HELMO
Haute Ecole
Libre Mosane

Garder mes identifiants en sécurité

Quelques réflexes simples pour protéger vos identifiants et réagir en cas de piratage.

1. Repérez les faux sites

N'entrez **jamais** votre mot de passe HELMo si l'une de ces conditions n'est pas remplie :

- L'adresse se termine exactement par **.helmo.be** ou est **login.microsoftonline.com** (ex. : sso1.helmo.be, learn.helmo.be, webmail.helmo.be)
- La page est en **https** (cadenas dans la barre d'adresse)

La plupart des faux liens arrivent par e-mail : apprenez à reconnaître un e-mail frauduleux.

⚠ Vous avez entré votre mot de passe sur un site douteux ? Changez-le immédiatement.

2. Utilisez un gestionnaire de mots de passe

La règle : **un mot de passe long et unique par service**. Un gestionnaire de mots de passe le crée, le retient et le remplit pour vous. Vous n'avez plus qu'**un seul mot de passe maître** à retenir.

KeePassXC : gratuit, open-source, vos données restent chez vous

- Ordinateur (Windows, macOS, Linux) : keepassxc.org
- Android : KeePassDX
- iPhone : KeePassium

Astuce : placez votre fichier coffre-fort sur OneDrive pour l'ouvrir depuis tous vos appareils.

Bitwarden : le plus simple, synchronisé automatiquement

- Version web : vault.bitwarden.eu
- Applications et extensions navigateur : bitwarden.com/download

⚠ Le mot de passe maître ne peut pas être récupéré : choisissez une phrase longue et ne l'oubliez pas.

3. Activez l'authentification multifacteur (MFA)

Avec le MFA, un pirate qui vole votre mot de passe ne peut quand même pas se connecter : il lui manque le code de votre téléphone. C'est la protection la plus efficace contre le piratage.

- Activez-le **partout** : messagerie, réseaux sociaux, banque, cloud…

- Préférez une **application** aux SMS, moins sûrs :
    - **Microsoft Authenticator** (recommandé pour HELMo) : Android · iPhone
    - **Google Authenticator** : Android · iPhone
    - **Authy** : Android · iPhone

⚠ **Activez la sauvegarde de votre application MFA** : sans sauvegarde, perdre ou changer de téléphone peut vous bloquer l'accès à tous vos comptes.

- Microsoft Authenticator : Paramètres › Sauvegarde (compte Microsoft personnel ou iCloud)
- Google Authenticator : connectez-vous à votre compte Google dans l'application
- Authy : Paramètres › Comptes › Sauvegardes

À HELMo, le MFA est **obligatoire et activé par défaut**. Vous avez changé de téléphone sans sauvegarde ? Consultez Mot de passe perdu et problèmes de MFA.

4. Vérifiez si vos données ont fuité

Même les grandes plateformes se font pirater (Adobe, Dropbox…). Vos identifiants circulent peut-être déjà chez les pirates.

Vérifiez votre adresse e-mail (HELMo et privée) et **inscrivez-vous aux alertes** :

- haveibeenpwned.com
- monitor.mozilla.org

Votre adresse apparaît ? **Changez le mot de passe** concerné, partout où vous l'avez utilisé.

5. Protégez votre ordinateur

Windows

- Microsoft Defender est intégré et suffisant pour la plupart des usages. Vérifiez qu'il est bien actif.
- Windows 10 n'est plus mis à jour depuis octobre 2025 : passez à Windows 11.
- Vous préférez un autre antivirus ? Consultez les comparatifs AV-Test ou AV-Comparatives. N'installez **jamais deux antivirus** en même temps.

macOS

- La protection est intégrée (XProtect, Gatekeeper) : aucun antivirus supplémentaire n'est nécessaire.
- Installez les mises à jour macOS dès qu'elles sont proposées.
- Installez vos applications depuis l'App Store ou le site officiel de l'éditeur.

Linux

- Faites régulièrement les mises à jour via le gestionnaire de paquets de votre distribution.
- Installez vos logiciels depuis les dépôts officiels (ou Flathub), jamais via des scripts trouvés au hasard.

Dans tous les cas : gardez votre système à jour et n'installez que des logiciels de source fiable.

Un doute sur un PC Windows ? Faites-le analyser gratuitement par un second antivirus, sans rien désinstaller :

- ESET Online Scanner
- Trend Micro HouseCall
