HELMo
Haute Ecole
Libre Mosane

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.