HELMO
Haute Ecole
Libre Mosane

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.
