publié le 08/10/2010 - mis à jour le 17/12/2021

« Sésame, ouvre-toi ! »

Pour que le mot de passe ne soit plus une passoire...

Descriptif :

Pour que le mot de passe ne soit plus une passoire...

Sommaire :

> ***Le mot de passe !*** *Si je suis un lecteur pressé qui n'est pas d'emblée séduit à l'idée de lire plusieurs paragraphes sur la question, je peux passer directement à la page 3 qui propose deux méthodes simples et efficaces pour créer et mémoriser rapidement des mots de passe « forts » (voir la définition du CERTA)… des travaux pratiques, en somme !*
> *jml*

● Le mot de passe… partout

DaveBleasdale - licenceCC/by

Aujourd'hui, les élèves et les membres de la communauté éducative utilisent quotidiennement les outils et produits numériques tant à l'intérieur qu'en dehors de l'école. Cet usage, en progression constante, se doit d'être accompagné, afin que l'élève et l'adulte puissent faire un **usage citoyen et responsable** de ces technologies.

S'il ne fait plus de doute que l'outil informatique est désormais incontournable voire indispensable pour les acteurs du système éducatif, quelques lourdeurs de fonctionnement peuvent exister et sont parfois mal vécues par les usagers.

Dans cette famille des raideurs irritantes, le mot de passe est souvent dans le peloton de tête.
Intimement lié aux indispensables règles de sécurité, il est souvent perçu, à la création et à l'usage, comme une contrainte rébarbative contrariant la souplesse d'utilisation que l'on espère de l'outil informatique.
Qui n'a d'ailleurs pas déjà manifesté sa mauvaise humeur lorsqu'il s'agit de retenir un énième mot de passe ? Qui ne s'est jamais tourné vers son administrateur pour un mot de passe -encore- oublié ?
Ces contrariétés peuvent avoir pour conséquences immédiates de réduire notre **vigilance** quant aux règles de sécurité minimales attendues… par exemple : on note son mot de passe sur un *post-it* collé consciencieusement sur l'écran de son ordinateur ; on suggère à l'élève de noter le sien sur son carnet de correspondance pour ne plus l'oublier ; on utilise le même mot de passe pour des applications diverses et de niveau de risque différent (courrier électronique, réseau de l'établissement, compte bancaire, messagerie instantanée, etc.)… en somme, on vide le mot de passe de sa raison d'être : « **limiter et protéger l'accès à une ressource ou un service** ».

Pour pallier ces dérives, cet article se propose de revenir sur l'importance d'un mot de passe, ses règles de construction, le contexte de son utilisation mais aussi et de façon plus pragmatique de proposer des solutions simples susceptibles d'en faciliter la construction et la mémorisation.

Le mot de passe… à l'école

Virtue Arts - licenceCC/by

En se connectant à leur messagerie, au réseau d'établissement, les élèves et les adultes de l'établissement sont confrontés aux mêmes difficultés.
En revanche, si la peine est partagée, c'est bien aux adultes d'inculquer « les bonnes pratiques » aux élèves et donc d'appliquer les « bons gestes ». La « sécurisation des données » fait d'ailleurs partie depuis plusieurs années des compétences numériques à faire acquérir (cf. Cadre de Référence des Compétences Numériques)

Cette responsabilité est lourde, difficile et souvent chronophage. Aussi, il n'est pas question de souligner avec arrogance les lacunes constatées dans le domaine mais davantage d'essayer d'apporter quelques pistes, modestes, susceptibles de permettre de concilier une **meilleure sécurisation** et un **meilleur confort d'utilisation**.
D'ailleurs, l'expérience prouve que l'injonction autoritaire pour l'utilisation d'un mot de passe fort peut conduire à l'effet inverse des résultats attendus (un mot de passe trop compliqué à retenir sera soit noté soit oublié !).
Aussi, si l'objectif est de rompre avec des comportements « dangereux », il doit aussi permettre d'appréhender non seulement ce qu'il faut faire, mais comment le faire. Éduquer à la sécurité n'empêche pas d'être réaliste et pragmatique.

Le mot de passe… fort

Définition :

> *"Un mot de passe fort est un mot de passe qui est difficile à retrouver, même à l'aide d'outils automatisés[1]. La force d'un mot de passe dépend de sa* ***longueur*** *et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de* ***minuscules****, de* ***majuscules****, de* ***caractères spéciaux*** *et de* ***chiffres*** *est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules."*
> *Site internet du Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques[2]*

enaissancechambara
licenceCC/by-sa

Les règles (et leur mise en œuvre réaliste) :

- 1. *Ne pas utiliser un seul mot de passe.*

Les services en ligne se multiplient et il semble irréaliste voire contreproductif (car l'utilisateur sera contraint de noter ses différents mots de passe) de suggérer la création et la mémorisation de dizaines de mots de passe différents.
En revanche, il est impératif de hiérarchiser et de distinguer le « niveau de risque » des applications (ou services) et de s'interdire une quelconque perméabilité entre elles. Si le site accessible par votre mot de passe ne sert qu'à réserver des salles, l'enjeu n'est pas le même que s'il s'agit d'un logiciel avec lequel vous pouvez par exemple envoyer des messages, renseigner des évaluations ou faire des achats. Si une base est piratée et votre mot de passe découvert il ne faut pas que l'usurpateur puisse utiliser tous vos comptes sensibles.
Ainsi, je n'utiliserai jamais le même mot de passe pour :

- ma correspondance (courriel, messagerie instantanée, liste de diffusion),

- mes publications (forum, site web, blog, wiki),
- mes transactions financières,
- mon accès réseau,
- mes applications protégées,
- etc.

et distinguerai toujours ce qui relève du contexte personnel et du contexte professionnel.

- 2. *Ne pas noter son mot de passe là où on irait le chercher*

Le mieux est de le retenir, mais si je ne m'en sens pas capable il doit être bien noté dans un endroit improbable, caché dans une liste, et pas en 1ère page de l'agenda.

- 3. *Ne pas autoriser le navigateur à enregistrer le mot de passe*

L'usage nomade des TIC implique d'être particulièrement vigilant lorsque l'on utilise un ordinateur autre que la machine domestique. Que l'on soit en salle des professeurs, au cdi, dans une salle de formation…, il convient de ne jamais autoriser le navigateur à enregistrer le mot de passe qui permet d'accéder à une application ou un service protégé (le navigateur demande par exemple « Voulez-vous que xx se souvienne du mot de passe ? »). Dans le cas contraire, une personne mal intentionnée pourrait -à mon insu- utiliser mon compte !

- 4. *Ne pas utiliser un mot de passe trop simple ou « attendu ».*

Ainsi, les combinaisons en séquence (11111 ; 12345 ; abcde), les suites du clavier (azerty ; wxcvbn ; …), les prénom, nom et date de naissance (en particulier de proches) ainsi que les mots qui se trouvent dans le dictionnaire (écrits à l'endroit ou à l'envers) sont à proscrire.
Le plus fâcheux consistant probablement à utiliser son identifiant comme mot de passe !

- 5. *Ne pas partager son mot de passe*

Sans sombrer dans la paranoïa aiguë, j'évite de taper mon mot de passe lorsque les regards se font trop indiscrets ! Dans le même esprit, je ne partage pas mon mot de passe, même avec un collègue amical, car ce collègue peut être imprudent ou entouré de personnes moins bien intentionnées.

● Le mot de passe… mémorisable

Brenda-Starr - licenceCC/by

Pour que les règles de la page précédente puissent être applicables, il convient de proposer pour la création d'un « **mot de passe fort** » quelques « **astuces** » susceptibles d'en favoriser la mémorisation.

○ La méthode phonétique :

Elle consiste à trouver une affirmation ou une question personnelle, facilement mémorisable, et à la transcrire en langage phonétique.

Exemple[3] : C'est si facile !
Devient : C6Fa6Le!

Exemple[1] : Si j'ai un deux-mâts neuf ?
Devient : 6G12Ma9?

○ La méthode des « premières lettres » :

Elle consiste à retenir une phrase personnelle, facilement mémorisable, et à la transcrire en ne retenant que la première lettre de chacun des mots :

Exemple[1] : L'armée des 12 singes – Terry Gilliam
Devient : L'ad12s-TG

Exemple[1] : Un tiens vaut mieux que deux tu l'auras
Devient : Utvmq2tl'a

La chaine de caractères déjà mémorisée :

Si vous avez déjà retenu une suite de caractères "forte" (par exemple T23=z*), vous pouvez y adjoindre pour chaque site une caractéristique qui le distinguera du mot de passe utilisé ailleurs. Par exemple pour le réseau de l'établissement T23=reseauz*, pour Labomep T23=Labomepz*

> Attention : je m'assure que les mots de passe créés répondent aux exigences attendues (cf. définition du CERTA), à savoir l'usage mêlé de minuscules, majuscules, chiffres et caractères spéciaux et de ponctuation (sauf caractères accentués).

Le mot de passe… Conclusion

Brenda-Starr - licenceCC/by

Allez, aujourd'hui je crée un mot de passe fort !

A,ajc1m2pf!

Annexe : utiliser un outil de stockage crypté

Certains logiciels proposent de stocker l'ensemble de vos mots de passe dans une base de données cryptée. L'accès à cette base de données se fait alors à l'aide d'un mot de passe unique.

Par exemple, *KeePass* logiciel gratuit et *Open source* permet de gérer vos mots de passe de manière sécurisée. La base de données cryptée utilise deux algorithmes connus et reconnus[4]. La protection s'effectue à l'aide d'un seul mot de passe ou par l'insertion d'un disque amovible (une clé USB par exemple).

- Avantage : un seul mot de passe à mémoriser.
- Inconvénient : si le logiciel est installé sur l'ordinateur domestique, on se retrouve coincé lorsque l'on utilise une autre machine car les mots de passe n'ont pas été mémorisés (sauf à conserver sur soi et en permanence son disque amovible... ce que d'aucuns ne trouveront pas très pratique).

(1) Exemples d'outils automatisés :

L'attaque par dictionnaire est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire (source : wikipedia).

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mot de passe cherché est constitué de peu de caractères (source : wikipedia).

(2) CERTA : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques

(3) Ne pas réutiliser ces exemples

(4) *Advanced Encryption Standard* (AES sur Wikipedia) et *Twofish*