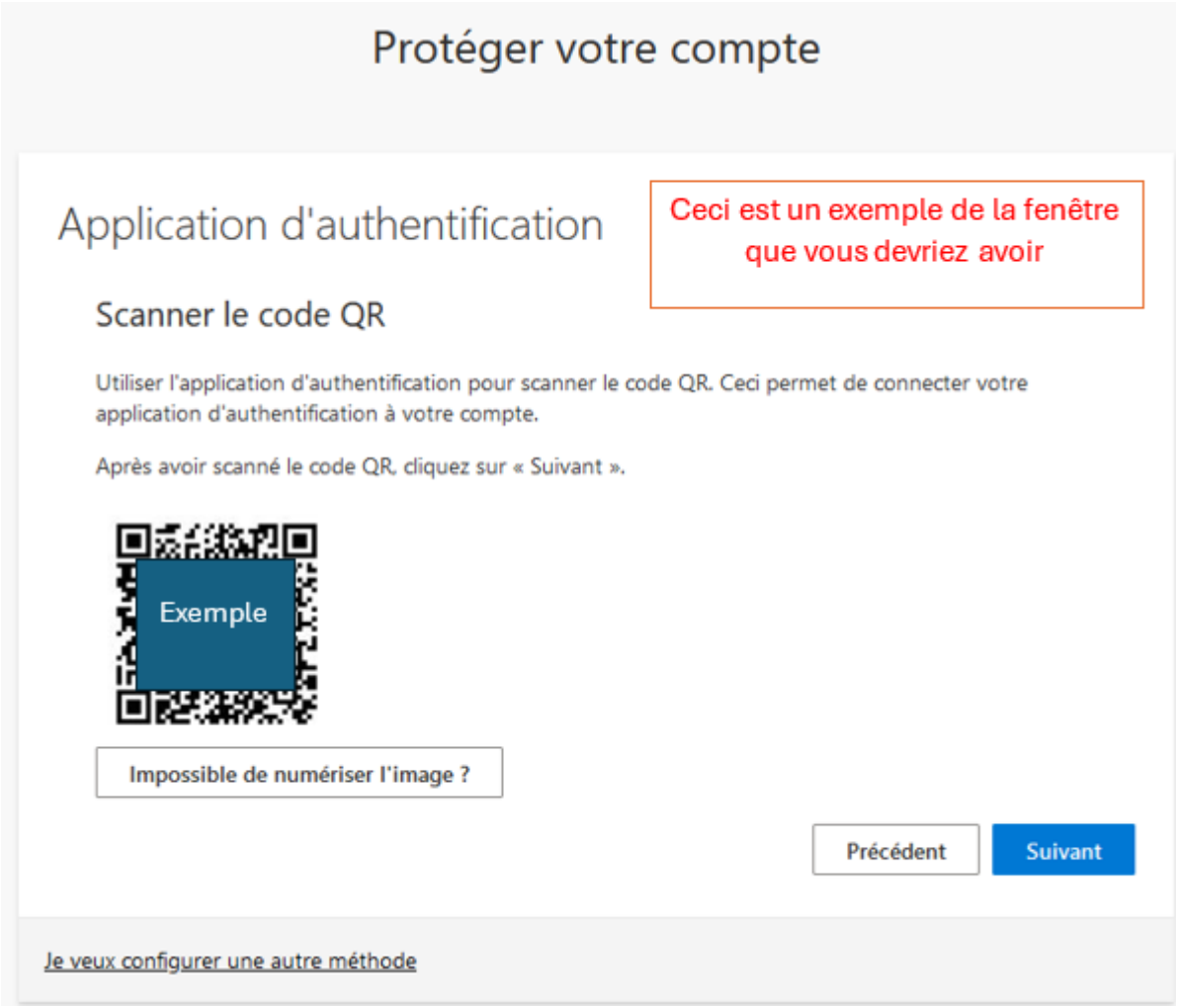
Si vous avez installé une application d'authentification, vous pouvez cliquer sur le lien mentionné « Je souhaite utiliser une autre application d'authentification » (qui fonctionne pour Microsoft Authenticator, Google Authenticator, ...). Si vous ne disposez pas d'un smartphone, il est possible d'encoder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

1. La fenêtre suivante apparaît alors :



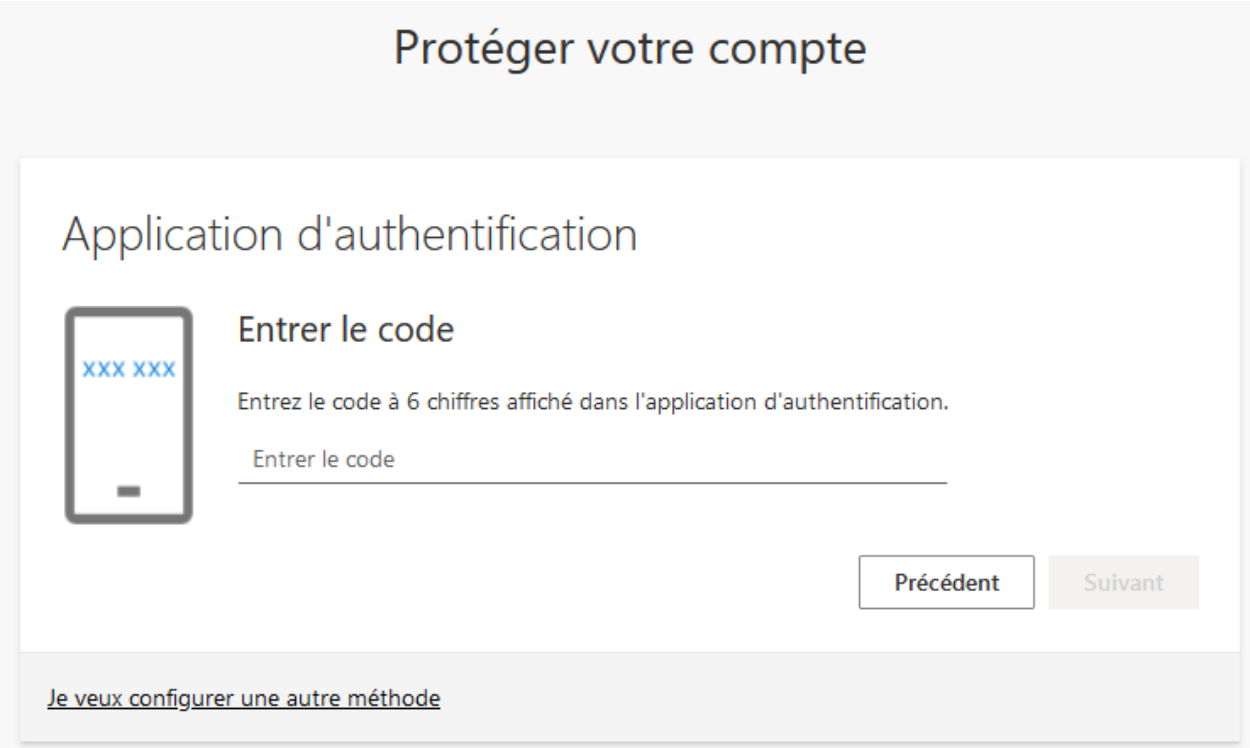
Il faut alors simplement cliquer sur Suivant

1. Le code QR apparaît sur la fenêtre suivante :



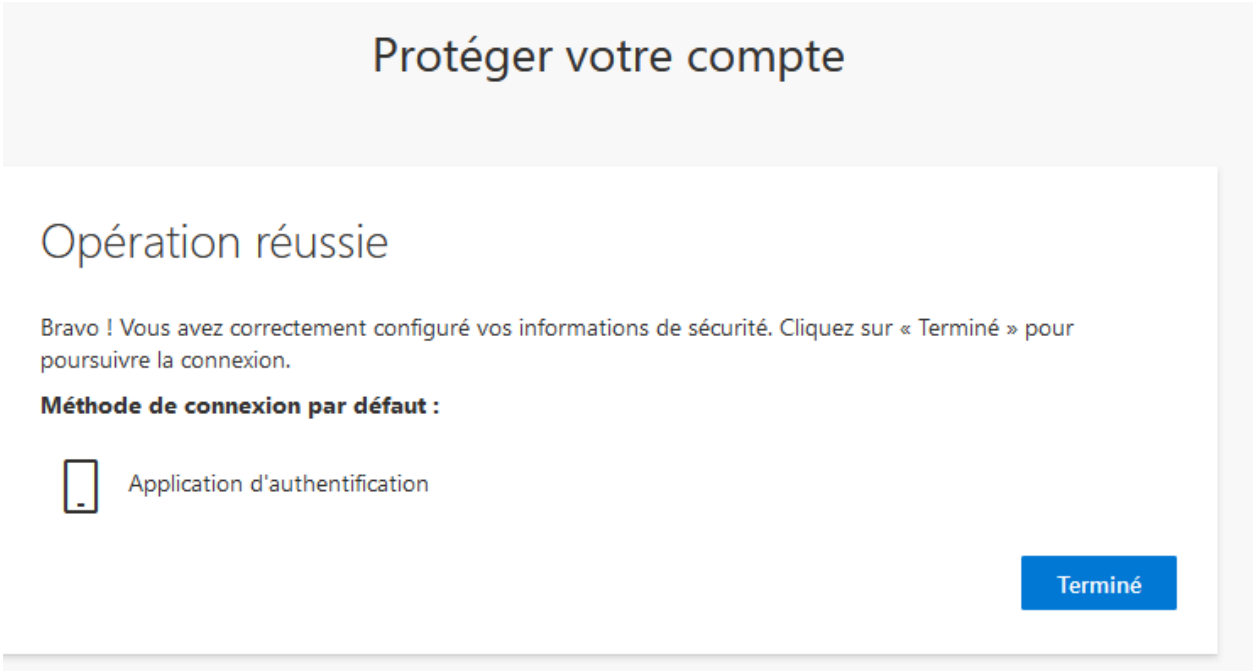
Il faut, ouvrir l'application d'authentification, et dans celle-ci, ajouter un compte (personnel s'il est demandé) et choisir Scanner un code QR. Présentez ensuite l'appareil photo de votre téléphone en regard de ce code. Cela provoquera automatiquement l'ajout du code dans l'application.

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.

Courrier électronique

Toutes les informations concernant vos e-mails HELMo

Accéder à ma boite mail HELMo

La technique la plus utilisée et la plus simple est d'utiliser la version en ligne (voir plus bas pour les autres solutions ou pour plus de précision sur l'utilisation).

Que ce soit sur votre ordinateur ou sur vos appareils mobiles, procédez comme suit :

- Avec votre navigateur habituel (Chrome, Firefox, Edge, Safari etc.), rendez-vous sur la page https://outlook.office.com/mail/
- Comme informations de connexion, utilisez
  - votre adresse e-mail HELMo (ex e.dupont@student.helmo.be)
  - le mot de passe que vous utilisez pour vous connecter à la plateforme Mon Espace, sauf si vous l'avez changé dans Office, alors il s'agit du mot de passe que vous avez vous-même paramétré.

Si vous désirez aller plus loin dans l'utilisation de la boîte mail (faire disparaitre l'onglet "prioritaire", trouver des contacts HELMo facilement ...). Vous pouvez suivre la documentation ci-dessous.

- Si vous avez l'habitude d'utiliser un programme sur votre appareil mobile (Application Salto, Thunderbird, Outlook, etc.) La documentation sur le paramétrage du **client Outlook** (remplaçant de tous vos clients de messagerie actuels) se trouve ici.
- Si vous avez l'habitude d'utiliser un programme sur votre ordinateur (Thunderbird, Outlook, etc.), celui-ci devra obligatoirement être remplacé par le **client Outlook** : La documentation se trouve ici.

Si vous utilisiez une application tierce (Thunderbird, Clawsmail, Apple Mail, Google Mail), vous avez peut-être remarqué qu'il n'est plus possible d'accéder à votre boite mail par ces applications.

Depuis le 1er octobre 2022, Microsoft a désactivé, pour **des raisons de sécurité**, l'authentification basique sur les protocoles IMAP/POP3, au profit de OAuth2. Pour rappel, **le service informatique supporte uniquement l'utilisation de l'application Outlook** (en version mobile, desktop ou web).

Si vous choisissez d'utiliser une autre application, cela se fait sous votre responsabilité **et** sans le support de la haute école. Les liens ci-dessous sont donnés à titre d'exemples et les paramètres présentés doivent probablement être adaptés.

- Apple Mail peut supporter cette authentification OAuth2 - https://support.apple.com/fr-be/HT201729
- Thunderbird (sous Linux, MacOS et Windows) en version récente, supporte l'authentification OAuth2 - https://kb.uwm.edu/uwmhd/page.php?id=109671
- GMAIL ne semble pas proposer de solution pour relever les boites Office 365. La seule solution est alors de configurer un transfert de votre courrier vers une autre adresse.

Comme nous ne supportons pas ces solutions, il est inutile de contacter le service informatique.

Problème d'envoi/réception d'e-mail

Je ne reçois pas certains e-mails

En premier lieu, vérifiez votre client mail

1. **Vérifiez que vos e-mails sont bien triés par date dans Outlook.com**.
2. Si vous en utilisez un, vérifiez les paramètres de votre client mail (Outlook, smartphone, tablette, compte Gmail...). **Il est possible que celui-ci soit paramétré pour supprimer les e-mails** une fois qu'il les a téléchargé, auquel cas vous ne les verrez plus apparaitre dans l'application Web.
3. Vérifiez les dossiers "Courrier indésirable" et"Eléments supprimés", parfois une mauvaise manipulation peut conduire à la mise à la corbeille de vos mails.
4. Vérifiez les règles de redirection de vos e-mails: https://outlook.office.com/mail/options/mail/rules

Je ne reçois pas certains e-mails ou je reçois des e-mails qui ne me sont pas destinés

Si ce sont des e-mails qui me sont adressés personnellement

En raison d'homonymies, il arrive que certaines adresses e-mails se ressemblent. En cas de distraction, cela peut créer la confusion conduisant à des erreurs de destinataires. Dans ce cas, il vous faut vous adresser directement à l'émetteur de l'e-mail pour l'informer du problème, il pourra alors rectifier et vous retirer de sa liste de diffusion le cas échéant.

Il convient d'être particulièrement attentif au suffixe des adresses e-mails (@helmo.be/@student.helmo.be) ainsi qu'au nombre de lettres qui composent la première partie de l'adresse e-mail. Par exemple, Jean Dupont et Jeanne Dupont se verront chacun attribuer une adresse e-mail qui pourrait correspondre aux deux personnes, à savoir j.dupont et je.dupont suivant leur ordre d'inscription à la Haute Ecole.

Le service informatique n'est pas en mesure d'intervenir en cas de confusion ponctuelle ou régulière de destinataires. Il est de la responsabilité des émetteurs de vérifier l'adresse des destinataires de leurs e-mails.

Si ce sont des e-mails concernant les horaires

Si vous êtes étudiant et que les e-mails que vous ne recevez pas concernent les **horaires,** veuillez vérifier votre sélection de groupe sur la page des horaires.

Si ce sont des e-mails groupés concernant les cours ou les actualités

Les e-mails d'actualités sont envoyés à des groupes cibles qui sont mentionnés sous l'actualité. Si vous ne recevez pas certains de ces e-mails c'est que vous ne faites pas partie des groupes cibles. Si c'est une erreur, il convient d'identifier à quels groupes l'e-mail a été envoyé et de vérifier pourquoi vous ne faites pas partie d'au moins un de ces groupes.

Les changements de cursus et sont répercutés dans les e-mails à partir du 14/09. En cas de changement de cursus, vous devez penser à :

- Faire la bonne sélection de groupes dans "Mon horaire"
- Vous désinscrire de vos anciens espaces de cours dans HELMo Learn et vous réinscrire dans les nouveaux espaces selon les modalités fournies par vos enseignants.

Il est possible que vous receviez toujours des e-mails adressés à votre ancien cursus jusqu'à ce que vous ayez signé votre PAE.

Si ce sont des e-mails provenant de Learn/Moodle

1. Vérifiez vos préférences de notification sur la plateforme Learn.
2. Vérifiez votre inscription aux cours d'où émanent les e-mails.
3. Le cas échéant, vérifiez votre abonnement aux notifications du forum d'où émanent les e-mails.

Je ne peux pas voir certaines pièces jointes

Types de pièces jointes acceptées

Notre installation mail filtre les pièces jointes de plusieurs façon. Notamment, les fichiers suivants sont systématiquement mis en quarantaine :

- Archive : .ace, .arj, .cab, .jar, .img, .iso, .lha, .lzh, .xz, .z
- Application: .exe, .elf, .com, .apk, .jnlp, .kext, .scr, .msi, .msix, .msp, .mst
- Lien / Script: .bat, .cmd, .lnk, .pif, .vb, .vbe, .vbs, .wsh
- Autre: .app, .appx, .ani, .deb, .dex, .dll, .docm, .hta, .lib, .library, .macho, .msc, .ppa, .ppam, .reg, .rev, .scf, .sct, .sys, .uif, .vxd, .w

Cette politique de sécurité proposée par Microsoft est celle recommandée pour une protection standard. C'est la raison pour laquelle elle est appliquée à HELMo.

Bug dans Outlook Online

Dans Outlook Online (https://outlook.office.com/mail), certains utilisateurs rencontrent un problème lors de la réception des mails et des pièces jointes lorsque le mail est signé numériquement. En effet, la barre d'information apparaît, mais pas les

fichiers annexés au mail.

Pour résoudre ce problème, avec Microsoft Edge (Chromium) :

1. Télécharger l'extension suivante : Microsoft S/MIME https://microsoftedge.microsoft.com/addons/detail/microsoft-smime/gamjhjfeblghkihfjdpmbpajhlpmobbp
2. Installer le MSI disponible ici : https://media.helmo.be/service-informatique/browser-update/SmimeOutlookWebChrome.msi
3. Redémarrer Edge et retenter d'ouvrir le mail … normalement, il sera toujours marqué comme invalide au niveau de la vérification S/Mime, mais les fichiers devraient être visibles.

Normalement, depuis Microsoft Edge, les mails et les fichiers annexés sont alors visibles.

Identifier et réagir à un e-mail frauduleux

Réagir à un e-mail frauduleux

Si vous avez répondu à un message frauduleux veuillez changer votre mot de passe sans tarder.

Si vous n'y avez pas répondu, ignorez simplement le message et supprimez-le.

Identifier un e-mail frauduleux

Le SPAM représente du courrier indésirable. Il est envoyé:

- par des entreprises qui espèrent, de cette façon, atteindre de nouveaux clients.
- par des attaquants qui espèrent obtenir des informations personnelles (carte de crédits, code pin, mot de passe, ...). On parle alors d'hameçonnage ou de phishing

Le SPAM est difficile à détecter automatiquement. En effet, cela nécessite la mise en place de nombreuses techniques. De plus, le SPAM évolue sans cesse (notamment avec l'arrivée des IA comme ChatGPT) et les techniques pour le combattre doivent également suivre.

A HELMo, plusieurs moyens de protection sont en place pour détecter un spam. Voici les **redflag** à identifier :

- Le mail indique **une personne de HELMo mais le sujet mentionne [EXTERNE]** -> soyez très prudent car le mail n'a pas suivi le chemin attendu. Vérifiez correctement l'adresse de l'expéditeur.
- Un message du type **Vousnerecevezpasbeaucoupdecourrierde...** est ajouté au texte du mail -> soyez prudent quant au contenu du mail.
- Le **sujet du mail mentionne [SPAM]** => Il faut être prudent quant au contenu du mail
- On **vous demande une action urgente** (pouvons-nous payer aujourd'hui ...) => probablement mail de spam
- Les liens dans les mails sont toujours à considérer avec beaucoup de précaution. A HELMo, la plupart du temps, ils sont analysés par Microsoft.

Il faut savoir que le service informatique ne communique jamais de mot de passe ou d'information confidentielle par mail simple.

Un autre indice important est l'adresse e-mail de l'expéditeur. Outre le nom affiché, vérifiez que le nom de domaine après le symbole @ appartient bien à l'entreprise à laquelle l'émetteur prétend appartenir. Méfiance cependant, certains fraudeurs introduisent une adresse e-mail fictive à la place de leur nom, ce qui peut vous laisser croire qu'il s'agit de l'adresse de l'expéditeur.

Par prudence, **en cas de doute, il vaut toujours mieux vérifier auprès du service informatique avant d'encoder vos identifiants.** Il faut rester vigilant face au courrier que l'on reçoit et face à son utilisation de l'outil informatique.

Liens utiles

- Testez vos réflexes face au hameçonnage : https://www.safeonweb.be/fr/quiz/test-du-phishing
- Microsoft a publié un article intéressant sur les bons réflexes à adopter face aux tentatives d'hameçonnage : https://aka.ms/LearnAboutSenderIdentification

Pourquoi recevez-vous du SPAM ?

Détecter un SPAM est assez difficile. En fait, le système informatique doit deviner si le courrier en question est, ou non, un SPAM. Pour ce faire, il va analyser le contenu du courrier et, attribuer un score à chaque mail. Les règles d'attribution des points pour le score sont proposées et déterminées par l'administrateur. Le score obtenu détermine si le courrier est :

- un courrier normal. Le score obtenu est alors faible.
- un SPAM probable. Le score obtenu est moyen et le système ajoute dans l'en-tête du courrier les mots [SPAM]. Il faut bien comprendre que dans ce cas, le système n'est pas sûr qu'il s'agit d'un SPAM.
- un SPAM certain. Le score obtenu est élevé et, dans ce cas, le système supprime le courrier en question.

Détecter correctement le SPAM revient à choisir les points pour chaque règle et le seuil pour déterminer si le courrier est normal, SPAM probable ou SPAM certain. Il est toujours possible de durcir les règles et modifier les seuils. Cependant, ces modifications ne sont pas anodines car elles pourraient conduire à décider qu'un courrier normal est un SPAM probable ou qu'un SPAM probable est un SPAM certain et dès-lors, conduire à la non réception de mails pourtant légitimes.

Pourquoi recevez-vous plus de SPAM qu'un autre ?

Pour envoyer du SPAM, il faut disposer des adresses mails valides. Ainsi, vous risquez de recevoir davantage de SPAM si:

- votre adresse mail est mentionnée sur le serveur web de la haute école
- vous utilisez votre adresse mail HELMo pour vous enregistrer sur des sites sur internet
- vous utilisez votre adresse mail HELMo dans des listes de diffusion
- vous mentionnez votre adresse mail HELMo sur les réseaux sociaux tels que Twitter, Facebook, Netlog, ...

Comment vous protéger mieux contre le SPAM?

Bien sûr, la première chose à faire est de ne pas trop exposer son adresse mail, si c'est possible (ne pas enregistrer son adresse mail HELMo sur n'importe quel site par exemple).

La seconde chose à faire est d'utiliser un client mail adéquat. Ainsi, Microsoft Outlook ou encore Mozilla Thunderbird sont largement recommandés car ils disposent chacun de filtres antispam intégrés et fonctionnels. Dans Outlook par exemple, vous pouvez d'ailleurs affiner le niveau de filtrage souhaité (menu Outils > Options > Courrier indésirable, il est possible de choisir le niveau de filtrage souhaité). Il est important de souligner que les remarques ci-dessus sont d'application dans Outlook.

La troisième chose importante est de rester vigilant. En effet, le mail est une application non sécurisée. Ainsi, vous ne pouvez jamais être sûr de l'expéditeur d'un mail sauf si ce dernier signe son mail numériquement.

Sécuriser mes appareils et identifiants

Retrouvez d'autres informations essentielles pour améliorer la sécurité de vos données dans cet article.

Réseaux et WiFi

Les procédures de connexion aux réseaux WiFi de la haute école.

Se connecter au Wifi

HELMo propose plusieurs réseaux Wifi, chacun est dédié à un usage spécifique.

Pour les étudiants et membres du personnel HELMo : HELMo-Wifi

Sélectionnez le réseau HELMo-Wifi et complétez les paramètres suivants :

- **Option 1:** Méthode EAP => PEAP et authentification MSCHAPv2. Il faut entrer vos identifiants HELMo. Il est parfois demandé de valider le certificat AC, vous pouvez choisir "Ne pas valider" ou"Certificats systèmes" et si un"nom de domaine" est demandé, vous pouvez entrer: wifi2021.wifi.helmo.be
- **Option 2:** Méthode EAP => EAP-TTLS, et authentification MSCHAPv2. Il faut entrer vos identifiants HELMo. Il est parfois demandé de valider le certificat AC, vous pouvez choisir "Ne pas valider" ou"Certificats systèmes" et si un "nom de domaine" est demandé, vous pouvez entrer: wifi2021.wifi.helmo.be

image

Si vous utilisez un appareil Android, vous pouvez visualiser la vidéo disponible ici.

Si vous utilisez un appareil iOS (iPhone/iPad), vous pouvez visualiser la vidéo montrant la configuration étape par étape.

01 Pour les membres d'un autre établissement d'enseignement supérieur : Eduroam

Qu'est-ce que le réseau Eduroam ?

Le réseau eduroam est un réseau Wifi sécurisé, disponible dans la plupart des institutions de recherche et d'enseignement européen. Ce réseau est également disponible à HELMo.

Vous **pouvez configurer les deux réseaux : HELMo-Wifi et eduroam** sur tous vos périphériques. Ainsi, si vous êtes hors des locaux de HELMo mais dans une institution partenaire, vous aurez accès à Internet.

La connexion utilise vos identifiants et votre mot de passe HELMo.

Comment se connecter à Eduroam ?

La connexion à eduroam est aussi facile que la connexion à HELMo Wifi. Il faut:

1. Choisir le réseau: eduroam
2. Entrez comme identifiant: [votreMatriculeHELMo]@helmo.be (par exemple: q220001@helmo.be)
3. Entrez votre mot de passe HELMo

Les autres paramètres restent identiques.

Remarquez que, lorsque vous êtes connecté à eduroam, vous êtes automatiquement mis dans un réseau particulier, qui vous donne principalement accès à Internet et pas aux ressources internes de votre institut. C'est la raison pour laquelle, quand vous êtes à HELMo, il est préférable de choisir HELMo-Wifi.

Pour les invités extérieurs : HELMo-OpenNET

Information importante: Si vous êtes membre d'un autre établissement d'enseignement, il est fort probable que vous disposiez d'un accès à eduroam avec vos données de connexion fournies par votre institution d'origine. Dans ce cas, connectez-vous simplement à ce réseau eduroam avec vos paramètres.

A HELMo, un visiteur est une personne ne disposant pas d'un accès institutionnel (ni login, ni mot de passe HELMo ou eduroam).

Pour les visiteurs, nous avons déployé le réseau Wifi HELMo-OpenNet. Dans la liste des réseaux Wifi, choisissez HELMo-OpenNet. Une fois connecté à ce réseau, la page de connexion apparaît et propose les principales options :

image

La connexion à ce réseau peut se faire de trois façons :

- Par auto-enregistrement et **réception d'un code par mail ou SMS**. Cette option permet au visiteur de s'enregistrer de manière autonome. Pour ce faire, il doit recevoir un code de connexion valable 1 journée. Celui-ci est envoyé par mail et, si souhaité, par SMS.
- Par auto-enregistrement **sans code** avec approbation d'un membre de HELMo. Cette option permet au visiteur de solliciter un membre de HELMo pour approuver sa demande de connexion au réseau.

Option 1: Auto-enregistrement et réception d'un code par mail ou SMS

Pour l'auto-enregistrement et la réception d'un code, il faut commencer par accepter les conditions d'utilisation spécifique du réseau.

Une fois celles-ci acceptées, il faut fournir les informations suivantes : le nom du visiteur, l'adresse mail du visiteur et, s'il souhaite recevoir le code par SMS également, son numéro de GSM. Il faut noter que le code est toujours envoyé par mail (il convient de vérifier le dossier Courrier Indésirable). Attention, la livraison du code par SMS n'est pas toujours garantie puisque certains opérateurs filtrent les SMS envoyés depuis des numéros courts.

image image

Une fois la demande finalisée, le code unique est envoyé par mail et, éventuellement, par SMS. Un exemple des messages envoyés est fourni ci-dessous.

image image

Le visiteur doit alors recopier le code reçu (par mail ou SMS) sur la page de connexion pour avoir accès à Internet.
image
Il faut noter que la dernière option (je me suis déjà enregistré et j'ai déjà reçu mon code unique) permet d'arriver au dernier écran pour entrer directement le code.

Option 2: Auto-enregistrement sans code avec approbation d'un membre de HELMo

Cette option permet de se connecter très facilement au réseau HELMo-OpenNet, sans code, en sollicitant un membre de HELMo.

Comme pour l'auto-enregistrement par SMS, il faut commencer par accepter les conditions d'utilisation. Ensuite, il faut introduire les informations suivantes : le nom du visiteur, l'adresse mail du visiteur et l'adresse mail du membre HELMo qui recevra la demande de connexion par mail.

image image

Une fois la demande envoyée, le membre HELMo reçoit un mail contenant les liens pour approuver ou refuser la demande (il faudra peut être vérifier le dossier Courrier Indésirable). Il dispose de 15 minutes pour opérer le choix.

image image

Si la demande est approuvée, la connexion est autorisée pour 1 journée.

Résoudre les problèmes de connexion

Je n'ai pas accès aux sites de HELMo mais bien à Internet

Vous avez certainement un soucis DNS dont la source peut être soit:

- Votre antivirus qui impose l'utilisation d'un serveur DNS sécurisé
- Vous avez forcé l'utilisation d'un serveur DNS comme celui de Google (8.8.8.8/8.8.4.4), celui de CloudFlare (1.1.1.1 / 1.0.0.1), ou de Quad9 (9.9.9.9)

Comment solutionner ce problème ?

- Vérifiez les options de votre antivirus (Avast/AVG/Comodo sont connus pour proposer cette option) pour désactiver l'option DNS (appelée parfois secure DNS ou encore Real site)
    - https://help.avast.com/en/av_free/10/etc_tools_secure_dns_overview.html
    - https://help.avg.com/en/avg_free/17/securityantivirus_securedns.html
    - https://www.comodo.com/secure-dns/
- Si vous avez forcé l'utilisation d'un serveur DNS externe, il est préférable, à HELMo de basculer vers l'utilisation des serveurs de l'école (en revenant à une configuration automatique du DNS)
    - https://support.microsoft.com/fr-be/help/15089/windows-change-tcp-ip-settings

Sans cette modification, vous risquez d'avoir continuellement des soucis avec les serveurs de la Haute Ecole.

Comment vérifier si tout est en ordre ?

1. Cliquer sur Démarrer (puis > Exécuter sur Windows 7/8.1) et puis entrer **nslookup.exe**
2. Entrer learn.helmo.be pour tester
    1. Si vous êtes à l'intérieur d'un campus HELMo, la réponse affichée devrait être
        1. Nom: learn.helmo.be
        2. Address: 192.168.3.200

        Si vous recevez une adresse du type 193.190.65.225 c'est que votre DNS est mal configuré.
3. Entrez exit pour quitter l'outil nslookup

Mon horaire en ligne

Ce chapitre vous explique comment accéder à votre horaire en ligne et que faire en cas de problème.

Comment synchroniser mon horaire de cours avec mon agenda personnel?

Vous avez la possibilité de synchroniser automatiquement votre agenda personnel avec votre horaire de cours de sorte que celui-ci s'affiche et se mette à jour automatiquement et de façon régulière dans votre application de gestion d'agenda.

La première étape est d'obtenir votre lien unique et personnel d'abonnement à votre horaire HELMo. Ce lien vous est réservé, si vous le diffusez vous acceptez que d'autres personnes ait accès à votre horaire de cours. Pour obtenir ce lien, rendez vous sur l'écran des horaires dans votre espace et cliquez sur le bouton"Exporter votre horaire".

Sur la page qui s'affiche à présent, dans la section "Votre horaire - Synchronisation automatique avec votre agenda", un bouton vous permet de générer un lien d'abonnement à mon horaire. Cliquez sur le bouton et copiez le lien qui s'affiche ensuite.

La suite de l'opération dépendra de votre client agenda. Par exemple, si vous utilisez Google Agenda, vous devrez suivre les étapes de la documentation de Google. Voici les documentations des principaux clients d'agendas:

- Google Agenda: https://support.google.com/calendar/answer/37100 (section"Ajout à l'aide d'un lien")
- Outlook.com: https://support.office.com/fr-fr/article/importer-un-calendrier-ou-s-y-abonner-dans-outlook-com-cff1429c-5af6-41ec-a5b4-74f2c278e98c(section "S'abonner à un calendrier")
- Apple Calendrier: https://support.apple.com/fr-fr/guide/calendar/icl1022/mac

Il faut savoir que la fréquence de mise à jour de votre horaire de cours dépendra de la configuration de votre client d'agenda. Il est donc possible que votre horaire de cours mette plusieurs heures avant d'être mis à jour dans votre agenda. Pour connaitre les délais de mise à jour, consultez la documentation de votre client d'agenda.

Vous gardez la possibilité de supprimer et recréer votre lien personnel de synchronisation dans Mon Espace. Le cas échéant, vous devrez reconfigurer votre client d'agenda pour vous abonner au nouveau lien.

Résoudre un problème avec mon horaire

Vous trouverez ici les procédures à suivre si vous constatez une anomalie avec votre horaire en ligne.

Je suis étudiant

Je n'ai pas accès à mon horaire de cours

Les horaires de cours sont disponibles dans le module "Mon horaire" de votre espace.

Certains instituts communiquent les horaires via leur propre canal. Renseignez vous sur les modalités de communication des horaires auprès du secrétariat de votre institut.

Mon horaire de cours est incomplet

Votre horaire personnel dépends de votre sélection de groupes, il est primordial que vous sélectionniez vos groupes avec attention.

Si un cours ne s'affiche pas dans l'onglet Mon horaire alors que cotre sélection de groupes est correcte, **il est possible que l'horaire de vos cours ne soit pas encore finalisé**. Vous pouvez vous en assurer en vérifiant vous-même via l'onglet "Horaire par cursus et bloc" ou auprès du secrétariat de votre institut mais soyez patient, vous recevrez un e-mail automatique à chaque mise à jour de votre horaire.

La constitution des horaires est un exercice compliqué car il dépend de nombreux facteurs externes qui changent fréquemment ; il n'est pas inhabituel que ce processus prenne un peu de temps en début d'année.

Certains instituts communiquent les horaires via leur propre canal. Renseignez vous sur les modalités de communication des horaires auprès du secrétariat de votre institut.

En cas de problème d'horaire, contactez le secrétariat ou l'horairiste de votre institut.

Je ne sais pas sélectionner mon cursus

Patience, les nouvelles inscriptions et les réorientations sont répercutées dans votre horaire 24h après leur encodage par le secrétariat académique. Si le problème persiste une fois ce délai passé, vérifiez votre dossier administratif auprès du secrétariat de votre institut.

Je rencontre un problème technique

En cas de problème technique, videz le cache de votre navigateur et supprimez vos cookies puis réessayez. Si le problème persiste, contactez le service informatique.

Maitriser mon navigateur Web

Procédures utiles pour la maintenance et l'utilisation de votre navigateur Web.

Quel navigateur Web dois-je utiliser?

Nos plateformes supportent les navigateurs récents. Sans vous imposer le choix d'un navigateur précis, nous vous conseillons de tenir votre navigateur à jour.

Tenir votre navigateur à jour vous garantira une expérience de navigation optimale et sécurisée. Les navigateurs à jour bloquent les menaces et sont compatibles avec les technologies Web les plus récentes. Si vous rencontrez des problèmes d'affichage, un affichage partiel ou une fonctionnalité qui ne se comporte pas comme attendu, c'est peut-être parce que votre navigateur n'est pas à jour.

Le site suivant vous indiquera si votre navigateur Web est à jour et vous informera sur les alternatives et sur la procédure pour les installer (avec publicité) : https://browser-update.org/update.html

Vider les cookies

Les cookies sont des informations stockées par les sites Web directement dans votre navigateur Web.

Vider les cookies d'un site Web peut parfois résoudre certains problèmes spécifiques.

Pour supprimer les cookies de votre navigateur, vous pouvez suivre ces instructions:

- Google Chrome: Vider le cache et supprimer les cookies - Ordinateur - Aide Compte Google
- Edge: Supprimer les cookies dans Microsoft Edge - Support Microsoft
- Mozilla Firefox: Effacer les cookies et les données de site dans Firefox | Assistance de Firefox (mozilla.org)
- Apple Safari: Effacer les cookies dans Safari sur Mac - Assistance Apple (BE)

Vider le cache de mon navigateur

Lorsque vous visitez un site Web, votre navigateur enregistre un certain nombre de ressources afin d'accélérer le chargement ultérieur de ce site Web.

Parfois, lorsqu'un site Web est mis à jour, les données contenues dans votre navigateur ne se mettent pas à jour, vous rencontrez alors des problèmes lors de l'utilisation du site Web. La solution est souvent de vider vous-même le cache de votre navigateur :

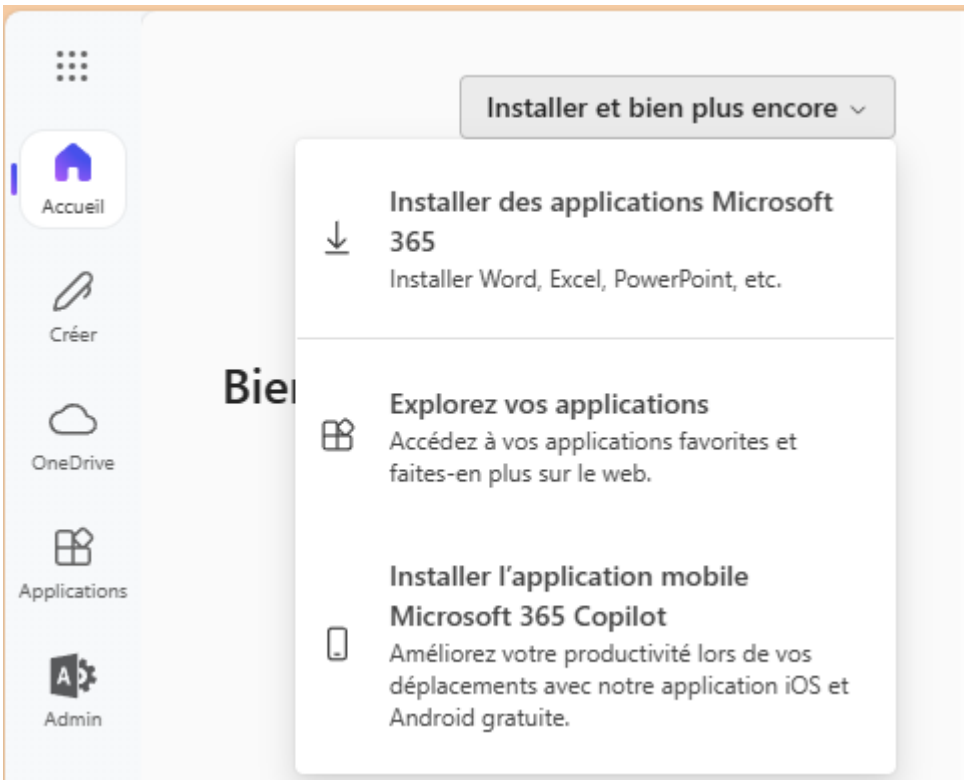
https://fr.wikipedia.org/wiki/Aide:Purge_du_cache_du_navigateur

Editer des documents et fichiers multimédias

Ce chapitre propose des guides pratiques pour ouvrir, éditer et réduire la taille de vos documents, vidéos, images et autres médias, tout en les les convertissant au format le plus adapté à leur usage.

Installer Microsoft Office gratuitement

HELMo offre une licence Microsoft à tous ses membres. Cette licence vous permet d'installer la suite Microsoft Office gratuitement sur un certain nombre d'appareils. Pour cela, rendez-vous sur https://office.com et suivez les instructions d'installation des applications Microsoft 365 :



En cas de problème

Il est important de noter que la haute école n'offre pas le support pour l'installation et l'utilisation de la suite Microsoft Office. Si vous avez des questions relatives à un produit Microsoft, vous devez suivre sa documentation officielle : https://support.microsoft.com/fr-fr/contactus.

Quand et pourquoi optimiser ses ressources multimédia ?

01 Pourquoi optimiser ses ressources ?

Voici deux excellentes raison d'optimiser ses fichiers multimédia : réduire votre empreinte écologique et rendre vos ressources accessibles au plus grand nombre.

En bref, optimiser, c'est du win-win : vous y gagnez, les destinataires de la ressource y gagnent et la planète aussi au passage.

1. Réduire le coût économique et écologique des données

Les ressources multimédia de tous types sont omniprésentes dans notre quotidien ; images, vidéos, enregistrements audios et fichiers de diverses natures constituent autant de supports massivement utilisés à HELMo et ailleurs. Ces supports occupent de l'espace sur les disques de vos appareils, nos serveurs et sur le cloud; leur partage consomme de la bande passante, ce qui nécessite une infrastructure réseau conséquente de bout-en-bout, en partant du datacenter jusqu'à l'utilisateur final.

L'acquisition, la maintenance et le renouvellement du matériel de stockage et de distribution, qu'il soit local ou externalisé, représentent **un coût tant économique qu'écologique** et il en va de même pour l'**énergie consommée** par tout ce matériel. Plus une ressource occupe de l'espace, plus couteux est son hébergement et son partage.

Sur nos serveurs et dans le cloud, des sauvegardes régulières sont réalisées pour vous permettre de récupérer vos ressources ou de revenir à une version précédente en cas de problème ; plusieurs versions de chaque ressources sont ainsi conservées, **multipliant par la même occasion l'espace disque** consommé par celles-ci.

Réduire l'espace utilisé par ses données lorsque c'est possible, c'est participer à minimiser l'impact environnemental du numérique. Cette action s'inscrit pleinement dans la démarche de sobriété numérique.

2. Maximiser la compatibilité des périphériques et accélérer le chargement

Chaque format a son usage. **Certains formats de fichiers, souvent plus lourds, sont destinés à faciliter leur édition par des logiciels spécialisés** tandis que **d'autres formats sont optimisés pour en faciliter le partage** en garantissant la compatibilité d'affichage sur le plus grand nombre d'appareils.

Par exemple, une vidéo déposée sur une plateforme telle que Moodle sera lue sur de nombreux navigateurs et périphériques différents (PC, Mac, smartphone, tablette,...), avec des qualités de connexion Internet variables et parfois soumises à des quotas (3G/4G/5G, fibre, ADSL...). Certains formats de vidéos sont créés spécialement pour l'usage sur le Web ! **Une ressource bien optimisée s'affichera sur tous les périphériques, se chargera plus vite, consommera moins de bande passante et de quota à l'utilisateur.**

La plupart des connexions domestiques possèdent une vitesse de téléchargement nettement supérieure à la vitesse d'envoi. **La vitesse d'envoi de votre connexion détermine la durée nécessaire au dépôt d'un fichier sur un serveur.** Reprenons notre exemple concret de vidéo déposée sur Moodle, si notre connexion Internet à domicile permet une vitesse d'envoi de 1,25 Mo/seconde (= 10 Mbps, une vitesse couramment proposée par les fournisseurs d'accès) et que notre vidéo non optimisée pèse 500 Mo, il ne faudra pas moins de 6 minutes et 40 secondes pour la déposer sur Moodle, pour peu que toute la bande passante y soit consacrée et que la connexion reste stable pendant cette durée. En optimisant notre vidéo, on peut diminuer de moitié ou davantage son poids et donc son temps de chargement. **Une ressource optimisée sera plus rapide à déposer sur un serveur ou un cloud.**

02 Quand optimiser ses ressources?

Dans la plupart des cas, **c'est lorsque l'on souhaite partager un fichier qu'il est le plus intéressant de l'optimiser**. Par exemple :

- Déposer une vidéo sur une plateforme d'e-learning comme Moodle ou Hôpital Virtuel
- Partager un fichier via le cloud
- Envoyer un e-mail, collectif ou non, avec une image d'illustration
- **De manière générale, dès que l'on dépose une ressource sur Internet**

Il est aussi intéressant d'optimiser ses données **avant de les archiver** afin d'économiser l'espace de stockage sur le support d'archivage.

Compression et optimisation des vidéos

Les vidéos sont des médias qu'il est particulièrement bénéfique d'optimiser.

Il existe une grande variété d'outils pour réaliser la compression et le transcodage des vidéos. Parmi ceux-ci, nous vous recommandons l'utilisation du logiciel libre **HandBrake**.

La documentation officielle de l'outil est en anglais, il existe cependant de nombreux guides d'utilisation disponibles sur Internet.

Compression et optimisation des images

L'optimisation des médias concerne également les images.

La première chose à faire pour obtenir l'image la plus rapide à charger est de la redimensionner pour l'usage que vous allez en faire : est-il pertinent d'utiliser une image ultra-haute résolution pour illustrer un article ou une communication dans un cadre de quelques pixels?

Une fois que votre image est dans la résolution la plus adaptée à son usage, certains outils vont pouvoir réduire son poids de façon conséquente sans perdre en qualité. Parmi ces outils, nous recommandons FileOptimizer qui est un condensé de différents logiciels de compression libres. L'outil présente une interface graphique qui va a l'essentiel et dont les paramètres par défaut sont déjà efficaces.

Passer systématiquement vos images par le logiciel FileOptimizer avant de les utiliser sur une plateforme Web est un très bon réflexe à avoir.

Vous pouvez consulter la page du projet ici : https://nikkhokkho.sourceforge.io/?page=FileOptimizer.

Organiser, transformer, signer ou compresser mes PDF

La haute école met à votre disposition un outil en ligne permettant d'effectuer de nombreuses actions sur vos fichiers PDF. Il vous permet, par exemple, de :

- **Supprimer** des pages
- **Fusionner** des documents
- **Extraire** certaines pages
- Faire **pivoter** des pages
- **Réordonner** les pages
- **Apposer votre signature** sur le document
- Changer les **métadonnées** du document
- **Compresser** votre fichier PDF

Retrouvez cet outil à l'adresse suivante :

https://pdf.helmo.be/

Stockage et partage de fichiers, édition collaborative... quelques outils pratiques

Présentations interactives

Office Mix : Plugin pour PowerPoint permettant l'ajout de quiz, screencasts... dans une présentation PowerPoint.

H5P : Ensemble de modules intégrés à HELMo Learn pour créer divers types d'activités tels que les vidéos interactives.

Stockage et partage de fichier

Microsoft OneDrive : Espace de stockage en ligne fourni avec votre compte HELMo et permettant de partager les ressources en mode lecture ou écriture. OneDrive propose un petit logiciel qui synchronise un dossier de votre ordinateur, tablette ou smartphone avec votre espace de stockage en ligne.

Google Drive : L'équivalent de OneDrive mais en version Google.

Dropbox : En plus de OneDrive, Dropbox offre un versionning de fichier pour récupérer un fichier perdu ou modifié erronément. Un logiciel de synchronisation est également disponible avec Dropbox.

WeTransfer : Plateforme de transfert de fichier limité dans le temps. Utile par exemple pour envoyer une pièce jointe volumineuse dans un e-mail.

Edition collaborative de documents

Microsoft Office365 : Ensemble de services cloud à destination du grand public. Ces services comprennent la suite bureautique classique Microsoft Office (Word, Excel, PowerPoint...) et sa version en ligne intégrée directement dans votre navigateur. Office365 permet entre autres d'éditer directement des documents stockés sur les plateformes cloud de Microsoft telles que Sharepoint ou OneDrive. La suite Office365 est offerte à tous les membres de HELMo.

Google Docs : Suite bureautique en ligne de Google. Elle permet les mêmes options qu'Office365 en ligne.

Etherpad : Editeur de texte en ligne, intégré à HELMo Learn et utilisable simultanément et en temps réel par plusieurs utilisateurs.