AGENCE
DU NUMÉRIQUE
EN SANTÉ

# ACSS

## Sensibilisation à la sécurité des mots de passe

*Statut : Validé* | *Classification : Publique* | *Version : v1.4*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

# SOMMAIRE

# 1 OBJET DU DOCUMENT

Les mots de passe sont au cœur de l'utilisation des outils numériques et jouent toujours un rôle important dans l'accès aux données. Que ça soit pour consulter ses emails, payer ses factures en ligne, accéder à des applications professionnelles, les occasions sont très nombreuses d'utiliser un mot de passe. Les perdre est très ennuyeux, se les faire voler est bien pire.

L'objet de ce document est donc de nous guider dans le choix de mots de passe pertinents et dans leur gestion optimale. Or ce problème est complexe et il n'existe malheureusement pas de solution simple comme nous allons voir. Néanmoins les solutions proposées dans ce document permettent d'augmenter sensiblement la sécurité des mots de passe que ceux-ci soient utilisés dans un cadre professionnel ou personnel.

Ce document aborde les sujets suivants :

- Un constat sur les mots de passe ;
- Les bonnes pratiques concernant les mots de passe ;
- La gestion des mots de passe.

# 2 CONSTAT

Destinés à protéger nos informations aussi bien professionnelles que personnelles, les mots de passe sont essentiels à notre sécurité dans l'espace numérique. Or bien que ces derniers fassent partie de notre quotidien, s'imprègnent de nos attaches – qui n'a jamais utilisé le nom de sa mère ou de son chat - nous les négligeons. Une fois sélectionnés pour accéder à un service, difficile d'y revenir. Parfois par peur de les oublier. Souvent par paresse… Et quand on en trouve un bon, et qu'il nous reste en tête, on commet l'erreur de l'utiliser partout... On appelle cela l'effet « boule de neige ».

Sachant que la plupart des sites stockent l'adresse de courriel et le mot de passe (de façon sécurisée ou pas), que l'adresse de courriel sert souvent de login (Paypal, Gmail, Facebook, etc.) et que généralement un même mot de passe est utilisé partout, il suffit juste qu'un pirate ait exfiltré des données contenant l'adresse de courriel et le mot de passe pour :

- Accéder à la boîte de courriel avec le mot de passe volé ;
- Accéder aux sites où l'adresse de courriel est utilisée comme login ;
- Accéder à tous les autres sites en utilisant la fonction de réinitialisation de mot de passe[1].

De plus, le pirate informatique n'est pas la seule personne dont il faut se protéger. En s'inscrivant sur un site douteux (téléchargement, moyen révolutionnaire pour gagner de l'argent en très peu de temps, etc.), et en renseignant son adresse de courriel et son mot de passe, il n'y a aucun moyen de savoir ce qu'en fera le propriétaire du site.

[1] http://www.aparame.com/article-pourquoi-ne-jamais-utiliser-2-fois-le-meme-mot-de-passe.php

# 3 LES BASES

## 3.1 La robustesse d'un mot de passe

Par abus de langage, on parle souvent de « force » d'un mot de passe pour désigner sa capacité à résister à une énumération de tous les mots de passe possibles[2]. Cette « force » dépend de la longueur du mot de passe et du nombre de caractères possibles (minuscules/majuscules, chiffres, ponctuation). Elle suppose que le mot de passe soit choisi de façon aléatoire.

Les mots de passe faibles sont toujours un des principaux vecteurs pour pénétrer un système d'information.

Attention, la longueur et la complexité d'un mot de passe ne sont pas synonymes de robustesse. Une méthode couramment utilisée par les utilisateurs afin de créer un mot de passe consiste à utiliser un mot issu du dictionnaire et y ajouter une suite de chiffres. Cependant, cette technique ne résiste pas à l'utilisation de règles d'automatisation disponibles avec les outils de « cassage » des mots de passe qui permettent de récupérer les mots de passe suivants pouvant être considérés comme complexes (caractères alphanumériques et longueur) :

- Password75001
- Bonjour !!
- Olivier22?
- m@m@n75000

Nous verrons qu'il est néanmoins possible malgré tout de rendre ce type de mots de passe plus robustes avec quelques modifications.

## 3.2 Les bonnes pratiques à respecter

Indépendamment de tout contexte, voici les recommandations minimales à respecter concernant le choix des mots de passe [3]:

- Avoir des mots de passe d'une taille d'au moins 12 caractères ;
- Avoir des mots de passe différents pour chaque application (pour contrer l'effet boule de neige) ;
- Choisir un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- Ne pas stocker les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible (post-it) ;
- Ne pas s'envoyer ses mots de passe par messagerie ;
- Modifier systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent (concerne plutôt les administrateurs) ;
- Attention aux questions secrètes (elles sont souvent utilisées comme un vecteur d'attaque[4]) ;
- Configurer les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis ;
- Renouveler ses mots de passe régulièrement (selon leur sensibilité).

Ces recommandations pouvant être difficiles à appliquer, nous verrons des méthodes permettant de générer des mots de passe les respectant et de les stocker de manière sécurisée.

[2] http://www.01net.com/editorial/584371/90-pour-cent-des-mots-de-passe-peuvent-etre-pirates/

[3] http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

[4] https://blog.elcomsoft.com/2009/05/secret-questions-are-vulnerable-to-guessing-attacks-study-says/

# 4 LA GESTION DES MOTS DE PASSE

Il y a plusieurs moyens de bien choisir ses mots de passe et de rendre ceux-ci plus robustes. Dans cette partie, nous verrons comment créer de bons mots de passe, comment les stocker de manière sécurisée.

## 4.1 Créer des mots de passe robustes

Nous allons voir trois méthodes pour créer des mots de passe originaux, différents, mais tout de même faciles à retenir.

### 4.1.1 La phrase secrète

Commençons par choisir une phrase à garder en tête. Par exemple : « le squash est le meilleur sport de France ». Prendre les initiales de la phrase et remplacer un caractère par un chiffre si possible (« de » devient « 2 », en anglais « for » devient « 4 », le « a » devient un « @ », etc.). Nous obtenons donc :

**lselms2F** (**l**e **s**quash **e**st **l**e **m**eilleur **s**port **d**e **F**rance)

Ensuite afin de compliquer le cassage du mot de passe, nous pouvons ajouter des caractères spéciaux. Par exemple, nous allons ajouter des caractères « # ».

**#lselms2F#**

Afin d'éviter l'effet boule de neige décrit plus haut, nous pouvons personnaliser le mot de passe pour chaque site utilisé. Nous pouvons par exemple ajouter les premières lettres du site ou de l'application et déplacer la majuscule d'un caractère vers la droite. Exemple pour Amazon :

**#lselms2F#aMa** (#lselms2F# + les 3 premières lettres d'Amazon puis le déplacement de la majuscule d'un caractère vers la droite).

Pour l'ANS, nous aurons : **#lselms2F#aNs**

Il est bien entendu possible de jouer avec toutes sortes d'ajouts, préfixes, suffixes, appendices en milieu de phrase ou autres règles exotiques. Simplement voici la base à retenir : une simple phrase, un ou plusieurs caractères spéciaux et une règle de différenciation. Ce mot de passe contient déjà un niveau de sécurité élevé, est facilement mémorisable et permet d'éviter l'effet boule de neige.

### 4.1.2 La méthode phonétique

Une autre méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple, la phrase « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am.

### 4.1.3 La faute d'orthographe

Nous avons vu précédemment que les mots de passe suivants, bien que complexes (caractères alphanumériques et longueur) n'étaient pas robustes car issus d'un dictionnaire :

- Password75001
- Bonjour!!
- Olivier22?
- Madrid789!
- Albert74587

Or avec l'ajout d'une faute d'orthographe, ces mêmes mots de passe deviennent robustes (car non compris dans un dictionnaire):

- Passwaurd75001
- Bomjour !!
- Olyvier22?
- Madryd789!
- Alberd74587

Concernant cette méthode et la méthode phonétique, penser à ajouter un préfixe/suffixe comme décrit dans la méthode de la phrase secrète afin d'éviter l'effet boule de neige.

## 4.2 Les gestionnaires de mots de passe

*En 2009, les utilisateurs avaient en moyenne 21 mots de passe. Ils en ont actuellement en moyenne 81.*[5]

Même si nous avons vu plusieurs méthodes afin de créer des mots de passe robustes, deux soucis de sécurité peuvent malgré tout se poser :

- la construction du mot de passe répond à un ensemble de règles définies (par exemple initiales d'une phrase + caractères spéciaux + 3 premières lettres du site), ce qui peut rendre le mot de passe prévisible (ce qui n'est jamais une bonne chose pour la sécurité) ;
- la nécessité d'avoir des mots de passe différents pour un nombre potentiellement élevé de comptes (mots de passe professionnels, personnels, etc.).

Virtuellement il existe un moyen d'avoir un meilleur niveau de sécurité grâce aux gestionnaires de mots de passe.

Un gestionnaire de mots de passe est un type de logiciel qui permet à un utilisateur de centraliser l'ensemble de ses identifiants et mots de passe dans une base de données accessible par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir[6].

En étant ainsi affranchi de la nécessité de se souvenir de ses différents mots de passe, nous pouvons nous permettre d'en choisir de plus robustes (voire totalement aléatoires) et d'avoir un mot de passe différent pour chaque compte. Les mots de passe sont stockés de manière chiffrée.

Le principal inconvénient d'un gestionnaire de mot de passe tient au fait que si le mot de passe principal est découvert, l'ensemble de ceux qui sont enregistrés est compromis.

Les gestionnaires de mots de passe peuvent être de différentes formes : logiciel autonome, plug-in, extension du navigateur web et être stockés soit en local, soit sur le web. Dans un contexte professionnel, il est recommandé de

[5] http://www.lesinrocks.com/2014/12/10/actualite/ce-mots-passe-disent-11537298/

[6] https://fr.wikipedia.org/wiki/Gestionnaire_de_mots_de_passe

stocker ceux-ci localement. En stockant ces mots de passe sur Internet avec des gestionnaires de mots de passe tels que Dashlane ou LastPass, nous prenons le risque que ceux-ci puissent être compromis[7].

Nous allons voir comment utiliser le produit KeePass[8], une solution certifiée par l'ANSSI.

### 4.2.1 KeePass

Le logiciel open source KeePass est un coffre-fort de mots de passe qui permet de gérer différents mots de passe de manière sécurisée et chiffrée. Tous les mots de passe sont stockés dans une base de données, verrouillée avec une clé maître ou un fichier clé. Il suffit de se rappeler du mot de passe maître ou de sélectionner le fichier clé pour accéder à la base de données.

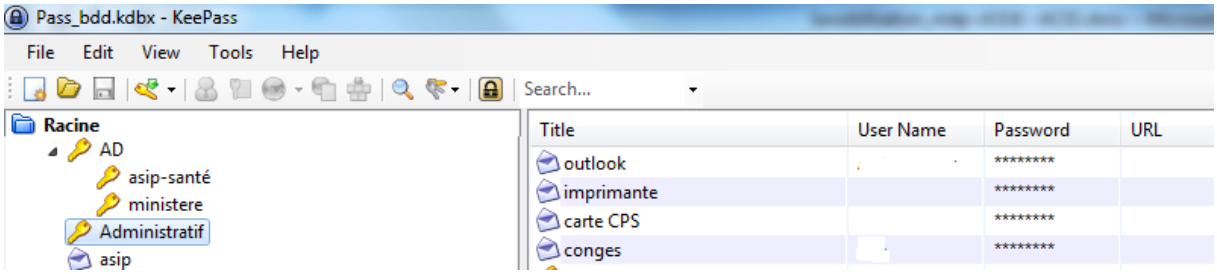



Figure 1 Stockage des mots de passe avec KeePass

Nous allons voir comment l'installer et l'utiliser[9]. A noter, qu'une version portable (sans installation existe) pour utiliser Keepass sur un support amovible de type clé USB.

#### 4.2.1.1 Installation

Cet outil est téléchargeable gratuitement sur son site officiel : https://keepass.info/. Attention, Keepass étant en version anglaise par défaut, il existe une astuce pour mettre celui-ci en français[10].

#### 4.2.1.2 Création de la base de données

Lors de la première utilisation, il est nécessaire de créer une base de données. La base de données peut être sécurisée par l'utilisation d'un **mot de passe principal** et / ou d'un **fichier clé**.

[7] http://www.numerama.com/magazine/33407-lastpass-pirate-les-mots-de-passe-exposes.html

[8] http://www.ssi.gouv.fr/uploads/IMG/cspn/anssi-cspn-cible_2010-07fr.pdf

[9] https://docs.ternum-bfc.fr/keepass-installation

[10] https://keepass.fr/comment-avoir-keepass-en-francais/


Figure 2 Création de la base de données

L'utilisation d'un gestionnaire de mots de passe sera le point de vulnérabilité de toute la sécurité. Le mot de passe / fichier clé sont les points faibles de la base de données, c'est pourquoi il ne faut pas les négliger. A l'inverse, leur perte entraînera l'impossibilité définitive de pouvoir retrouver les informations qu'elle contient. Il est important d'en faire des sauvegardes !

Par précaution, il convient de sauvegarder le fichier KeePass sur plusieurs espaces de stockage différents pour éviter de perdre définitivement des données importantes. Il est conseillé d'en faire une copie dans son disque partagé (afin qu'il soit sauvegardé automatiquement) et de le copier sur un support usb.

Le mot de passe doit être suffisamment robuste pour assurer un niveau de sécurité élevé mais attention il faut être capable de le retrouver.

Une fois la base de données créée, l'interface de l'outil apparaît :

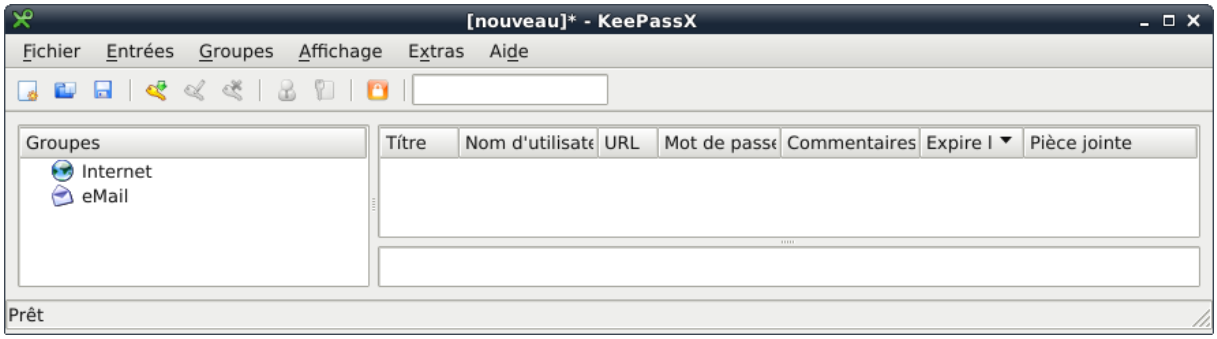



Figure 3 L'interface d'utilisation de Keepass

Il faut alors enregistrer la base (Fichier -> Enregistrer sous)

### 4.2.1.3 La création de mots de passe

Pour simplifier l'utilisation, il est suggéré de créer des groupes et des sous-groupes pour la recherche et la gestion des identifiants. Pour créer un nouveau groupe, il faut aller dans Groupes -> « Ajouter un nouveau groupe ».

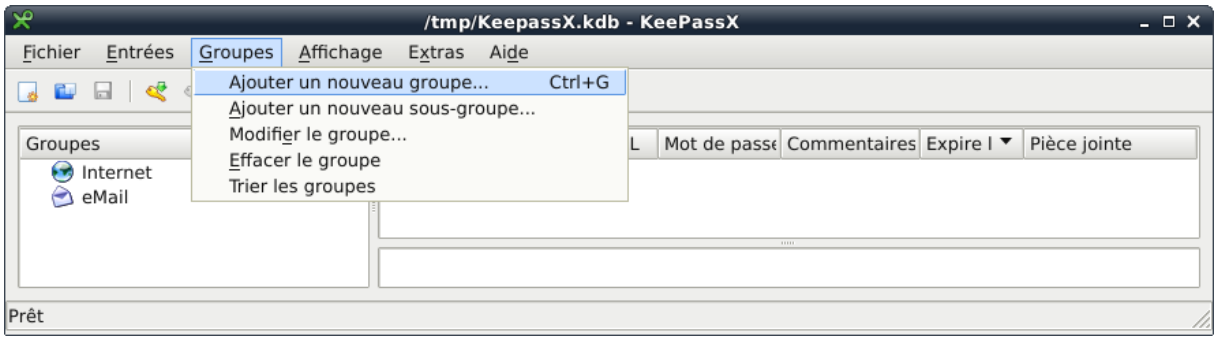



Figure 4 Création d'un nouveau groupe

Une fois le groupe créé (dans notre exemple Asip), on ajoute ensuite une nouvelle entrée (Menu Entrées -> « Ajouter une nouvelle entrée »). Par exemple, nous allons ajouter une entrée pour un répertoire partagé sous Windows.

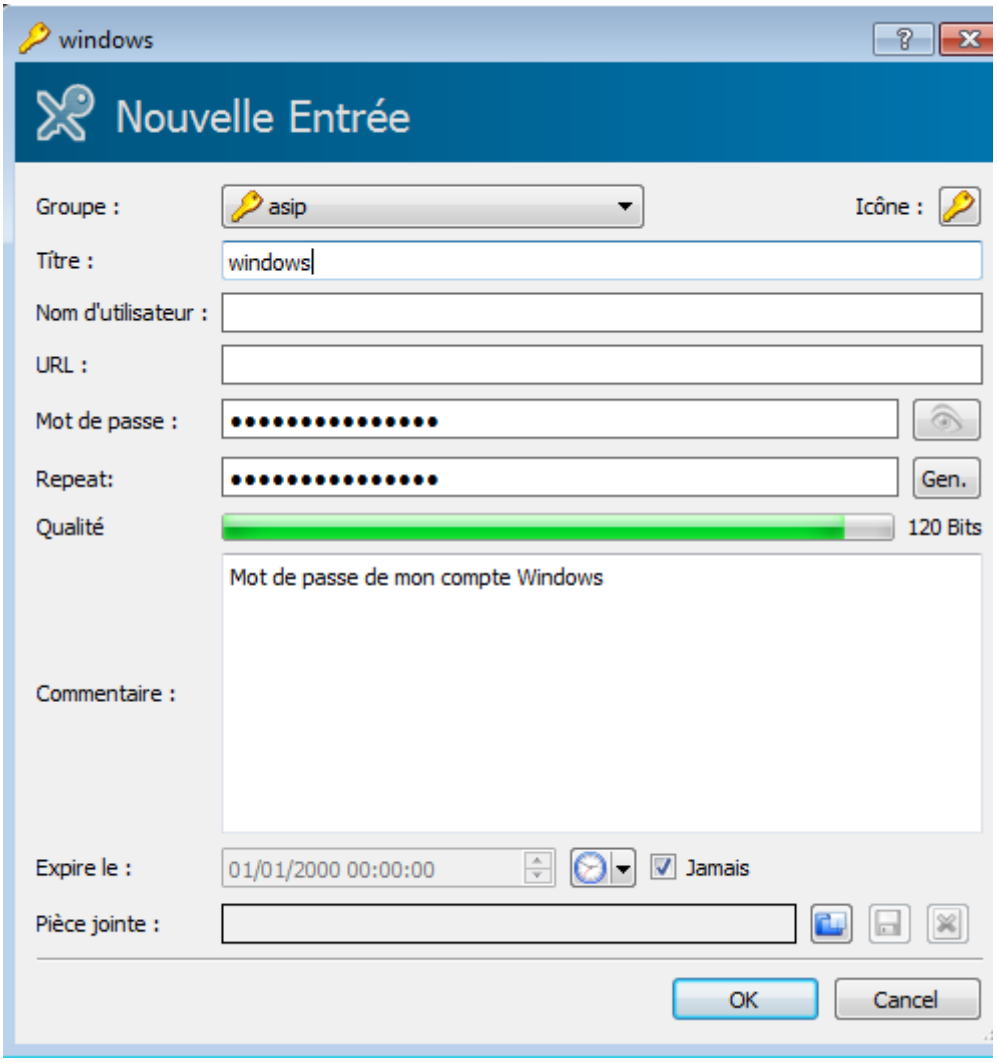



Figure 5 Ajout d'une nouvelle entrée

Pour récupérer le mot de passe, 2 solutions :

- Faire un clic droit sur l'entrée et copier le mot de passe

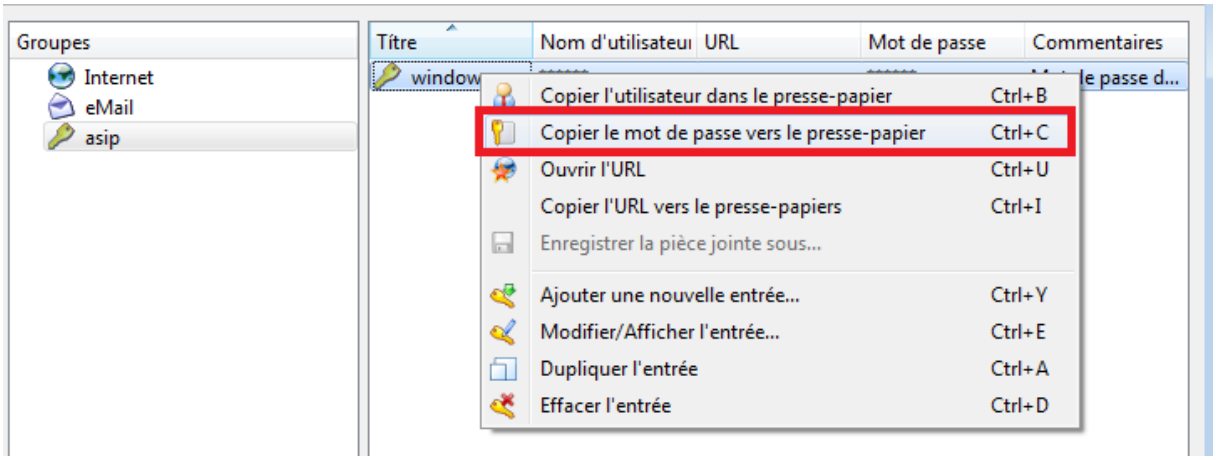



Figure 6 Récupérer son mot de passe n°1

- Cliquer sur l'entrée et sur la petite icône représentant un œil.

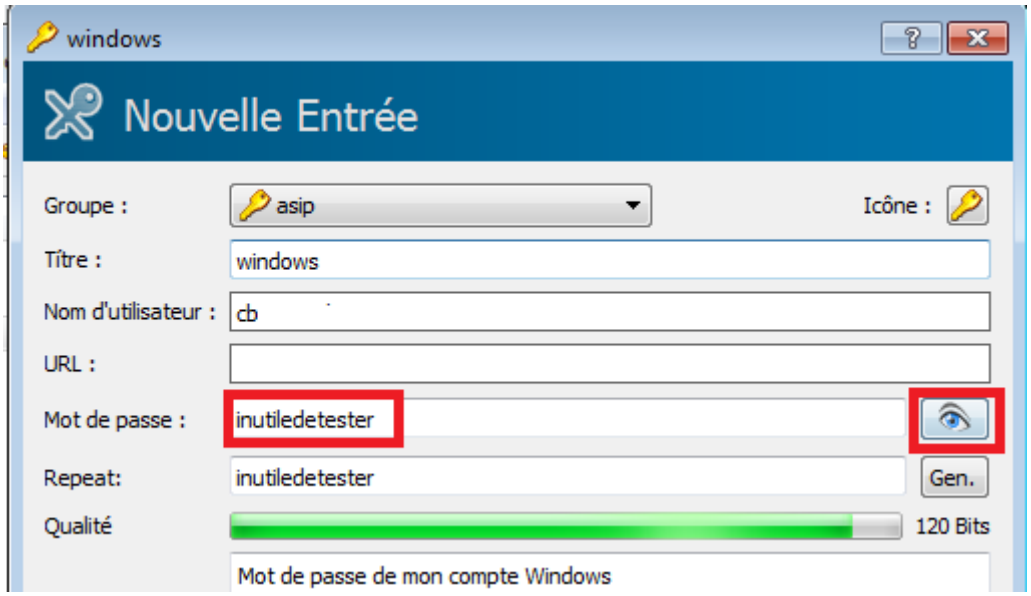



Figure 7 Récupérer son mot de passe n°2

Concernant le choix du mot de passe (par exemple lors de l'inscription sur un site Internet), il est plus sûr de générer un mot de passe aléatoirement. Le **générateur** permet ainsi de définir les caractères à utiliser ainsi que la longueur du mot de passe (le plus long possible puisqu'il n'est plus nécessaire de s'en souvenir).

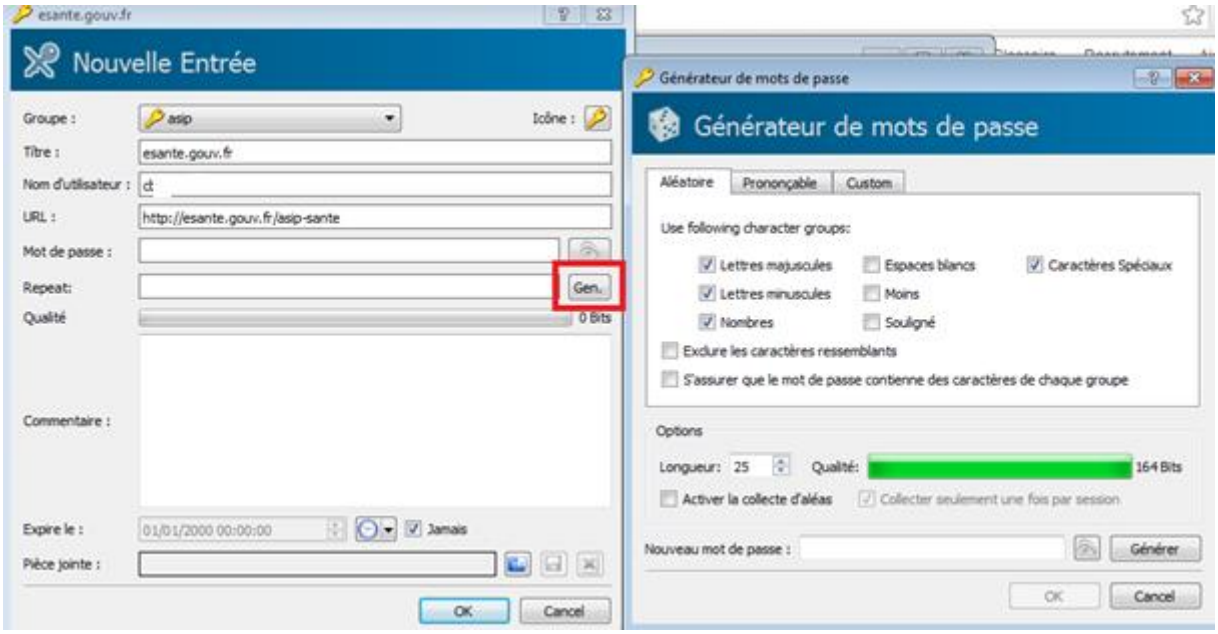



Figure 8 Utilisation du générateur aléatoire

### 4.2.1.4 Authentification

#### 4.2.1.4.1 S'authentifier sur un site web avec KeePass

KeePass gère l'authentification sur les sites web (fonction d'auto-complétion des champs login/mots de passe). Voyons par exemple comment utiliser cette fonctionnalité avec le site Amazon.fr.

La première étape est la même que décrite précédemment, à savoir créer une nouvelle entrée dans KeePass et de renseigner ses identifiants :

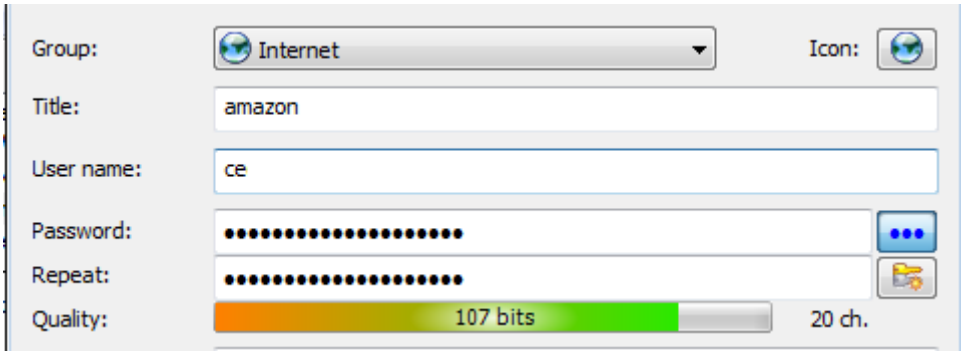
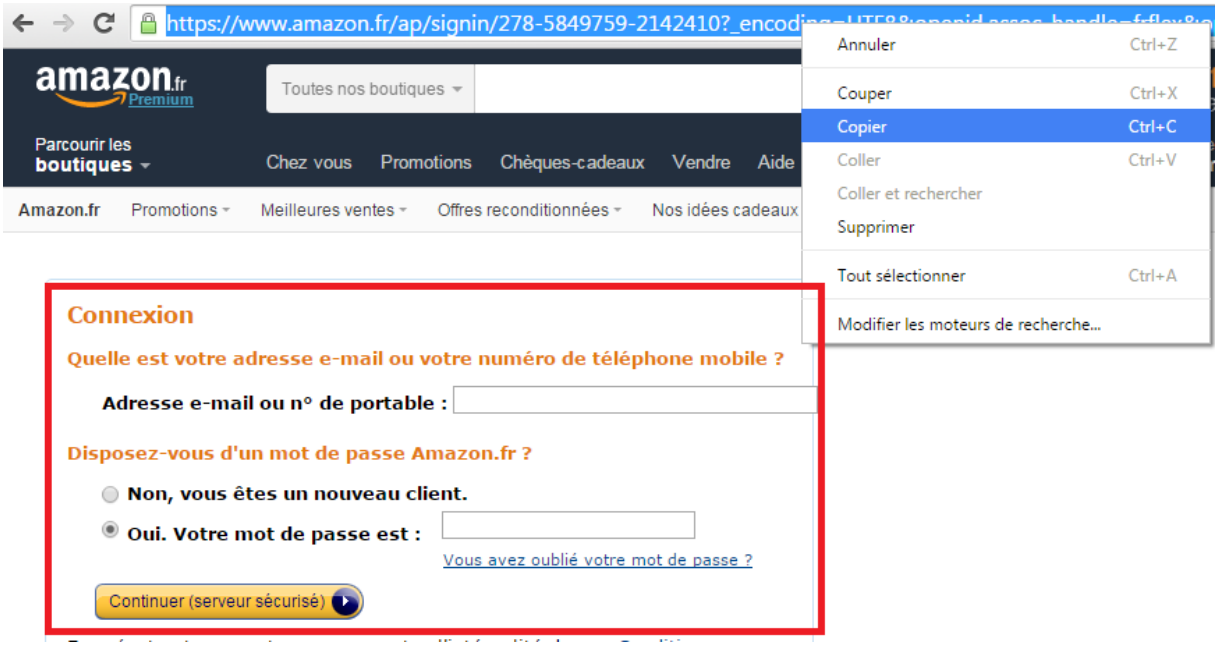
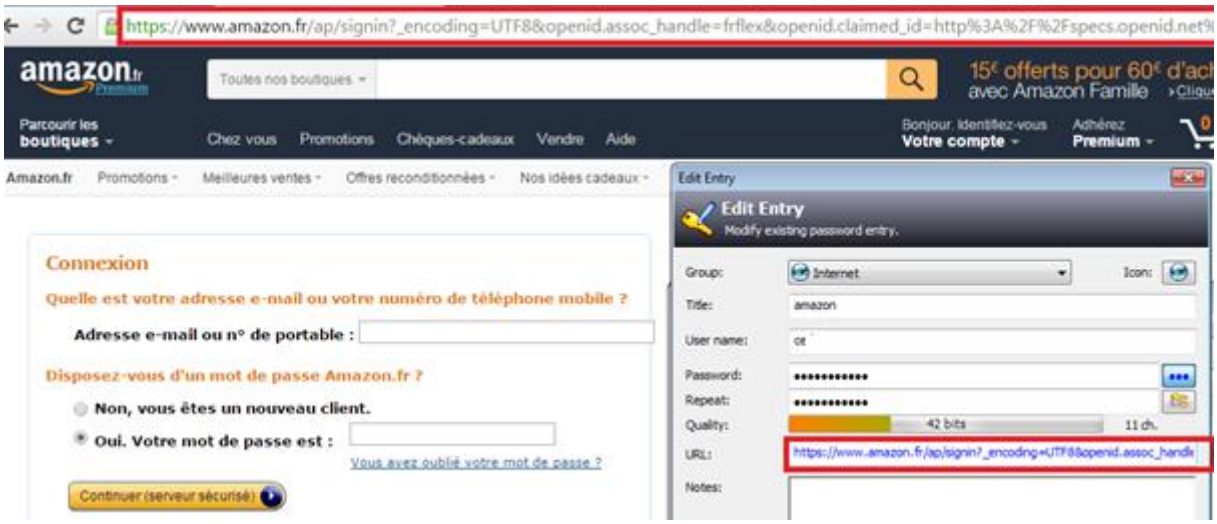



Figure 9 Utilisation de l'autocomplétion pour un formulaire web

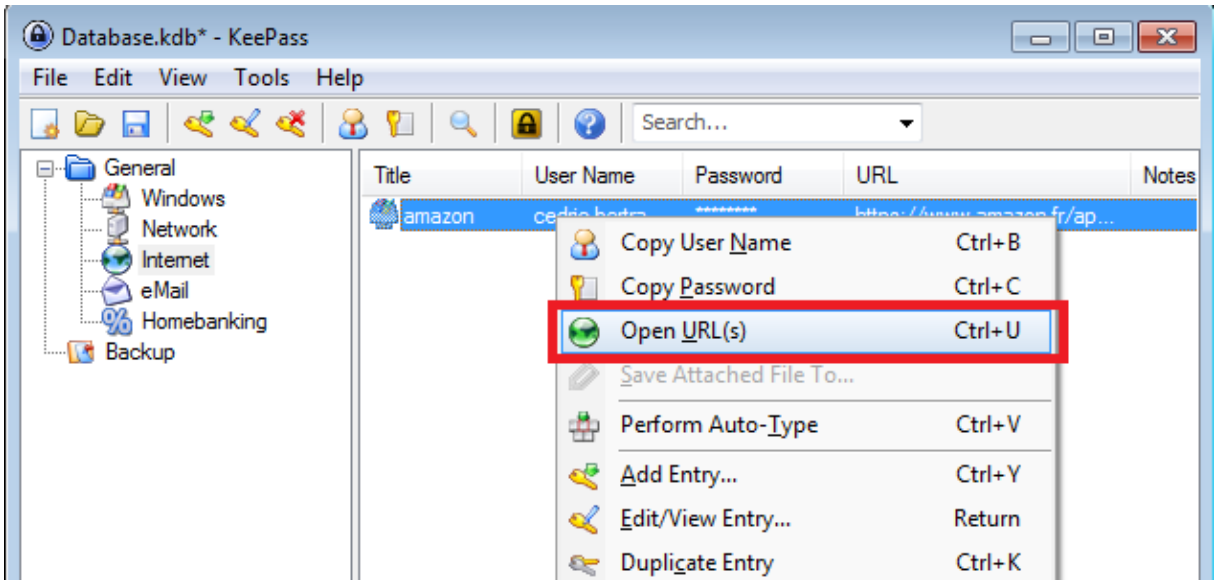
La deuxième étape consiste à se rendre sur la page d'identification d'amazon et à copier l'adresse de connexion.



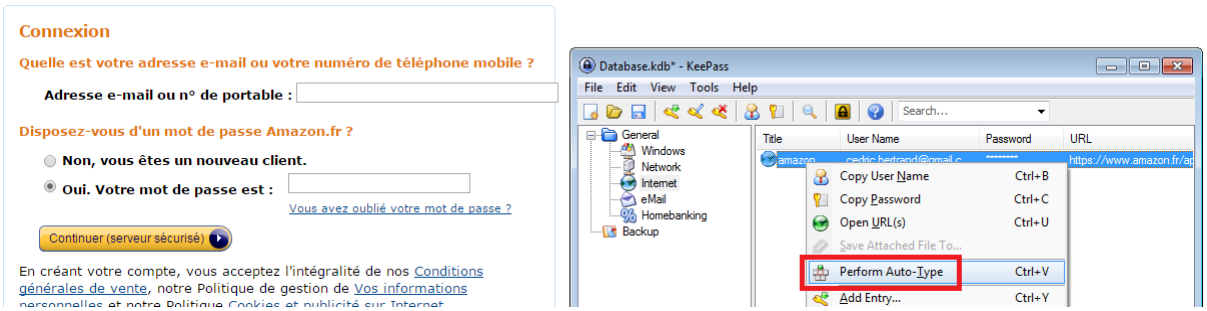

Ensuite on copie cette adresse et on l'indique dans la case URL de KeePass :



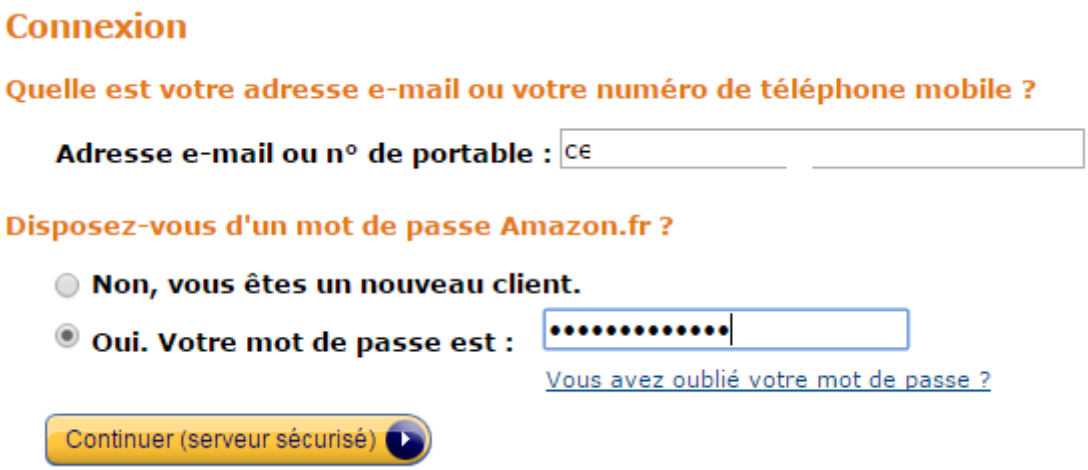

Les informations renseignées, on valide celles-ci. Puis nous faisons un clic droit sur l'entrée KeePass correspondante et on sélectionne l'option « open URL(s) » :




Un onglet (correspondant à l'adresse inscrite dans la case « URL » renseignée plus tôt) s'ouvre alors dans le navigateur. La dernière étape consiste ensuite à sélectionner l'option « Perform Auto-Type » (« Exécuter la copie automatique » en français) afin que les informations d'identification soient renseignées :




Les informations d'identification ont alors été complétées automatiquement :




#### 4.2.1.4.2 S'authentifier sur une application hors-ligne avec KeePass

Sur une application hors ligne (exemple : compte Windows, etc.), KeePass ne permet pas de fonction d'auto-complétion, il faut renseigner les informations d'authentification manuellement.

#### 4.2.1.5 Points importants

Les points importants à se rappeler pour l'utilisation de KeePass (ou d'un autre gestionnaire de mots de passe) sont :

- Le choix du mot de passe principal est primordial. Il doit être suffisamment robuste et en même temps pouvoir être mémorisé. Si le mot de passe principal est perdu, il n'y a aucune possibilité de récupérer le contenu du fichier coffre.
- Le fichier coffre doit être régulièrement sauvegardé. Ne pas hésiter à le sauvegarder dans son répertoire utilisateur sur le réseau (afin qu'il soit sauvegardé automatiquement), se l'envoyer par courriel ou encore le sauvegarder sur clé USB.

# 5 CONCLUSION


Conçus pour protéger l'accès aux systèmes et pour préserver la confidentialité de notre vie privée, les mots de passe sont un des points centraux de la sécurité des systèmes d'information. Synonymes de contraintes par la nécessité qu'ils soient différents, changés régulièrement, et robustes, il arrive qu'on les déteste.

En attendant les nouveaux systèmes d'identification qui puissent être avalés, implantés ou injectés[11], ils sont malheureusement incontournables dans notre quotidien et indispensables à la sécurité du système d'information. Nous contribuons chacun à la sécurité de notre système d'information par notre comportement, nos actions, et notre authentification.

[11] http://www.slate.fr/story/100693/futur-mot-de-passe

# 6 ANNEXES

## 6.1 Glossaire

| ***Acronyme*** | *Signification* |
|---|---|
| **ANSSI** | Agence Nationale de la Sécurité des Systèmes d'Information |
| **Gestionnaire de mot de passe** | Outil permettant de centraliser un ensemble de mots de passe |

## 6.2 Les différentes attaques sur les mots de passe

Afin d'éviter qu'un mot de passe ne soit facilement retrouvé par un outil conçu à cet effet, il peut être intéressant de connaître les différentes méthodes utilisées par les outils automatisés pour découvrir les mots de passe.

### 6.2.1 Les attaques par force brute

Cette attaque consiste à tester toutes les combinaisons possibles d'un mot de passe. Plus il existe de combinaisons possibles pour former un mot de passe, plus le temps moyen nécessaire pour retrouver ce mot de passe sera long.

Un mot de passe, d'une longueur minimale de douze caractères et constitué d'au moins trois des quatre groupes de caractères (minuscules, majuscules, caractères spéciaux et chiffres), sera difficilement découvert par cette attaque dans un temps raisonnable. En général, cette méthode est la dernière utilisée par les pirates.

### 6.2.2 Les attaques par dictionnaire

Cette attaque consiste à tester une série de mots issus d'un dictionnaire. Il existe toutes sortes de dictionnaires disponibles sur Internet pouvant être utilisés pour cette attaque (dictionnaire des prénoms, dictionnaire des noms d'auteurs, dictionnaire des marques commerciales...). En utilisant un mot de passe n'ayant aucune signification, cette attaque ne donnera aucun résultat. Cependant, plusieurs règles de transformation des mots du dictionnaire sont utilisées par les outils automatisés pour augmenter le nombre de combinaisons possibles. Citons par exemple :

– le remplacement d'un ou de plusieurs caractères du mot du dictionnaire par une majuscule

(bUreAU) ;

– le remplacement de certains caractères par des chiffres comme par exemple le S en 5 (mai5on) ;

– l'ajout d'un chiffre au début ou à la fin d'un mot (arbre9) ;

– l'ajout des mots de passe déjà découverts.

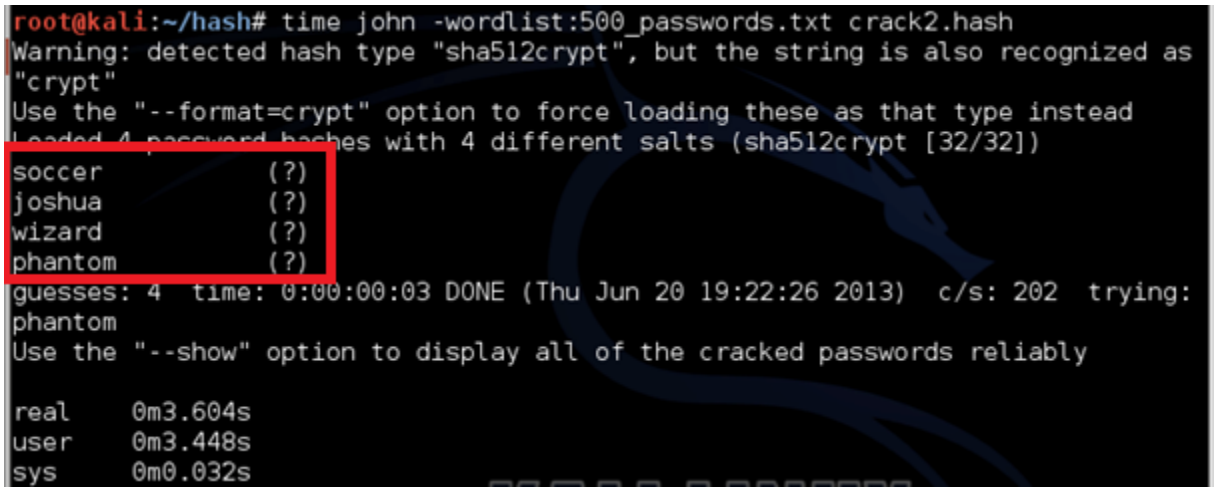



Figure 10 Exemple de logiciel pour casser les mots de passe

### 6.2.3 Les attaques hybrides

Ce type d'attaque est une combinaison entre l'attaque par force brute et par dictionnaire. Elle vise particulièrement les mots de passe constitués d'un mot traditionnel et suivi de lettres ou de chiffres (ex : Password95014).