Hygiène numérique

Les mots de passe

Atelier proposé
par Medication Time

FONDATION afnic pour la solidarité numérique

Sous l'égide de Fondation de France

Un mot de passe, pourquoi ?

- Un mot de passe est un mot ou une série de caractères utilisés comme **moyen d'authentification** pour prouver son identité lorsque l'on désire accéder à un **lieu protégé**, à un compte informatique, un ordinateur, un logiciel ou à un service dont l'accès est limité et protégé. (définition wikipédia),
- Les mots de passe sont centraux dans nos utilisations du numérique : pour déverrouiller PC et smartphone, pour accéder à nos mails, à des services en ligne (banque, commerce, etc),
- Selon l’usage, il est plus ou moins important d’avoir un mot de passe robuste (cas de la boîte mail).

Les pires mots de passe

CLASSEMENT	MOT DE PASSE	TEMPS NÉCESSAIRE POUR LE DÉCHIFFRER
1	**password**	< 1 Seconde
2	**123456**	< 1 Seconde
3	**123456789**	< 1 Seconde
4	**guest**	10 Secondes
5	**qwerty**	< 1 Seconde
6	**12345678**	< 1 Seconde
7	**111111**	< 1 Seconde
8	**12345**	< 1 Seconde

Source : Nordpass.com 2022

Votre mot de passe ?

- Contient t’il des infos personnelles ?
- Est-il composé de chiffres, lettres min/maj, caractères spéciaux ?
- Est-il composé de plus 12 caractères ? De 10 ? de 8 ?

Temps requis pour déchiffrer un mot de passe

Traduction libre des données recueillies par Hive Systems via howsecureismypassword.net (2020)

NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	$7(10^{48})$ ans

Attaques sur les mots de passe

- Attaques en ligne (directement sur site) ou hors-ligne (suite à une fuite de données : voir https://haveibeenpwned.com/),
- Attaques par dictionnaires (fichiers contenant des milliers de mots de passe),
- Attaques par brute-force (tester toutes les combinaisons possibles),
- Attaques via sources ouvertes (par déduction via des données récoltés sur le net, les réseaux sociaux),
- Toutes ces attaques sont complémentaires et combinables !

Un bon mot de passe

- **Il doit être long** (pas moins de 12 caractères),
- Il doit être complexe (majuscules, minuscules, chiffres, symboles),
- Pas d’éléments personnels dedans, car peuvent être trouvé sur réseaux sociaux, ou facile à trouver pour un proche,
- Gardez le pour vous, ne pas le partager même avec des proches,
- En cas d’interception ou de fuite de données, il doit être unique,
- Pour certains usages, Il doit être pratique, facile à mémoriser.

Mémoriser des mots de passe sûrs

Pour combiner longueur et mémorisation :

les phrases de passe (pas moins de 6 mots) :

- Combinez des minuscules et des majuscules : '*MoN chat est uN MartieN*'
- Faites alterner des lettres et des chiffres : '*l3 ch4t m4ng3 d3s c4rott3s bl3u3s*'
- Incluez des symboles ou des signes de ponctuation : 'ch@t & ch1en$ égale copains ?'
- Combinez des mots empruntés à plusieurs langues : 'Let Them Eat 1e gateaU du ch()colaT'

ATTENTION

aux sites permettant de tester la robustesse de son mot de passe !!! (Ex : https://howsecureismypassword.net/)

- Ils peuvent enregistrer notre mots de passe, l’ajouter à des dictionnaires.
- Si utilisation, ne pas tester son vrai mot de passe mais un équivalent.

La gestion des mots de passe

Le carnet !

- Attention ou se trouve ce carnet, dangereux si à côté de l’ordi à la maison ou dans la sacoche du pc en déplacement.
- Demande de ressaisir manuellement les mots de passe pour chaque connexion.

La gestion des mots de passe

Le gestionnaire de mots de passe du navigateur !

- Par défaut les mots de passe sont stockés en clair dans le navigateur, si quelqu'un a accès à notre ordi, il a accès aux mots de passe.
- Possibilité de configurer un mot de passe maître pour sécuriser,
- Il faut faire confiance à l'éditeur du navigateur (Mozilla :Firefox, Google:chrome, Microsoft :edge,...),
- Certains navigateurs permettent de synchroniser ses identifiants entre plusieurs appareils via la création d'un compte tiers,

La gestion des mots de passe

Il y a le logiciel **KeepassXC** (https://keepassxc.org/)

Keepassxc est un logiciel de gestion de vos mots de passe ou coffre-fort.

KeepassXC (https://keepassxc.org/)

• KeepassXC permet de créer des mots (ou phrases) de passe robustes,
• KeepassXC est plutôt conçu pour une **utilisation locale**, sur un seul PC. Il ne permet pas facilement la synchronisation de vos mots de passe entre plusieurs terminaux,
• Keepassxc enregistre les mots de passe dans une **base de données chiffrées** accessible seulement avec le mot de passe maître. Cette bdd est un fichier facilement déplaçable,
• KeepassXC se **synchronise avec votre navigateur** via une extension pour auto-compléter les formulaires d'authentification.

La gestion des mots de passe

Il y a des **services en ligne** de coffre-fort et gestion de mots de passe.

• Ces services en ligne permettent de créer des mots (ou phrases) de passe robustes et de les **synchroniser avec votre navigateur** et **entre plusieurs terminaux**.

• Ils enregistrent les mots de passe dans une **base de données chiffrées** accessible seulement avec le mot de passe maître. Cette bdd est **hébergé en ligne**.

• Certains semblent être open-source et donc auditables, d'autres sont propriétaires,

• L'utilisation de base peut être gratuite, des abonnements payants permettent d'étendre le nombre de mots de passe enregistrés et/ou des fonctionnalités.

Quelques gestionnaires de mots de passe en ligne :

- BitWarden : https://bitwarden.com/
- Dashlane : https://www.dashlane.com/fr
- 1Password : https://1password.com/fr

- Bien se renseigner avant d’utiliser un de ces services

- Des assos proposent des services de gestion de mots de passe en ligne : voir sur https://chatons.org

La double authentification

- La double authentification (2FA) est une méthode d'authentification forte par laquelle un utilisateur peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) **après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification.** (source wikipédia),
- Un exemple est la réception sur son téléphone d’un code par texto pour valider un paiement en ligne.
- La 2FA peut aussi passer par une application sur le smartphone, mais obligation d’être possesseur du matériel adapté.

La fin des mots de passe

- Un passkey est un justificatif numérique utilisé comme méthode d'authentification pour un site web ou une application. **La norme des passkeys est un type d'authentification sans mot de passe,** promu par le World Wide Web Consortium et l'Alliance FIDO. Ils sont souvent stockés par le système d'exploitation ou le navigateur web et synchronisés entre les appareils d'un même écosystème à l'aide du nuage, mais ils peuvent également être limités à un seul appareil, comme une clé de sécurité physique.

Sources

- https://fr.wikipedia.org/wiki/Mot_de_passe
- https://fr.wikipedia.org/wiki/Robustesse_d%27un_mot_de_passe
- https://patrowl.io/fr/le-tableau-de-la-resistance-des-mots-de-passe)
- https://securityinabox.org/fr/guide/passwords/
- https://fr.wikipedia.org/wiki/Double_authentification
- https://en.wikipedia.org/wiki/Passkey_(authentication)

MERCI DE VOTRE ATTENTION !!!

Association MedicationTime

https://medicationtime.org/
contact@medicationtime.org

Supports des ateliers disponibles sur https://trashuniverse.org/

Atelier soutenu par la