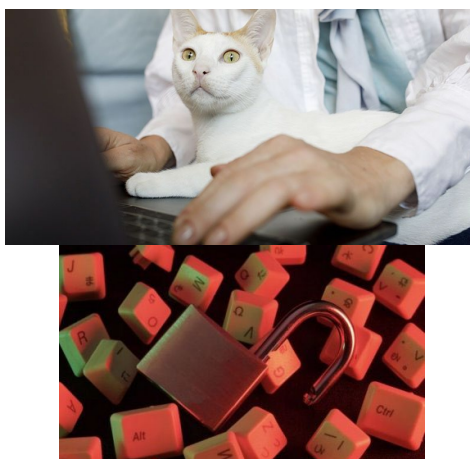


Tuto : comment créer un mot de passe solide ?



Choisir un mot de passe solide (et pas medor22)

Saviez-vous qu'en France, la suite de chiffres "123456" était le mot de passe le plus utilisé en 2022 ? C'est le vôtre ? Eh bien sachez que c'est également le mot de passe le moins sécurisé. L'entreprise de sécurité numérique NordPass publie régulièrement son classement des pires mots de passe utilisés dans le monde. Il détaille aussi le nombre de fois où le mot de passe a été utilisé et combien de temps il faut à un hacker pour le trouver. Spoiler alert : il faut moins d'une seconde pour trouver la suite de chiffres précédemment mentionnés (et pas besoin d'être un hacker pour ça, à vrai dire).

À l'heure où les pirates informatiques sont de plus en plus performants, on a besoin de mots de passe résistants. Vous avez peur de les oublier s'ils sont trop nombreux ou trop compliqués ? N'ayez crainte, voici quelques astuces pour devenir de véritables virtuoses du mot de passe.

Le mot de passe le plus utilisé... est aussi le pire

Chaque année, NordPass publie une enquête sur "les 200 mots de passe les plus utilisés". En 2022, l'entreprise notait que "malgré une sensibilisation croissante à la cybersécurité, les vieilles habitudes ont la vie dure." En effet, les mots de passe considérés comme faibles sont toujours autant utilisés. "Par rapport aux données observées en 2021, 73 % des 200 mots de passe les plus courants en 2022 restent les mêmes", note le rapport.

En France, les trois mots de passe les plus populaires sont "123456", "123456789" et "azerty" (comme l'ordre des lettres de votre clavier). Résultat, ils peuvent être déchiffrés en moins d'une seconde, comme 83 % des mots de passe de la liste en 2022.

Dans le monde, le mot **"password"** (« **emot de passe** », en français) a été utilisé par les internautes près de **4 929 113 fois**, pour sécuriser leur compte. Faisant de lui le numéro 1 de la liste.

Globalement, NordPass révèle des usages communs à de nombreux pays. Par exemple, "l'utilisation de son propre nom pour sécuriser ses comptes" reste encore fréquente". De même, les internautes ont tendance à opter pour la facilité en utilisant "des combinaisons simples de chiffres, de lettres et de symboles". Raison pour laquelle le mot de passe "123456" reste si populaire dans l'Hexagone mais aussi en Colombie, au Brésil ou encore au Japon.

3 astuces pour créer des mots de passe sécurisés

Connaissez-vous la technique dite par "force brute" ? Il s'agit d'essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Une technique d'autant plus facile pour les hackers qui utilisent des ordinateurs pouvant tester des dizaines de milliers de combinaisons par seconde.

Heureusement, pas besoin de se faire des nœuds au cerveau pour apprendre à créer ses mots de passe. En fait, la plateforme gouvernementale Cybermalveillance nous délivre quelques astuces simples à mettre en place pour que ça devienne un jeu d'enfant.

Voici Les règles à retenir pour créer des mots de passe comme un pro : Opter pour un mot de passe long et complexe : une longueur minimum de 12 caractères, un mélange de majuscules et de minuscules, des chiffres, et symboles (ponctuation ou caractères spéciaux).

Ne pas y inclure de lien direct avec vos données personnelles ou biographiques, par exemple votre date de naissance ou celle de vos enfants. En effet, ces informations se trouvent facilement sur Internet.

Ne pas choisir un mot du dictionnaire ou une suite de chiffres comme "123456". Aujourd'hui, les pirates utilisent des outils automatisés leur rendant le déchiffrement de ces combinaisons extrêmement simple.

Vous craignez de manquer d'inspiration ou pire, de ne pas vous souvenir de tous ces mots de passe ? Pas de panique, les générateurs et gestionnaires de mots de passe peuvent vous sauver la mise. **Voici deux solutions pour vous faciliter la vie** :

 **KeePass** est un logiciel libre certifié par L'ANSSI. Il dispose d'une fonction vous permettant de générer des mots de passe complexes et robustes. En plus, il vous permet de stocker en toute sécurité vos mots de passe.

 Sur le site de la CNIL, vous pouvez également vous entraîner à générer un mot de passe fort et simple à retenir. Pour cela, il vous suffit de taper votre mot de passe dans la barre de recherche du site, puis de cliquer sur "générer votre mot de passe".

Gérer vos mots de passe pour les rendre plus sûrs

Avoir de solides mots de passe c'est bien mais savoir les gérer c'est encore mieux.

Parce qu'en matière de sécurité la forme est aussi importante que le fond, **voici les règles à retenir pour gérer ses mots de passe comme un pro** : Varier les mots de passe, en veillant à n'utiliser qu'un mot de passe par appareil ou "compte sensible" (boîte e-mail, banque en ligne,...).

Les changer régulièrement : idéalement tous les 3 mois et surtout au moindre soupçon de leur divulgation ou de leur compromission.

Ne pas le noter sur un support informatique non protégé. Cela vaut pour les notes de votre téléphone et les fichiers de votre ordinateur. Et ne nous parlez surtout pas de post-it ... Si vous avez peur de l'oublier, mieux vaut utiliser un gestionnaire de mot de passe.

N'utilisez pas vos mots de passe sur un ordinateur partagé. Si vous devez vraiment le faire, privilégiez le mode ""navigation privé", n'enregistrez pas votre mot de passe et pensez à bien fermer votre session.

Ne jamais le communiquer à un tiers. D'ailleurs, on ne le répétera jamais assez mais aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone.

Activer la double authentification ou "authentification à deux facteurs", chaque fois que c'est possible.

N'hésitez pas à changer les mots de passe par défaut qui vous sont proposés par les différents services auxquels vous accédez. Et toi Orange tu fais quoi ? À travers son programme d'ateliers numériques, Orange s'engage à rendre le numérique accessible à tous. Les ateliers sont ouverts à tous les âges et à tous les niveaux de connaissance, qu'on soit client Orange ou pas. Ils durent en moyenne 1h et peuvent s'effectuer en ligne ou en physique. Durant l'atelier "Protéger ses données personnelles", vous apprendrez par exemple à créer un mot de passe robuste, vous prémunir des arnaques les plus fréquentes en ligne, effacer votre historique de navigation, sécuriser vos achats en ligne, ou encore préserver vos équipements (mobiles, ordinateurs, tablettes). Pour participer, rien de plus simple. Il vous suffit de réserver la date et l'heure de votre cours en ligne, en cliquant sur : [ce lien](#) ! publié le 4 mai,