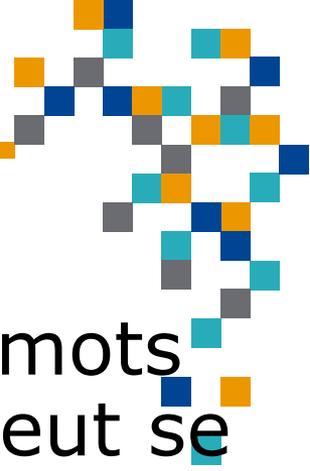




PROTÉGER SES COMPTES EN LIGNE: QUELLES SONT MES OPTIONS ?

MARS 2021

PRÉPARÉ PAR: DENIS BERGERON



- Protéger nos comptes en ligne avec des mots de passe robustes et propres à chacun peut se faire de différentes façons.
- Sujets traités dans cette présentation:
 - Évaluer nos besoins
 - Revue des options disponibles pour gérer ses mots de passe.
 - Un outil complémentaire efficace: l'authentification à double facteur



Partie 1

Survol des options disponibles

Revue des besoins vs options disponibles

Gestionnaires de mots de passe en ligne



Partie 2

Gestionnaires avec données dans notre appareil: Myki et KeePass

Gérer ses mots de passe avec son fureteur

Fichier « maison » crypté

L'authentification à double facteur (2FA)

■ Plusieurs façons de gérer nos mots de passe.

1. Gestionnaires de mots de passe en ligne

- Quelques exemples de **gestionnaires payants**:

Dashlane

1Password

Keeper

LastPass

NordPass

RoboForm

1. Gestionnaires de mots de passe en ligne (suite)

- Quelques exemples de gestionnaires offrant une version **gratuite**:
 - Dashlane (1 appareil, 50 mots de passe max.)
 - Keeper (1 appareil)
 - LastPass (1 type d'appareil)
 - RoboForm (1 appareil)
 - NordPass (1 appareil à la fois)
 - etc.
- Exemple de gestionnaire offrant une solution **open source**:
 - Bitwarden

2. Quelques fureteurs web pour gérer ses mots de passe

Firefox

Chrome

Edge

Safari

3. Gestionnaires sauvegardant nos mots de passe à l'intérieur même de notre appareil

Myki

KeePass (application open source)

4. Fichier maison crypté et sauvegardé localement ou dans notre espace cloud

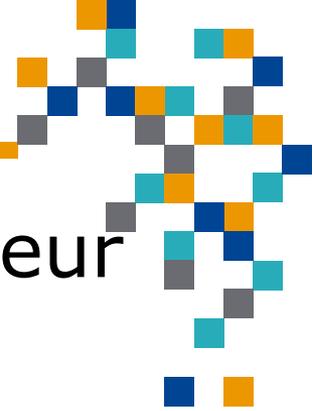
Besoins vs options disponibles



■ Pour nous aider à choisir:

Analyser nos besoins ou attentes par rapport aux possibilités de chaque option.

Besoins vs options disponibles



1. Sauvegarde cryptée des codes d'utilisateur et des mots de passe dans le cloud

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Oui	Non	Oui

2. Synchronise l'accès aux mots de passe entre tous nos appareils

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Pas toujours	Oui	Oui	Non

Besoins vs options disponibles



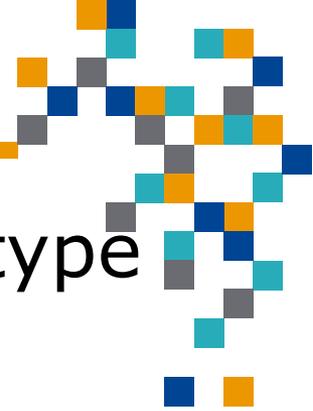
3. Accès aux mots de passe protégé par un mot de passe principal ou un code d'accès

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Idem au code utilisateur	Oui	Oui

4. Génère des mots de passe robustes

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Oui	Oui	Non

Besoins vs options disponibles



5. Possibilité de contrôler le nombre et le type de caractères des mots de passe créés

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Pas toujours	Oui	Oui

6. Possibilité d'utiliser le 2FA pour accéder aux mots de passe

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Pas toujours	Non	Oui	Non

Besoins vs options disponibles



7. Possibilité d'utiliser plus d'un fureteur web pour accéder à nos comptes en ligne

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Non	Oui	Oui

8. Peut conserver en plus les informations telles que questions de sécurité, code divers, etc.

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Non (utiliser un autre fichier crypté)	Oui	Oui

Besoins vs options disponibles



9. Peut autoriser une autre personne à accéder à certains des mots de passe

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Pas toujours	Non	Pas toujours	Non

10. Émet des avis de sécurité (mots de passe faibles, réutilisés, fuite de données, etc.)

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Oui	Non	Non

Besoins vs options disponibles



11. Possibilité de récupérer les mots de passe si perte ou destruction de nos appareils

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Oui	Non, sauf si copie de sauvegarde	Oui si sauvegarde dans le cloud

12. Préremplit les champs code d'utilisateur, mots de passe, cartes de crédit

Gestionnaire web payant	Gestionnaire web non payant	Fureteur web	Application avec sauvegarde dans l'appareil	Fichier maison crypté
Oui	Oui	Oui	Oui	Non

Gestionnaires de mots de passe en ligne



- Le choix de **gestionnaires en ligne** est vaste...
- Plusieurs offrent des fonctionnalités et des prix très semblables.
- De nombreux sites web spécialisés proposent à chaque année une comparaison des gestionnaires qu'ils considèrent être les meilleurs.

■ Exemples de sites web spécialisés publiant une comparaison annuelle:

- Safety Detectives
- Cloudwards
- PCMag
- Tom's Guide
- CNet
- Digital Trends
- Clubic
- Wirecutter (New York Times)

- **La revue de Wirecutter, révision du 5 février 2021, est particulièrement complète et intéressante:**
 - Grille de 10 critères de comparaison.
 - De la quarantaine de produits identifiés au départ, 8 rencontraient l'ensemble des critères.
 - Ces 8 gestionnaires ont été testés pendant une semaine sur chacune des plateformes courantes (PC, Mac, iOS, Android).
 - De ces 8 produits, les 2 suivants ont fait l'objet d'une recommandation: **1Password et Bitwarden.**

- **Parmi les 7 autres sources consultées, les gestionnaires de mots de passe suivants sont ceux qui font partie le plus fréquemment des 5 premiers choix proposés pour 2021:**
 - Dashlane
 - Keeper
 - LastPass
 - Bitwarden (code open source)
 - 1Password
- Abonnement annuel: fourchette de prix variant entre 10 \$ US (Bitwarden) et 60 \$ US (Dashlane)

■ Parmi les gestionnaires en ligne gratuits ceux-ci ont fait notamment l'objet d'une mention par PCMag en 2021:

- LogmeOnce
- Bitwarden
- PassHub
- NordPass



Questions (?)



Partie 2

Gestionnaires avec données dans notre appareil: Myki et KeePass

Gérer ses mots de passe avec son fureteur

Fichier « maison » crypté

L'authentification à double facteur (2FA)

■ Myki

- Premier choix de gestionnaire gratuit recommandé par PCMag.
- Application compatible iOS, Mac, Microsoft et Android.
- Mots de passe enregistrés dans votre téléphone avec copie de sauvegarde dans vos autres appareils.
- Code d'accès spécifique (ou empreinte digitale) protège les mots de passe.

■ Myki (suite)

- Possibilité de synchroniser les mots de passe avec son ordinateur ou d'autres appareils mobiles via un serveur de relais qui ne sauvegarde pas vos données (télécharger l'application ou télécharger l'extension de navigateur disponible pour Chrome, Edge, Firefox, Safari, Opera).
- Intègre une application d'authentification 2FA.
- Possibilité de générer une copie de sauvegarde cryptée de ses données, qui peut être conservée dans son espace cloud.



■ KeePass

- Gratuit, code open source.
- Compatible Mac, Windows, iOS, Android.
- Mots de passe sauvegardés dans un fichier crypté (base de données) de votre ordinateur.
- Possibilité de les synchroniser sur votre téléphone en téléchargeant l'application KeePass.

■ KeePass (suite)

- Une version « portable » existe, permettant de télécharger KeePass sur une clé USB.
- Peut servir de solution de rechange si votre gestionnaire de mots de passe en ligne est inaccessible temporairement.
- Plus complexe à utiliser, plusieurs versions et extensions disponibles, interface vieillotte.

■ Pour ceux ayant un compte Apple et utilisant Safari

- Le gestionnaire de mots de passe Trousseau iCloud est intégré au fureteur Safari pour Mac, iOS et iPadOS.
- Avec vos appareils mobiles, il peut être géré à partir de l'application Réglages, onglet Mots de passe.
- Avec votre ordinateur Mac, ce trousseau peut être géré dans les préférences de Safari et aussi à partir de l'utilitaire Trousseaux d'accès.
- Accès à vos mots de passe en entrant votre mot de passe d'utilisateur (ordinateur) ou votre code d'accès à votre appareil mobile (téléphone, tablette).

- **Pour ceux ayant un compte Microsoft et utilisant Edge ou Chrome**
 - Le gestionnaire de mots de passe Remplissage auto Microsoft est intégré au fureteur Edge.
 - Il se présente sous la forme d'une extension pour le fureteur Chrome.
 - Il est aussi intégré à l'application Microsoft Authenticator sur iOS et Android.
 - Accès à vos mots de passe en entrant votre mot de passe d'utilisateur (ordinateur) ou votre code d'accès à votre appareil mobile (téléphone, tablette).

■ Pour ceux utilisant Firefox

- Gestionnaire de mots de passe Firefox Lockwise: une extension de Firefox.
- Vous pouvez définir un mot de passe principal pour accéder à vos mots de passe depuis votre ordinateur. Pour y accéder à partir de votre téléphone ou tablette, vous utilisez le code d'accès de votre appareil.
- Le mot de passe principal peut être différent de votre mot de passe d'utilisateur.

Fichier « maison » crypté



- Sauvegarde des informations requises pour accéder à vos comptes en ligne dans un fichier de type Word, Excel ou autres:
 - Noms d'utilisateurs
 - Mots de passe
 - Questions de sécurité
 - Etc.
- Fichier crypté avec accès protégé par un mot de passe.
- Sauvegardé à 2 endroits: par exemple, dans votre espace cloud et dans votre ordinateur.
- Pour accéder à un de vos comptes, vous pouvez « copier - coller » vos informations du fichier au site web.
- Méthode plus onéreuse que les autres décrites précédemment.

■ Quelle que soit la méthode choisie...

- En plus d'avoir un mot de passe robuste et unique pour chacun de vos comptes en ligne, il est important de le **changer périodiquement**.
- Dashlane contient un outil de changement automatisé des mots de passe certains sites web.
- Même si la fiabilité des gestionnaires de mots de passe en ligne et des outils offerts par les fureteurs web est excellente, une panne de service ou un problème d'accès n'est pas impossible.



■ Quelle que soit la méthode choisie... (suite)

- Le cas échéant, si vous conservez dans votre ordinateur ou dans votre espace cloud un dossier crypté contenant une copie à jour de vos mots de passe, vous ne serez pas mal pris...
- À l'inverse, si vos mots de passe sont sauvegardés à l'intérieur de vos appareils, une copie de sécurité cryptée conservée ailleurs (un espace cloud sécurisé) pourrait être d'un grand secours en cas de perte ou destruction de tous vos appareils.

L'authentification à double facteur (2FA)



■ En quoi cela consiste-t-il ?

- Méthode très efficace pour sécuriser davantage l'accès à nos comptes en ligne, particulièrement ceux détenant des informations sensibles.
- En plus de nom d'utilisateur et du mot de passe, un élément d'information additionnel est demandé lors de l'accès.
- Pour les sites web offrant le 2FA: dans certains cas le 2FA est imposé et dans d'autres cas l'utilisateur peut choisir de l'activer ou non.
- L'authentification 2FA peut se faire de plusieurs manières, variant selon les entreprises/services avec lesquels nous transigeons.

■ Principales méthodes d'authentification 2FA

1. Méthodes largement répandues:

- Répondre à une question de sécurité (ex: ARC, Revenu Québec, Tangerine, BRC);
- Code d'accès temporaire reçu par téléphone, SMS ou courriel (ex: BNC);

2. Méthodes moins répandues, mais plus sécuritaires

- Notification push transmise à un appareil « de confiance » et demandant d'approuver ou refuser l'accès au compte (ex: Apple).



2. Méthodes moins répandues, mais plus sécuritaires (suite):

- Code, unique et temporaire, généré à la chaîne par votre ordinateur, téléphone ou tablette, au moyen d'une application d'authentification (« software token ») ou d'une physique clé de sécurité certifiée (« hardware token »);
- **Exemples d'applications d'authentification:**
 - Authy
 - Duo
 - 2FA Authenticator
 - Google Authenticator
- **Exemples de clé de sécurité certifiée:**
 - Clé USB Yubikey (plusieurs modèles)
 - Clé Google Titan

L'authentification à double facteur (2FA)



■ Remarques

- Quelques entreprises/services utilisant les clés **YubiKey**:
Google, Microsoft, Facebook, Twitter.
- Quelques entreprises/services utilisant l'application 2FA **Authy**:
Facebook, Twitter, Google, Firefox, **PayPal**, **Amazon**.

Références



1. https://www.safetydetective.com/recommended2-pm/best-password-managers/?gclid=CjwKCAiAi_D_BRApEiwASslbJ2RRlchZl-yMmdJSojX19qaLYU7ruL2N26mr-vlVtS7sXg8NzKtYoRoCtNMQAvD_BwE
2. <https://www.cloudwards.net/best-password-manager-for-ios/>
3. <https://www.pcmag.com/picks/the-best-password-managers>
4. <https://www.pcmag.com/picks/the-best-free-password-managers>
5. <https://www.tomsguide.com/us/best-password-managers,review-3785.html>
6. <https://www.cnet.com/how-to/best-password-manager/>
7. <https://www.nytimes.com/wirecutter/reviews/best-password-managers/#why-cant-you-just-use-your-browser>
8. <https://www.digitaltrends.com/computing/best-password-managers/>

Références



9. <https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel-gratuit-windows.html>
10. https://www.pcastuces.com/pratique/internet/microsoft_authenticator_mots_passe/page1.htm
11. https://en.wikipedia.org/wiki/Firefox_Lockwise
12. <https://authy.com/what-is-2fa/>
13. <https://www.nytimes.com/wirecutter/reviews/best-two-factor-authentication-app/>
14. <https://www.plurilock.com/cybersecurity-facts/seven-authentication-token-families-compared/>



Questions (?)