Dans le cadre de ses fonctions d'enseignant, Antoine va régulièrement consulter ses mails professionnels. Par simplicité, il a choisi un mot de passe faible : sa date de naissance. Ce mot de passe a très facilement été reconstitué lors d'une attaque utilisant un outil automatisé : toutes les personnes identifiées dans son carnet d'adresses vont recevoir un mail de Phishing bien conçu, certain cliqueront sur les liens et perdront le contrôle de leurs ordinateurs suite à une attaque de malware.

Malgré le développement de mécanismes d'authentification intrinsèquement plus robustes, l'usage des mots de passe est encore relativement répandu, notamment pour l'authentification sur Internet.

L'ANSSI[1] recommande très fortement, dans tous les cas où cela est possible, l'utilisation de technologies d'authentification forte (utilisation de certificats d'authentification sur carte à puce, utilisation de schéma d'authentification à plusieurs facteurs, etc.). Cependant, l'utilisateur n'est pas toujours maître des choix qui s'offrent à lui en matière d'authentification.

Fig. 1: la clé OTP utilisée dans l'éducation nationale pour sécuriser certains accès

Pour protéger vos informations, il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Voici quelques recommandations :

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- Ne demandez jamais à un tiers de générer pour vous un mot de passe ;
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles ;
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible ;
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle ;
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres.

1 ANSSI : Agence nationale de la sécurité des systèmes d'information

Calculer la « force » d’un mot de passe

Qu’est-ce que la « force » d’un mot de passe ?

Par abus de langage, on parle souvent de « force » d’un mot de passe pour désigner sa capacité à résister à une énumération de tous les mots de passe possibles.

Cette « force » dépend de la longueur L du mot de passe et du nombre N de caractères possibles. Elle suppose que le mot de passe est choisi de façon aléatoire. Elle se calcule aisément par la formule N.L.
Mais il est plus difficile d’estimer si la valeur ainsi obtenue est suffisante ou pas.

Comment estimer la « force » d’un mot de passe ?

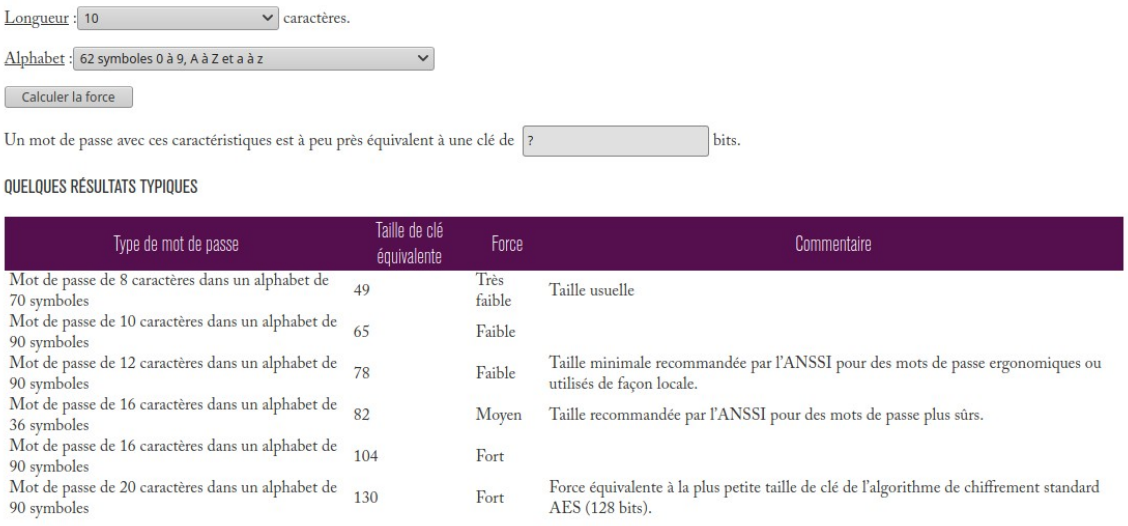
La force d’un mot de passe peut être estimée par comparaison avec les techniques cryptographiques. Une taille de clé cryptographique de 64 bits est aujourd’hui considérée comme non sûre, car les capacités de calcul modernes permettent de retrouver cette clé en énumérant toutes les clés possibles. Or une telle clé peut être vue comme un mot de passe de 64 caractères où les seuls caractères possibles sont 0 et 1. La « force » d’un tel mot de passe est donc 64.

Les règles édictées par l’ANSSI en matière de mécanismes cryptographiques imposent par exemple une taille de clé minimale de 100 bits. Il est même recommandé une taille de clé de 128 bits pour des clés dont l’usage présumé est de longue durée. Il est par ailleurs communément admis que des tailles de clé de 80 bits sont désormais exposées à des attaques utilisant des moyens techniques conséquents.

Ces chiffres permettent de calibrer la « force » d’un mot de passe.
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 :



Longueur : 10 caractères.

Alphabet : 62 symboles 0 à 9, A à Z et a à z

Calculer la force

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

QUELQUES RÉSULTATS 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).

Fig. 2: le calculateur de l'ANSSI
https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

Tel que l'indique l'ANSSI :
il n'existe pas de règle universelle. La robustesse d'un mot de passe dépend en pratique :

- de la force intrinsèque du mot de passe, c'est-à-dire sa complexité intrinsèque;
- du mécanisme mis en oeuvre pour vérifier le mot de passe et de ses caractéristiques techniques (temps de vérification, mécanisme cryptographique sous-jacent notamment) ;
- du modèle d'attaquant considéré. La résistance contre tous les types d'attaquants imaginables est intrinsèquement plus difficile à atteindre que la simple résistance aux attaques opportunistes par lesquelles l'attaquant va essayer les mots de passe les plus triviaux les uns après les autres sans connaissance a priori du système cible ;
- éventuellement, en fonction des mécanismes techniques mis en oeuvre et du modèle d'attaquant,
- du nombre d'authentifications ratées autorisées avant blocage d'un compte protégé par le mot de passe ;
- des mécanismes d'alerte éventuels. Certains systèmes permettent à l'utilisateur de prendre connaissance de manière sûre du nombre d'échecs d'authentification infructueux. D'autres lèveront une alerte à destination d'un administrateur ou bloqueront le compte de l'utilisateur concerné.

Néanmoins, voici quelques règles simples pour vous aider à construire des mots de passe plus efficaces :

- Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire.
- Deux méthodes simples peuvent vous aider à définir vos mots de passe :
  - • La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;
  - • La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » : aE2lP,lJ2Géa!
- Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle...) ne doivent jamais être réutilisés pour d'autres services.
- Modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box...) ;
- ne pas conserver les mots de passe dans des fichiers ou sur des Post-its ;
- ne pas préenregistrer ses mots de passe dans les navigateurs, lors de l'utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements...).

Pour aller plus loin

Phrase secrète vs mot de passe

Une phrase secrète (passphrase, en anglais) est un groupe de mots et de caractères utilisé comme moyen d'authentification pour prouver son identité lorsque l'on désire accéder à une ressource ou à un service dont l'accès est protégé. C'est l'équivalent d'un mot de passe, mais en plus sécurisé.

Les mots de passe sont généralement courts, de 6 à 10 caractères. Ces derniers sont généralement suffisants pour se connecter aux comptes utilisateur dans les systèmes d'exploitation (Windows, GNU/Linux, macOS…) lesquels sont programmés pour détecter plusieurs tentatives d'accès incorrectes et pour protéger les mots de passe stockés. En revanche, ils ne sont pas sûrs pour une utilisation avec des systèmes de chiffrement.

Les phrases secrètes sont beaucoup plus longues, de 25 à 64 caractères (espaces compris). Leur plus grande longueur rend les phrases secrètes beaucoup plus sûres que les mots de passe.

Pour garantir une **meilleure protection contre les pirates**, la plupart des programmes de sécurité vous permettent d'ailleurs d'entrer une phrase secrète plutôt qu'un mot de passe, comme :

- Les protocoles de sécurité Wi-Fi WPA/WPA2 ;
- Les gestionnaires de mots de passe (LastPass, KeePass…) ;
- Les logiciels de chiffrement de données (VeraCrypt, BitLocker…) ;
- Le logiciel de chiffrement cryptographique PGP, souvent utilisé pour signer, chiffrer et déchiffrer des e-mails ;

Dans l'idéal, une phrase secrète devrait être :

- Connue uniquement par vous ;
- Assez longue pour être sûre ;
- Difficile à deviner – même par quelqu'un qui vous connaît bien ;
- Facile à retenir ;
- Facile à saisir.

Les logiciels de gestion de mots de passe

Bitwarden. Gérer tous vos mots de passe sur tous vos appareils - https://bitwarden.com/

Comment se souvenir de la liste des mots de passe que génère chaque jour notre vie numérique ? À moins d'avoir une mémoire d'éléphant ou s'adonner aux mots de passe simplistes ou aux mémos sur de petits bouts de papier collé ici ou là. Sans compter que les choses se compliquent avec des services qui pour notre bien demandent de changer régulièrement le mot de passe que vous avez eu tant de peine à retenir.

Un logiciel comme Bitwarden va prendre soin de l'ensemble des identifiants et mots de passe dont vous avez besoin dans votre quotidien numérique.

Il va créer pour vous un coffre sécurisé dans les nuages. Vous allez ainsi pouvoir accéder à vos données de n'importe où, sur n'importe lequel de vos appareils. Votre chambre forte est optimisée pour une utilisation sur les ordinateurs de bureau, les ordinateurs portables, les tablettes et les téléphones.

Vos données sont entièrement cryptées avant de quitter votre appareil, vous seul y avez accès. Même l'équipe de Bitwarden ne peut pas lire vos données.

Vos mots de passe accessibles de partout

Bitwarden est très pratique à utiliser au quotidien. Il se présente sous différents formats. Vous pouvez télécharger une application dédiée pour Mac, PC ou Linux. Vous avez aussi la possibilité de l'installer sur votre smartphone ou tablette. Il est enfin possible d'accéder à l'ensemble de vos mots de passe via le web et le site de Bitwarden.

Mais l'utilisation la plus pratique reste l'extension à installer sur votre navigateur. Bitwarden en propose pour la plupart d'entre eux. Une fois installé, l'accès à un site sécurisé par un mot de passe est très facile. Si le mot de passe est déjà présent dans votre coffre sécurisé Bitwarden, lorsque vous arrivez sur la page de connexion, un clic sur le petit logo Bitwarden et aussitôt votre identifiant et votre mot de passe s'inscrivent automatiquement dans les champs de connexion. Magique. Si vous n'avez pas de compte et que vous en créez un, dans ce cas Bitwarden va vous demander si vous souhaitez mémoriser et conserver dans votre coffre-fort le mot de passe.

Le service est de qualité et va vous simplifier la vie. Vous vous demanderez même après comment vous avez pu vivre sans lui. Enfin, vous n'allez plus avoir besoin de vous encombrer la mémoire avec des mots de passe dans tous les sens. Enfin, il faudra quand même vous en souvenir d'un. Un seul, mais il est important. C'est le mot de passe "maître" qui va vous permettre d'accéder au coffre-fort de Bitwarden et à son précieux contenu.

Bitwarden est libre et gratuit, mais vous pouvez soutenir le projet avec un abonnement de 10€ pour toute une année.

Firefox Lockwise - https://www.mozilla.org/fr/firefox/lockwise/

Une autre solution fiable, libre et gratuite, Firefox Lockwise, le gestionnaire de mots de passe du navigateur internet Firefox.

Il permet entre autres :

- **Enregistrer et stocker vos mots de passe**. Il vous aide à vous identifier sur les sites et services WEB ;
- Compléter automatiquement les champs identifiants et mots de passe déjà enregistrés ;
- **partager les mots de passe** entre appareils avec la synchronisation (Android, IOS, Windows, Mac, Linux,etc.) ;
- Vous **prévenir lorsque le mot de passe est compromis** via Firefox Monitor.

Ici donc pas besoin d'une extension supplémentaire, tout est intégré dans votre navigateur Firefox et est donc totalement transparent.

Dans un cas comme dans l'autre, ces deux applications stockent vos mots de passe de manière sécurisés sur des serveurs en les chiffrant en AES-256-GCM.

De quoi être bien mettre à l'abri vos mots de passe et identifiants en vous facilitant la vie !