



KeePass

Introduction



- Les services Conseils I6T



Introduction

Guy Talbot :

- Travaille en TI depuis 1980

Actuellement : pigiste.

- Sécurité de l'information
- Réseau et télécommunication
- Architecture technologique





À propos de

KeePass Password Safe :

Un gestionnaire de mots de passe publié sous GPL v2 ou ultérieur, qui sauvegarde les mots de passe dans un fichier chiffré appelé « base de données ».

Cette base est accessible avec le mot de passe principal. Il peut être accompagné d'une clé sous la forme d'un fichier pour renforcer la sécurité d'accès au fichier chiffré.





Pourquoi un gestionnaire de mots de passe ?

Un mot de passe est un moyen d'authentification.

- Une preuve que l'on n'est bien qui on prétend être.

Les moyens reconnus d'authentification :

- Quelque chose qu'on connaît. (Mot de passe)
- Quelque chose qu'on possède. (Clé numérique)
- Ce que l'on est. (Biométrie)
- Quelque chose qu'on sait faire. (Signature)





Pourquoi un gestionnaire de mots de passe ?

Un bon mot de passe.

- 1) Secret.
- 2) Ne peut pas être deviné.
- 3) Bonne entropie
 - 1) Longueur
 - 2) Variété de caractères





Pourquoi un gestionnaire de mots de passe ?

Un mot de passe ne doit être connu que de vous.

Facebook, Instagram, Google, Microsoft, etc.

Vol de données :

En 2013 et 2014, Yahoo s'est fait voler les données de 1,5 milliard d'utilisateurs incluant les signatures de mots de passe.

On ne doit pas réutiliser un mot de passe.





Pourquoi un gestionnaire de mots de passe ?

Comment se souvenir d'un mot de passe de 12 caractères aléatoires ? (Minuscules, majuscules, chiffres, caractères spéciaux)

Comme ce souvenir de 20 mots de passe ?

On'utilise un gestionnaire de mots de passe.





Pourquoi un gestionnaire de mots de passe ?

• Besoins :

- Protéger nos mots de passe.
- Organiser nos mots de passe.
- Produire des bons mots de passe.
- Faciliter l'utilisation de nos mots de passe.

- \$\$\$





(parenthèse)

- Authentification forte ?
 - Authentification à deux (ou plus) facteurs (2FA)
 - Quelque chose qu'on connaît. (Mot de passe)
 - Quelque chose qu'on possède. (Clé numérique, OTP)
 - Ce que l'on est. (Biométrie)
 - Quelque chose qu'on sait faire. (Signature)
- Authentification à deux étapes (2SA)
 - SMS





Options

- Fureteurs
- Commerciales « gratuites »
- Logiciel libre





Fureteurs

- Firefox
- Chrome
- Opera
- IE

- Protéger nos mots de passe.
- Organiser nos mots de passe.
- Produire des bons mots de passe. **X**
- Faciliter l'utilisation de nos mots de passe.

- \$\$\$





Commerciales

- Lastpass
- 1Password
 - Version « gratuite » de produits commerciaux.
 - Solutions infonuagiques.
- Protéger nos mots de passe.
- Organiser nos mots de passe.
- Produire des bons mots de passe.
- Faciliter l'utilisation de nos mots de passe.
- \$\$\$





Sélection d'un logiciel libre

- Plateforme
 - Windows
 - Linux
 - OSX
 - IOS
 - Android
 - WEB (Auto hébergée)
 - JAVA
 - HTML5





Sélection d'un logiciel libre

- Maturité
 - Réputation
 - Communauté (Commanditaires)
 - Mises à jour
 - Documentation





Logiciels libres

- KeePass Password Safe





Plateforme

- Version 1 (Classic)
 - Entretien uniquement
 - Windows
- Version 2 (Professional)
 - Version active
 - Windows exclusivement
 - .net 2,0 minimum
 - Exécutable avec mono !





Protéger vos mots de passe

- Structure du fichier est :
 - Libre
 - Documenté
 - Algorithme de chiffrement robuste

<http://keepass.info/help/base/security.html>





Alternatives

- KeePassXC (Windows, OSX, Linux)
- KEYWEB (HTML 5)
- MiniKeePass (iBidule)
- KeePass2Android
- ...

<http://keepass.info/download.html>





Keepass

- Organiser nos mots de passe.
- Produire des bons mots de passe.
- Faciliter l'utilisation de nos mots de passe.
 - Plug-ins (<http://keepass.info/plugins.html>)





DÉMO





Questions Commentaires

