Gérer ses mots de passe

ATHANOR
CENTRE CULTUREL

Ville de
Guérande

athanor-guerande.fr

Introduction

De nombreuses pratiques quotidiennes sont aujourd'hui médiées par l'informatique personnelle : finances, achats en ligne, démarches administratives, courriel et autres messageries…

Les mots de passe sont des éléments de sécurité cruciaux, l'équivalent de clés qui permettent de vous identifier sur un service en ligne et éviter qu'une autre personne accède à vos informations ou fasse des actions en votre nom. Un mot de passe trop simple ou répété peut facilement être forcé ou subtilisé et menacer l'ensemble de vos pratiques numériques.

Si ceux-ci semblent être une formalité irritante, il est possible de créer des mots de passe à la fois forts et mémorables à l'aide de quelques techniques simples.

1. Créer un mot de passe

Nordpass, « **Les 200 mots de passe les plus utiliés en 2022** », 2023, https://nordpass.com/fr/most-common-passwords-list/

Un bon mot de passe répond à quatre critères :

- **Long** (plus de 8 caractères),
- **Unique** (mélange lettres, chiffres et caractères spéciaux),
- **Impossible à deviner** (n'a pas de lien avec votre vie personnelle),
- **Mémorable** (pour ne pas dépendre d'une base de données ou être tenté d'aller au plus simple)

Choisir la base de son mot de passe

Deux méthodes sont disponibles pour commencer à créer un mot de passe fort : les mots au hasard ou la phrase de passe.

Les mots au hasard

Construisez une phrase simple (sujet - verbe - complément) à l'aide de trois mots choisis au hasard dans un dictionnaire, puis supprimez les espaces.

Exemple : *mouette ondule automatiquement* devient *mouetteonduleautomatiquement*

La phrase de passe

Choisissez un proverbe, une citation ou des paroles de chanson mémorable, et ne gardez que la première lettre de chaque mot.

Exemple : « *Tout le monde médit de moi, sauf les muets, ça va de soi.* » (Georges Brassens) devient *tlmmdmslmcvds*

Renforcer son mot de passe

Une fois la base du mot de passe choisie, il faut augmenter son entropie, sa complexité potentielle, et ainsi le rendre encore plus difficile à deviner ou à découvrir par énumération.

Remplacer des lettes

Remplacez certaines lettres par des symboles similaires : A = @, O = 0, E = €, S = $, I = 1, T = 7…

Exemple : *m0uetteondule@utomatiqu3m3nt*, *7lmmdm$lacvd$*

Ajouter des caractères spéciaux

Ajoutez des caractères non-alphanumériques, si possible au milieu du mot de passe (entre la proposition principale et subordonnée, en rétablissant la ponctuation…)

Exemple : *mouetteOndule!automatiquement*, *=tlmmdm;slacvds!*

Un bon mot de passe demeure un mot de passe mémorable, et le mieux est l'ennemi du bien : ne rendez pas votre mot de passe complexe au point de devenirs confus.

Différencier son mot de passe

Il est fortement recommandé d'**utiliser un mot de passe différent pour chaque site web ou service en ligne**. Il suffirait autrement d'une attaque informatique sur un seul site ou service mal sécurisé pour qu'un acteur mal intentionné puisse accéder à l'ensemble de vos informations personnelles.

Un moyen de différencier ses mots de passe à peu de frais est **d'ajouter un mot en rapport indirect avec le site ou service au mot de passe** : « voyage » ou « « locomotive » pour la SNCF, « finances » ou « monnaie » pour votre banque, « messages » ou « lettres » pour votre boîte mail…

Exemple *: !mouetteOndule;automatiquementvoyage*, *=tlmmdm;slacvds!finances*

Il est également possible d'utiliser plusieurs souches de mot de passe selon les sites et services concernés : un mot de passe pour les usages personnels, un mot de passe pour les usages professionnels, et un mot de passe les usages « jetables » (inscriptions à usage uniques, boutiques…).

2. Gérer ses mots de passe

Une bonne politique personnelle des mots de passe ne résout pas tous les problèmes : les sites et services sont toujours plus nombreux, et tous n'ont pas les mêmes demandes en matière de mots de passe. Certains sites imposent une longueur maximale, n'acceptent pas certains caractères spéciaux, demandent une majuscule… Certains services utilisent des codes PIN de 4 ou 6 chiffres ou ne vous laissent pas choisir votre identifiant.

Si noter et centraliser ses mots de passe présente des risques de perte ou de vol, oublier ses mots de passe peut bloquer l'accès à des services ou sites web à des moments cruciaux, et encourage la création de mots de passe simplistes et peu sécurisés.

Navigateurs web

Votre **navigateur web** (Microsoft Edge, Google Chrome, Opera) comporte un gestionnaire de mots de passe, qui peut enregistrer vos informations de connexion à des sites web, et remplir les formulaires de connexion pour vous lors d'une future visite.

Néanmoins, les informations enregistrées ne sont pas particulièrement protégées, et sont accessibles par toute personne ayant accès à votre ordinateur ou votre session. Confier vos mots de passe à votre navigateur vous rend également dépendant de celui-ci.

Keepass

Keepass est un logiciel dédié à la gestion sécurisée de mots de passe. Il s'agit d'un logiciel libre, open-source et entièrement gratuit. Il permet une meilleure organisation de ses mots de passe et un haut niveau de sécurité certifié par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Il est également possible d'imprimer sa liste de mot de passe pour conserver une copie physique.

PC Astuces, **« Mettre ses mots de passe en lieu sûr »**, https://www.pcastuces.com/pratique/windows/stocker_mots_passe/page2.htm

Attention, téléchargez Keepass uniquement depuis le site **keepass.info**

Keepass a été « porté » sur de nombreux supports : Android, iOS, macOS… Il est ainsi possible de copier/coller une base de données d'un PC à un smartphone ou tablette et d'en profiter à tout moment.

Keepass est à télécharger sur le site **keepass.info**. Le site et le logiciel sont en anglais, mais une traduction française est disponible (voir guide d'installation à droite).

Services payants

Des gestionnaires de mots de passe payants existent, la plupart sur abonnement : 1password, Bitwarden, Lastpass, Nordpass… Certains logiciels antivirus, tels que Kaspersky ou BitDefender, incluent également ces services dans leurs abonnements premium.

Corentin Bechade, *Les Numériques*, « Le piratage de LastPass plus grave que prévu, il est peut-être temps de changer vos mots de passe », 2022.

https://www.lesnumeriques.com/appli-logiciel/le-piratage-de-lastpass-plus-grave-que-prevu-il-est-peut-etre-temps-de-changer-vos-mots-de-passe-n201359.html

L'intérêt de ces services est de simplifier votre vie : stockage en ligne, synchronisation automatique sur tous les appareils, alerte en cas de fuite d'un site web…

Néanmoins, ces services ne sont pas plus sécurisés qu'un logiciel libre comme Keepass, voire présentent de nouveaux problèmes de sécurité : dépendance à un abonnement, gestion de vos informations personnelles par un tiers, possibilité de piratage de l'entreprise…

Carnet de mot de passe

Noter tous vos mots de passe sur un carnet dédié peut sembler dangereux, notamment en cas de perte, de vol ou de destruction. Néanmoins, ce carnet ne peut pas être piraté et ne requiert pas l'utilisation d'un appareil numérique : il peut donc s'agir d'une solution plus efficace que celles citées précédemment.

Des carnets à mots de passe dédiés sont disponibles dans le commerce, certains avec un système alphabétique similaire à ceux des annuaires. Vous pouvez également acheter et remplir ces carnets en deux exemplaires pour vous prémunir de toute perte.

Figure 1 - Un exemple de carnet à mot de passe

3. Le futur des mots de passe

Avec la démocratisation et l'importance accrue des outils numériques, des pratiques conçues pour et par des professionnels sensibilisés à la sécurité de l'information ne conviennent plus à un public général, qui désire un minimum de friction. Des alternatives au mot de passe traditionnel sont ainsi en cours de réflexion.

L'identification biométrique

L'**identification biométrique** consiste à identifier un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales : reconnaissance faciale ou vocale, empreintes digitales, voire démarche… Ces identifiants évoluent peu et sont quasiment impossibles à falsifier.

La reconnaissance faciale et digitale est d'ores et déjà disponible sur la plupart des smartphones, ce qui permet de les déverrouiller sans avoir à saisir d'identifiant.

L'identification biométrique est une technologie controversée : fichage des individus, exploitation commerciale, fuite des données… Le stockage et l'utilisation de ces données hautement personnelles par des états ou des entreprises privées peuvent interroger.

L'identification à deux facteurs

Trois facteurs permettent de s'identifier auprès d'un site ou d'un service :

- Ce que l'on sait (mot de passe),
- Ce que l'on possède (smartphone, adresse mail…),
- Ce que l'on est (biométrie : empreinte digitale, reconnaissance faciale…).

L'**authentification deux facteurs** supplée le mot de passe (ce que l'on sait) avec un facteur d'identification supplémentaire. Votre banque peut ainsi vous demander de valider une transaction depuis leur application smartphone ou en accédant à votre boîte mail (ce que l'on possède).

Pour une personne mal intentionnée, ce facteur supplémentaire rend considérablement plus difficile l'accès à des informations personnelles ou l'usurpation d'identité.

Les passkeys

Les **passkeys**, que l'on peut traduire par « clés d'accès », sont une technologie émergente où le smartphone est l'élément clé de l'identification. Contrairement à l'authentification deux facteurs, il n'est plus question de mot de passe : le smartphone gère le processus de bout en bout.

Nicolas Six, Le Monde, « Fini les mots de passe ? Les « passkeys » expliqués en trois questions », 2022, https://www.lemonde.fr/pixels/article/2022/09/12/fini-les-mots-de-passe-les-passkeys-expliques-en-trois-questions_6141237_4408996.html

Lors de la mise en place du passkey, le smartphone reçoit une clé, qui est stockée dans sa mémoire sécurisée. Il devient alors le seul appareil à pouvoir répondre à une « question » de sécurité qui lui est transmise lors de l'authentification. Il ne reste alors à l'usager d'à saisir un code PIN ou présenter son empreinte digitale.

Si cette technologie semble simple d'utilisation, elle présente le défaut de concentrer toutes les questions de sécurité sur l'objet smartphone. Il semble actuellement laborieux de transférer ses clés d'un appareil à l'autre, et il n'est pas possible de noter ses clés sur un coin de table. L'usager se trouvera également démuni en cas de perte, de vol ou de dysfonctionnement de son appareil.

Conclusion

Le mot de passe reste un système lourd et contraignant. Néanmoins, il s'agit du système le plus simple et le plus sécurisé imaginé jusqu'à présent. Avec quelques astuces et un peu de méthode, il est possible de gérer sa sécurité informatique sans trop de maux de tête.

Pour aller plus loin

- GIP ACYMA, *cybermalveillance.gouv.fr*, **« Pourquoi et comment bien gérer ses mots de passe ? »**, 2019, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe
- CNIL, **« Les conseils de la CNIL pour un bon mot de passe »**, 2017, https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe
- William Culbert, *Les Echos*, **« Opinion | Les données biométriques, un risque inédit pour la sécurité »**, 2019, https://www.lesechos.fr/idees-debats/cercle/opinion-les-donnees-biometriques-un-risque-inedit-pour-la-securite-992773

Date de dernière mise à jour : décembre 2025