

Créer un mot de passe secret, complexe et robuste

Bannir les mots de passe par défaut

Achèteriez-vous une nouvelle porte d'entrée pour votre maison dont toutes les portes du même modèle disposeraient de la même clé pour ouvrir ? Probablement non...

En informatique, c'est la même chose. Vous venez d'acquérir votre nouveau matériel informatique ? Un smartphone ? Un objet connecté ? Ces appareils disposent peut-être d'un mot de passe par défaut. Malheureusement il s'agit bien souvent d'un mot de passe générique et basique (pour ne pas dire inutile) du style « 0000 » vous permettant de vous y connecter pour le configurer après l'avoir déballé.

L'une des premières actions à réaliser sera de le modifier pour créer un mot de passe robuste. C'est à ce moment précis que votre porte d'entrée se verra accompagnée d'une nouvelle clé que vous seul aurez en votre possession.

Certains constructeurs d'appareils vous forcent à le changer, d'autres vous incitent simplement à le faire et les moins bons d'entre eux ne vous indiquent rien.

Exemple d'une notice de téléphone proposant le code PIN 0000 par défaut :

22.1. Modifier le code PIN de la carte SIM

Note: Votre carte SIM est protégée le code PIN. Il vous est demandé lorsque vous allumez votre mobile. Le code PIN par défaut est 0000 si vous ne l'avez jamais personnalisé. Pour la sécurité de vos données, il est conseillé de le personnaliser.

- 1 Sélectionnez **Paramètres de sécurité**.
- 2 Sélectionnez ensuite **Sécurité SIM**.
- 3 Puis sélectionnez **Modifier PIN**.
- 4 Saisissez le code PIN actuel de la carte SIM.
- 5 Saisissez un nouveau code PIN.
- 6 Appuyez sur le bouton central pour valider.
- 7 Saisissez le nouveau code PIN à nouveau pour confirmer la modification.

 La notion de **mot de passe par défaut** est détaillée dans le guide d'utilisation accompagnant votre nouveau matériel.

Les bonnes pratiques

Construire un mot de passe robuste

Vous devez maintenant créer un nouveau mot de passe pour remplacer celui qui vous a été donné par défaut ? Ou vous devez tout simplement vous créer un mot de passe pour votre messagerie ou votre compte de réseau social ?

La force d'un mot de passe dépend de **sa longueur** et du **nombre de caractères** possible pour le construire. Cela traduit la capacité de celui-ci à résister à la tentative de le trouver si on testait toutes les combinaisons de mots de passe possibles.

Prenez l'exemple d'un cadenas de vélo avec un code à 4 chiffres. Le nombre de combinaisons possibles est de 10 000 (0000 à 9999). En imaginant qu'une personne malintentionnée souhaite vous dérober votre vélo, il lui faudra tester toutes ces combinaisons. Si 2 secondes lui sont nécessaires pour tester chaque combinaison, il lui faudra moins de 6 heures pour voler votre vélo.

En mettant de côté le fait que le voleur peut briser votre cadenas (ce n'est pas l'objet de ce chapitre), si votre vélo a une valeur marchande élevée et qu'il est stocké dans un lieu accessible à l'abri des regards, l'opération est longue, fastidieuse mais pas impossible.

Pour un mot de passe informatique, c'est pareil. Si votre mot de passe est trop facile à deviner, une personne tierce peut en tester plusieurs pour tenter d'accéder à vos données. Et en matière d'informatique, la personne qui cherchera à trouver votre mot de passe se fera aisément aider par des programmes ou des logiciels qui testeront en boucle, à sa place, des milliers de combinaisons.

-  **L'attaque par brute force** consiste à trouver un mot de passe en testant une à une toutes les combinaisons possibles.
-  Pour pallier les tests en boucle, des sites proposent parfois un blocage de compte lorsqu'un nombre trop élevé de mots de passe erronés est saisi ou une temporisation de quelques secondes ou quelques minutes pour permettre la saisie d'un nouveau mot de passe.

Les bonnes pratiques

Pour un mot de passe robuste, il est recommandé généralement qu'il contienne au moins 12 caractères et qu'il comporte au moins 3 des 4 types de caractères parmi les suivants :

- minuscules
- majuscules
- chiffres
- caractères spéciaux (! ou \$ par exemple)

Il est bien entendu que les 12 caractères ne doivent ni être une suite alphabétique du type abcdefghijkl ni être une suite de touches du clavier azertyuiopqs, et encore moins un mot du dictionnaire !



ANSSI

Agence nationale de la sécurité des
systèmes d'information

[in](#) [d](#) [t](#) [e](#) [n](#)

[DECLARATION VULNERABILITE](#) |
 [EN CAS D'INCIDENT](#) |
 [ALERTES](#) |
 [PRESSE](#) |
 [RECRUTEMENT](#)

Taille de clé équivalente	Force d'un mot de passe
64	très faible
64<80	faible
80<100	moyen
> 100	fort

COMMENT RENFORCER MON MOT DE PASSE ?

Une question qui se pose fréquemment est : mais quels critères dois-je employer pour mes mots de passe ? Huit caractères, dix caractères, des chiffres, des majuscules, etc ? Une première règle à savoir est qu'il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe. Mais pour s'en rendre compte, le mieux est d'utiliser le petit calculateur ci-dessous :

Longueur : caractères.

Alphabet :

Un mot de passe avec ces caractéristiques est à peu près équivalent à une clé de bits.

QUELQUES RESULTATS TYPIQUES

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).

Le site Internet de l'ANSSI permet d'estimer la force d'un mot de passe.

Les bonnes pratiques

Une technique permettant de mixer différents types de caractères et de disposer d'un mot de passe robuste tout en le retenant de manière assez simple consiste à créer celui-ci à partir des premières lettres des mots d'une phrase. La **CNIL** (Commission Nationale de l'Informatique et des Libertés) propose sur son site Internet un tel générateur, disponible à l'adresse www.cnil.fr/fr/generer-un-mot-de-passe-solide

☛ En parcourant le site de la CNIL, vous pouvez vous créer un mot de passe fort à partir d'une phrase. Exemple, à partir de la phrase « Je me crée un mot de passe fort de 12 caractères et 3 caractères différents ! », vous générerez le mot de passe Jmcumdpfd12ce3cd!. Gardez cette phrase pour vous !

The screenshot shows the CNIL website's password generator interface. At the top, the CNIL logo is centered, with navigation links for 'MES DÉMARCHES', 'THÉMATIQUES', 'TECHNOLOGIES', 'TEXTES OFFICIELS', and 'LA CNIL'. To the right are buttons for 'PARTICULIER' and 'PROFESSIONNEL', and social media icons for search, Facebook, and Twitter. The main heading is 'Générer un mot de passe solide'. Below it, a subheading states: 'Cet outil vous aide à construire un mot de passe fort et simple à retenir. Aucun mot de passe n'est récupéré par le site de la CNIL.' The first step is '1 Choisir une phrase que vous retiendrez facilement'. It provides three examples of phrases and a section 'En panne d'inspiration ?' with a link to 'Nos astuces pour construire un mot de passe sûr'. A text input field is labeled 'Saisir votre phrase' with the placeholder 'Saisir une phrase, de préférence ponctuée'. Below this, a list of requirements for a strong password is shown: 1. Un nombre, 2. Une majuscule, 3. Un signe de ponctuation ou un caractère spécial (dollar, dièse, ...), 4. Une douzaine de mots. At the bottom is a button labeled 'Générer votre mot de passe'.

CNIL.

PARTICULIER PROFESSIONNEL

MES DÉMARCHES | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL |

Générer un mot de passe solide

Cet outil vous aide à construire un mot de passe fort et simple à retenir.
Aucun mot de passe n'est récupéré par le site de la CNIL.

1 Choisir une phrase que vous retiendrez facilement

Exemples :

- Mon mot de passe est un secret bien gardé depuis 25 ans !
- Le rire seul échappe à notre surveillance. Natalie Clifford-Barney, 1920.
- Le carré de l'hypoténuse est égal à la somme des carrés des 2 autres côtés.

En panne d'inspiration ?
Nos astuces pour construire un mot de passe sûr

Saisir votre phrase

Saisir une phrase, de préférence ponctuée

Pour un mot de passe de douze caractères ou plus, votre phrase doit contenir au moins :

- 1 Un nombre
- 2 Une majuscule
- 3 Un signe de ponctuation ou un caractère spécial (dollar, dièse, ...)
- 4 Une douzaine de mots

Générer votre mot de passe

Page de génération d'un mot de passe solide sur le site Internet de la CNIL.

Les bonnes pratiques

Nous l'avons vu, votre mot de passe ne doit pas être facile à deviner par une tierce personne. Oubliez donc tout de suite le prénom de vos enfants, celui du chien ou de votre conjoint(e). Cela vous protégera non seulement des personnes qui vous connaissent (et connaissent le nom de votre chien...) mais aussi de personnes qui vous sont totalement inconnues et qui, par recoupement de données (en consultant votre profil Facebook par exemple), trouveraient aisément ce type d'information.

Certains systèmes ou objets ne vous permettront peut-être pas de créer des mots de passe robustes avec différents types de caractères, mais simplement avec des chiffres par exemple. Tentez donc d'être le plus inventif et le plus secret possible.



Le code de verrouillage de votre téléphone est-il votre date ou votre année de naissance ? Si oui, vous savez ce qu'il vous reste à faire !

Un usage, un mot de passe

En matière de sécurité, il vaut mieux anticiper et supposer que les précautions et les mesures prises ne sont jamais suffisantes. Dans le cas des mots de passe, l'anticipation revient à se placer dans la situation où votre mot de passe, aussi solide soit-il, pourrait être découvert. Ainsi, deux conseils en matière de bonne gestion de ses mots de passe :

- séparez bien le domaine personnel du domaine professionnel, n'utilisez pas de mots de passe identiques (ce sujet est évoqué dans une autre section de ce livre),
- n'utilisez pas le même mot de passe pour tous vos accès. Si vous vous faites dérober votre mot de passe ou bien si le site Internet sur lequel vous vous connectez subit une fuite de données, c'est l'ensemble de vos comptes qui deviendraient accessibles.

La difficulté à disposer d'autant de mots de passe est de tous les retenir. Des solutions existent, nous les détaillons un peu plus loin.

Certains sites Internet proposent des systèmes facilitant l'accès à leurs services. Par exemple, le service public propose de vous identifier pour accéder à vos services sur les sites des administrations (CAF, impôts, sécurité sociale, etc.) à partir du compte d'une autre administration dont vous êtes déjà usager. Cela vous permet de ne retenir qu'un seul identifiant et un seul mot de passe pour accéder à l'ensemble des sites des services administratifs en ligne.

Les bonnes pratiques

Pour mettre en œuvre ce système, il vous suffit de vous rendre sur le site d'une des administrations partenaires avec **FranceConnect** et de cliquer sur le bouton. Vous pouvez alors vous connecter à cette administration à l'aide d'identifiants que vous connaissez déjà (impôts, Assurance Maladie, La Poste, MSA, Mobileconnectetmoi). FranceConnect transmet alors aux administrations partenaires les informations vous concernant (nom, prénom, sexe, date et lieu de naissance).



Je choisis un compte pour me connecter sur :

Ameli

impots.gouv.fr Assurance Maladie L'Identité Numérique

mobile connect et moi santé famille retraite services Alicem

☐ Se souvenir de mon choix

Exemple ici : vous pouvez vous connecter au site de l'Assurance Maladie (Ameli) avec un identifiant et un mot de passe d'une autre administration.

👉 En cas de vol du mot de passe, vous ne serez pas obligé de le modifier sur l'ensemble des plateformes administratives, mais une seule fois.

Les bonnes pratiques

En entreprise, on rencontre parfois **le système SSO** (*Single Sign-On*) qui permet d'accéder à l'ensemble des applications nécessaires en se connectant une unique fois. Comme pour le système précédent, cette technologie permet bien des avantages, notamment la simplicité pour les utilisateurs lors de l'identification ou la modification du mot de passe des différentes applications en une seule fois. Cependant, elle comporte naturellement des risques. Parmi ceux-ci, on peut aisément comprendre qu'une personne malintentionnée qui aurait connaissance du mot de passe de l'utilisateur peut alors accéder à l'ensemble des applications dudit utilisateur. Pour cette raison, idéalement, la mise en œuvre de SSO devra a minima s'accompagner d'un système d'authentification à deux facteurs, système que nous détaillerons un peu plus loin.

Renouveler son mot de passe

Il est conseillé de changer vos mots de passe régulièrement. Certains sites Internet vous forcent d'ailleurs à le faire. De manière générale, il est vivement conseillé de modifier régulièrement son mot de passe : imaginez une personne malintentionnée qui aurait découvert votre mot de passe et qui se connecterait sur votre compte quotidiennement sans que vous le sachiez ? Le changement de votre mot de passe l'empêcherait de poursuivre ses accès frauduleux.



Certains sites Internet ou certaines applications vous envoient une notification par e-mail ou SMS lorsqu'une connexion sur votre compte depuis un nouvel appareil est détectée. Cela permet de déceler un éventuel accès frauduleux à votre compte.