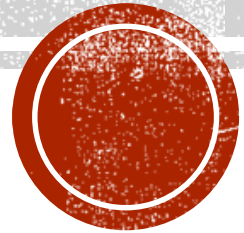
COMMENT GÉRER SES MOTS DE PASSE EFFICACEMENT ?



Et en toute sécurité

UNE DIFFICULTÉ CROISSANTE

- Un nombre d'identifiants et mots de passe en augmentation constante impossible à retenir
  - Démarche courantes : service-public, impôts, ameli, fournisseurs d'énergie, mutuelles, assurances, mon espace santé etc…
  - Sites de vente en ligne : Amazon, Ebay, Leboncoin, etc…
  - Sites de réservation : SNCF, Booking, Airbnb, EasyJet, loueurs de véhicules, théâtres, évènements culturels, Doctolib, etc…
  - Comptes informatique : comptes email, codes accès PC/tablettes/téléphones, codes wifi, codes cartes SIM, comptes Cloud
  - Finances: comptes bancaires, cartes de crédit, secure pass
  - Tous les sites qui offrent des services personnalisés : ACSMicro, réseaux sociaux etc…
- D'où la tentation d'utiliser le même mot de passe simple à retenir

POURQUOI NE PAS UTILISER LE UTILISER LE MÊME MOT DE PASSE SIMPLE À RETENIR

- Régulièrement de sites se font hacker, si ce site conserve vos id et vos mots de passe en clair il est facile ensuite de les essayer sur votre messagerie ou sur des sites plus sensibles que celui sur lequel ils ont été trouvés
  - **2,6 milliards** de comptes en ligne piratés en 2017 (Source : Dashlane)
- Votre mot de passe de messagerie est l'un des plus importants à protéger.
  - Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services sensibles auxquels vous pouvez accéder
- Les 8 mots de passe les plus utilisés sont cassés en moins d'une seconde :
  - 123456, Password, 12345678, qwerty, 12345, 111111, 123123, 1234567, (Source : SplashData)
- Vos infos ont de la valeur sur le Dark Web :
  - N° de sécurité sociale : 1 $
    E-mail et mot de passe : 0,70 à 2,30 $
    Permis de conduire : 20 $
    N° de carte de crédit : 8 à 22 $
    Dossier médical complet : > 1 000 $
    (Source : Keeper)

ALORS QUELLES SONT LES BONNES PRATIQUES ?

- Utilisez un mot de passe différent pour chaque service
  - Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable.

- Utilisez un mot de passe suffisamment long et complexe
  - Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

- Utilisez un mot de passe impossible à deviner
  - Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré.
  - Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

COMMENT CRÉER UN MOT DE PASSE SOLIDE ?

- La méthode des premières lettres :

  Un tiens vaut mieux que deux tu l'auras
  1tvmQ2tl'A

- La méthode phonétique :

  J'ai acheté huit CD pour cent euros cet après-midi
  ght8CD%€7am

Inventez votre propre méthode connue de vous seul !

ALORS QUELLES SONT LES BONNES PRATIQUES ? (SUITE)

- Changez votre mot de passe au moindre soupçon
  - Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

- N'utilisez pas vos mots de passe sur un ordinateur partagé
  - Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

ALORS QUELLES SONT LES BONNES PRATIQUES ? (SUITE)

- Changez les mots de passe par défaut des différents services auxquels vous accédez
  - De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

- Choisissez un mot de passe particulièrement robuste pour votre messagerie
  - Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Permettant d'utiliser la fonction « mot de passe oublié »
    Votre mot de passe de messagerie est donc l'un des plus importants à protéger.

ALORS QUELLES SONT LES BONNES PRATIQUES ? (SUITE)

- Activez la « double authentification » lorsque c'est possible
  - Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique. Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés.
- Quelques services proposant la double authentification
  - • Outlook/Hotmail, Gmail, Yahoo Mail…
    • Facebook, Instagram, LinkedIn, Snapshat, Tik Tok, Twitter…
    • Skype, Teams, WhatsApp, Zoom…
    • Amazon, eBay, Paypal…
    • Apple iCloud, Dropbox, Google Drive, OneDrive…

COMMENT MÉMORISER ET RETROUVER SES MOTS DE PASSE

- La méthode mnémotechnique, un pari risqué
  - Certains ont décidé de ne jamais stocker leurs mots de passe quelque part et ont adopté une méthode mnémotechnique. On peut par exemple partir d'un code secret de base que l'on est certain de retenir et que l'on va adapter pour chaque compte d'utilisateur en lui appliquant un algorithme secret. Exemple : mot de passe = [code secret] + [un dérivé du nom du service web].
  - Certes, on obtient des mots de passe qui sont tous différents, mais le fait d'utiliser un procédé mnémotechnique crée le risque qu'un pirate le découvre un jour.
- Le calepin, moins ridicule qu'on pense
  - Si vous en avez moins de vingt et que vous n'êtes pas très nomade, il est tout à fait envisageable d'utiliser un petit calepin.
    L'avantage, c'est qu'aucun pirate ne pourra voler son contenu par l'intermédiaire d'un malware. Il faudra quand même ne pas oublier de créer régulièrement une copie à déposer dans un endroit sûr, idéalement un coffre-fort. Pas vraiment pratique.
  - Mais il y a quand même un risque important, c'est de perdre ou de se faire voler ce support physique que l'on aura toujours à proximité. Le contenu pourrait alors être exposé à des tiers. Mais il existe des astuces pour réduire ce risque. Vous pouvez par exemple vous doter d'un code secret que vous serez le seul à connaître et que vous intégrerez systématiquement à chaque mot de passe.

COMMENT MÉMORISER ET RETROUVER SES MOTS DE PASSE (SUITE)

- Avec le navigateur,
  - Si vous avez plusieurs dizaines de mots de passe à gérer, vous pouvez être tentés d'utiliser votre navigateur pour enregistrer vos mots de passe,
  - C'est très pratique, les mots de passe sont remplis de façon transparente dans les formulaires
- Une solution à éviter
  - Les mots de passe ne sont pas toujours stockés de façon chiffrée.
  - Quelqu'un qui accède à votre espace de travail peut aller sur tous vos services protégés par mots de passe
  - La seul connaissance du mot de passe Windows permet de siphonner tous vos codes secrets
  - Si vous changez de navigateur ou d'appareil, vous n'avez plus accès à vos mots de passe
  - les navigateurs ne bénéficient pas d'une grande protection et sont des cibles faciles pour les hackers.
    En 2021, les navigateurs web les plus populaires ont été les cibles d'un malware qui volait les mots de passe enregistrés, baptisé CopperStealer par Proofpoint. La société spécialisée dans la sécurité informatique avait déjà identifié, en 2020, un logiciel malveillant similaire, appelé Redline Stealer qui œuvrait sous Windows. Les utilisateurs de Mac ne sont pas épargnés non plus, puisqu'ils ont dû faire face, en 2021, à un malware multiplateforme, nommé XLoader.

COMMENT MÉMORISER ET RETROUVER SES MOTS DE PASSE (SUITE)

- Utiliser un gestionnaire de mots de passe
  - Principe : Il s'agit d'un coffre fort sous forme d'une base de données, chiffrée et protégée par un mot de passe maître contenant les données que vous voulez protéger, les mots de passe mais aussi tout autre information confidentielle comme les numéros de carte de crédit, de passeport etc…
  - Ensuite viennent s'ajouter toute une ribambelle de fonctionnalités :
    - remplissage automatique des formulaires de connexion en ligne grâce à des extensions de navigateur,
    - synchronisation automatique entre multiples terminaux (PC's, tablettes, smartphones), grâce au cloud,
    - génération automatique de nouveaux mots de passe robustes,
    - audit de la qualité des mots de passe utilisés,
    - alertes de compromission,
    - authentification forte,
    - authentification biométrique
    - enregistrement de notes chiffrées, etc.

GESTIONNAIRES DE MOTS DE PASS
UN LARGE CHOIX

- Gratuits (open source)
  - Keepass
  - Bitwarden
- Payants
  - Enpass
    - Version gratuite : sans limitation sur PC, 25 mots de passe maxi synchronisés sur mobiles
    - Version payante affichée à 22€/an mais proposée à 11€/an ou 65€ à vie sur le Play Store
  - 1Password 24$/an
  - Lastpass 35€/an
    Version gratuite : un seul appareil
  - Dashlane 53€/an
    Version gratuite : 50 mots de passe maximum, un seul appareil

KeePass – les caractéristiques

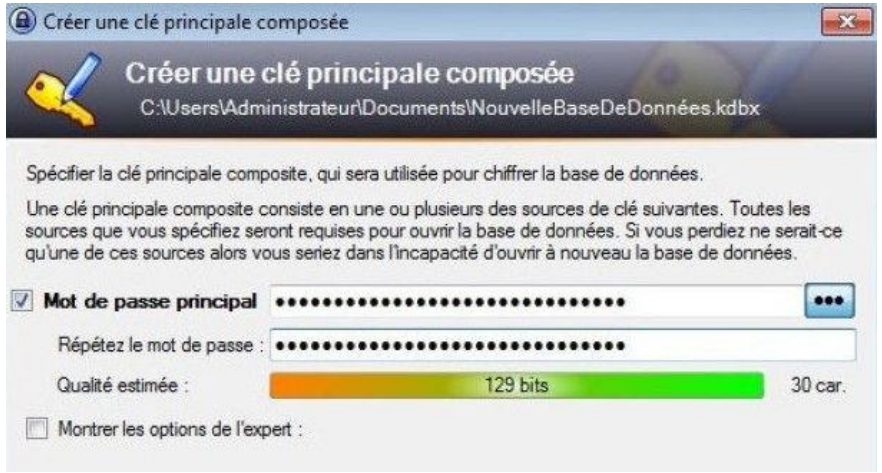
- Accès au coffre fort
  - par mot de passe unique
  - par fichier clé stocké sur un périphérique USB ou un CD
  - par le compte Windows
  - Par empreinte digitale sur smatphone
- Stockage du coffre en local ou sur un serveur cloud pour un accès partagé
- Cryptage AES (clé de 256 bits) ou TwoFish (clé de 256 bits + blocs de 128 bits)
- Classement des informations dans différentes catégories, avec ajout de commentaires, liens Internet, dates d'expiration, champs personnalisés, pièce jointes
- Générateur de mot de passe
- Indicateur de la qualité des mots de passe
- Sauvegardes automatiques
- Windows, macOS, Linux, Windows Phone, Android, iOS et BlackBerry.
- Existe en version portable et WEB (https://app.keeweb.info), ne nécessitant donc aucune installation
- Nombreuses versions non officielles et une multitude de plugins

KeePass – Mise en œuvre

- Télécharger et installer keepass ou keepass portable
  - Site de référence https://keepass.info/, Site en français https://keepass.fr/
- Pour stocker la base sur le cloud et y accéder depuis plusieurs appareils
  - Il faut mettre le plugin kee Anywhere https://keeanywhere.de/
    dans `C:\Program Files\KeePass Password Safe 2\Plugins`
  - A la première utilisation, il faut être connecté sur le compte cloud pour enregistrer les paramètres de connexion dans Kee Anywhere. Pour les autres utilisations il n'est pas utile d'être connecté sur le compte, ça se passe de manière transparente.
  - Support de **Dropbox, Google Drive, OneDrive, Box ou encore Amazon**
- Si on veut franciser le logiciel, mettre le fichier `French.lngx`
  https://keepass.info/translations.html
  dans `C:\Program Files\KeePass Password Safe 2\Languages`
- Utilisation sur Androïd: télécharger Keepass2Android sur Google Play Store

KeePass – Mise en œuvre (suite)

- Créer un coffre fort par : `Fichier>Nouveau` et choisir le mot de passe principal



Tuto vidéo : https://youtu.be/XTnDKJl1zOQ

- Créer ou importer les entrées dans le coffre

KeePass – Mise en œuvre (suite)

- Mise en œuvre de la saisie automatique, sans plugin
  - Positioner le curseur sur le premier champ du formulaire à remplir
    Dans keepass sélectionner l'entrée concernée et dans le menu contextuel choisir « Accomplir la saisie automatique » ou faire Ctrl+V
  - Il est possible de personnaliser la séquence par défaut {USERNAME}{TAB}{PASSWORD}{ENTER} ou par ex {USERNAME}{ENTER}{DELAY 1000}{PASSWORD}{ENTER}
- Mise en œuvre de la saisie automatique avec le plugin Keeform https://keeform.org/
  - Installer l'add-on pour Keepass
  - Installer l'add-on pour le navigateur (Chrome, Firefox, Edge)
  - Dans keepass sélectionner l'entrée concernée et double cliquez sur l'adresse URL, les champs userid et password se rempliront automatiquement

Enpass – les caractéristiques

- Accès au coffre fort
  - par mot de passe unique
  - par Windows Hello
  - Par empreinte digitale sur smartphone
- Stockage du coffre fort en local avec possibilité de synchronisation cloud ou directement sur un cloud
- Cryptage AES (clé de 256 bits)
- Classement des informations dans différentes catégories, avec ajout de commentaires, liens Internet, sections et champs personnalisés, pièce jointes
- Nombreux modèles prédéfinis : connexion, carte de crédit, licences, passeports etc…
- Générateur de mot de passe
- Audit des mots de passe en interrogeant le service https://haveibeenpwned.com
- Indicateur de la qualité des mots de passe
- Sauvegardes automatiques
- Windows, macOS, Linux, Android, iOS
- Existe en version portable

Enpass mise en œuvre

- Télécharger et installer Enpass ou Enpass portable
  - Site https://www.enpass.io/
- Lancer Enpass PC et suivre la procédure guidée :
  - choisir l'emplacement du coffre fort : sur le PC ou dans un cloud
  - cliquer sur créer un nouveau coffre et fournir le mot de passe principal
  - cliquer sur installer une extension navigateur pour valider la saisie automatique (Chrome/Firefox/safari/Edge/Opera/Vivaladi)
  - cliquer sur déverrouiller la version pro : accès au coffre par Windows Hello, thème sombre, modèles personnalisés)
- Aller dans les paramètres, onglet synchronisation et choisir la méthode de synchronisation multi-appareils : Onedrive, Dropbox, GoogleDrive, icloud, WebDAV, NextCloud, Box, Wifi réseau local
- Installer Enpass pour Androïd et valider la saisie automatique Androïd dans les paramètres Enpass Androïd en cochant « Préremplir>Service Préremplir Androïd »

Enpass mise en œuvre (suite)

- Cliquer sur + pour créer des éléments ou importer des éléments par Menu>Fichier>importer
- Mise en œuvre de la saisie automatique
  - Sur PC
    - Afficher la page de login
    - Cliquer sur l'icône Enpass en haut et à droite du navigateur, les données rentreront automatiquement dans le formulaire d'identification
  - Sur smartphone
    - Afficher la page de login
    - Taper sur le bouton « Préremplir » *image ci-contre* →