## LES TUTORIELS D’ARTCOM

==========

# Les mots de passe

Par Lionel Troyon (AdaptaWeb / AdaptaPrint)

Révision 2 - 29.04.2024

## Des tutoriels ArtCom – Pourquoi ?

ArtCom est une association visant à fédérer les artisans commerçants de Monthey, et protéger leurs intérêts.

Dans ce cadre, il est évident que le partage d'informations, d'astuces et pratiques est une forme d'entraide dont le but est d'améliorer la situation de chacun.

Ainsi, chaque personne membre de l'association qui détient un savoir-faire précis et reconnu, est cordialement invitée à le partager bénévolement par le biais de tutoriels tels que celui-ci. N'hésitez donc pas à contacter le comité ArtCom si vous désirez vous lancer dans une telle démarche.

Merci pour votre implication.

Le comité ArtCom

## A propos de l'auteur

Je me nomme Lionel Troyon, je suis actuellement propriétaire d'AdaptaWeb et AdaptaPrint.

Mes formations :
- Webdesigner diplômé
- Formation complémentaire de webdeveloppeur
- CFC d'employé de commerce
- Diplôme d'aide comptable

## Le thème : « les mots de passe »

J'ai choisi le thème des **mots de passe**, car je vois souvent des failles de sécurité par ce biais, en raison de la méconnaissance du public des risques et des pratiques à éviter, et à fortiori des bonnes pratiques à mettre en œuvre. Avec ce tutoriel, j'espère aider les membres d'ArtCom à minimiser leurs risques.

## Table des matières :


| | | |
|---|---|---|
| **Partie 1 : Les risques** | A. Risque d'usurpation d'identité | Page 3 |
| | B. Risque de perte de données | Page 3 |
| | C. Risque de vol de données personnelles | Page 3 |
| | D. Risque de vol de données de tiers | Page 4 |
| **Partie 2 : Les pratiques à éviter** | A. Utiliser un mot de passe trop simple | Page 4 |
| | B. Utiliser le même mot de passe pour plusieurs accès | Page 4 |
| | C. Ne jamais changer ses mots de passe | Page 5 |
| | D. Partager un mot de passe | Page 5 |
| | E. Tenir une liste de mots de passe | Page 5 |
| | F. Mémoriser les mots de passe dans le navigateur | Page 5 |
| | G. Utiliser le remplissage automatique des formulaires | Page 5 |
| **Partie 3 : Les bonnes pratiques** | A. Utiliser des mots de passe compliqués | Page 6 |
| | B. Utiliser des mots de passe longs | Page 6 |
| | C. Utiliser un mot de passe pour chaque accès | Page 6 |
| | D. Utiliser le login à la manière d'un mot de passe | Page 6 |
| | E. Renouveler ses mots de passe | Page 7 |
| | F. Utiliser l'identification à plusieurs facteurs | Page 7 |
| | G. Utiliser un gestionnaire de mots de passe | Page 7 |
| **Résumé** | | Page 8 |

# Partie 1 : les risques

## A. Risque d'usurpation d'identité

Le premier risque est l'usurpation d'identité.

Cela peut se faire sur plusieurs plateformes :

- Application d'email (Outlook, Gmail etc.)
- Réseaux sociaux (Facebook, LinkedIn, Instagram etc.)
- Divers forums et sites participatifs
- Sites marchands
- Site de votre entreprise

➔ Du moment qu'un hacker découvre votre mot de passe, il peut facilement accéder à votre place aux applications ou sites concernés par le mot de passe en question, et donc se faire passer par vous.

➔ Si par malheur vous utilisez le même mot de passe pour plusieurs sites ou applications, il suffit au hacker d'essayer votre mot de passe sur plusieurs plateformes pour avoir facilement accès à plusieurs espaces en votre nom.

## B. Risque de perte de données

Pire que la simple usurpation d'identité, il y a la perte de donnée.

➔ Une fois logué à votre place, le pirate peut effacer des données, en remplacer d'autres, ou en introduire de nouvelles.

➔ L'effacement, la modification ou l'introduction de données à votre place peut être suffisamment discret pour pas que vous ne le détectiez de suite ; et le risque suivant est qu'il se peut que vous n'arriviez plus à différencier quelles sont les bonnes et quelles sont les mauvaises données.

Si par exemple il se connecte à votre place dans un système de gestion de votre entreprise, il peut tout à fait corrompre ou effacer des données importantes, que ce soient des articles, des commandes, des factures, des données personnelles etc. En fait, toutes les données sur lesquelles vous pouvez vous-même agir sont potentiellement en danger.

## C. Risque de vol de données personnelles

Nous avons tous des données sensibles, personnelles ou tout simplement embarrassantes.

➔ L'accès et la divulgation de données privées peut être embarrassant, compromettant que ce soit dans la sphère privée ou professionnelle.

➔ Le vol de données telles que des numéros de cartes bancaires ou des accès à des sites marchands peut avoir des conséquences financières.

Quasi tout se faisant maintenant sur internet, je vous laisse imaginer tout ce que vous avez renseigné comme données sur les différents sites auxquels vous accédez depuis des années, que ce soit sur un plan personnel ou privé (ça fait peur, n'est-ce-pas ?).

### D. Risque de vol de données de tiers

Jusqu'à présent, je ne vous ai parlé que de risque personnel, mais vous devez prendre conscience que lorsqu'un hacker a accès à votre place à une plateforme sur laquelle vous gérer des données de tiers, celles-ci sont également en danger.

➔ Imaginez qu'un pirate accède à un site de gestion de commandes ; il peut voir les données des clients. Et si par malheur des mots de passe de clients ou de collaborateurs sont stockés en clair sur cette plateforme (c'est illégal, mais cela se fait encore), c'est un véritable jackpot pour notre voleur.

➔ Non seulement vous risquez des dommages personnels (vos données), mais en plus vous pourriez risquer du pénal s'il s'avère que les données sous votre responsabilité ont été piratées en raison d'un manque de sécurité de votre part.

Vous êtes responsables (dans la limite du possible) de la protection des données que des tiers vous confient, il n'y a pas que vos propres données qui sont en jeu.

## Partie 2 : les pratiques à éviter

### A. *Pratique à éviter :* Utiliser un mot de passe trop simple

Utiliser des mots de passe trop simples équivaut à aider les hackers à les trouver.

A bannir **absolument** :

- Les dates de naissance (même celle de la belle-mère)
- Les codes postaux
- Le nom du chat
- Les suites de chiffres genre « 1234 »
- Les suites de lettres genre « abcd »
- Les mots idiots comme « password »

Dans l'idéal, il faudrait bannir tous les mots communs, les noms, les surnoms, les marques. En fait, tout ce dont vous êtes capables de vous souvenir est de fait un mauvais mot de passe !

### B. *Pratique à éviter :* Utiliser le même mot de passe pour plusieurs accès

Vous connaissez la définition du porte-clé ?

***« Dispositif permettant de perdre toutes ses clés d'un seul coup »***

➔ Utiliser le même mot de passe pour plusieurs sites, c'est un peu la même chose ; car la première chose que fait un hacker quand il trouve un mot de passe, c'est l'essayer sur tous les sites et applications possibles et imaginables.

*C'est pour cette raison qu'il est absolument interdit de stocker des mots de passe en clair ou dans un cryptage réversible dans des bases de données. Au début d'internet, il y avait des milliers de forums utilisant des bases de données avec les datas en clair… un véritable paradis pour les hackers. Imaginez les possibilités quasi infinies de nuire à de multiples personnes lorsqu'un pirate obtient tout une liste d'adresses emails et de mot de passe en*

*s'introduisant dans une base de données sans le moindre cryptage des données, à une époque où les gestionnaires de mots de passe n'existaient pas et où quasi tout le monde utilisait le même mot de passe quasi partout.*

Avec l'expérience, nous savons maintenant que la sécurité absolue n'existe pas en informatique, mais plus vous ajoutez de difficultés à trouver votre mot de passe (et votre login), plus vous réduisez les risques.

## C. *Pratique à éviter :* Ne jamais changer ses mots de passe

➔ Plus vous utilisez longtemps le même mot de passe pour un accès, plus vous donnez de temps et donc de chance aux pirates de le trouver.

Il convient donc de modifier régulièrement ses mots de passe.

## D. *Pratique à éviter :* Partager un mot de passe

➔ Utiliser le même mot de passe pour plusieurs personnes (par exemple un login dans une entreprise) est vraiment à éviter.

Si dans une entreprise vous devez avoir accès au même site (par exemple sur un site de fournisseur), je vous recommande de regarder s'il existe la possibilité d'ajouter une personne de contact ou de créer un second compte. Si ce n'est pas possible, il convient de limiter au maximum le nombre de personne connaissant le mot de passe, et surtout ne pas le partager dans une liste ou un message.

## E. *Pratique à éviter :* Tenir une liste de mots de passe

➔ Tenir une liste de mots de passe (genre une liste Excel), c'est vraiment comme laisser toutes vos clés accrochées sur le palier avec comme seule sécurité la porte de l'immeuble.

➔ S'il s'agit d'un login à un site, vous ne devez pas craindre de perdre son mot de passe. De toute façon vous aurez forcément un moyen de régénérer un mot de passe. Il vaut mieux perdre un mot de passe et devoir remplir un formulaire de récupération que de tenir une liste de mots de passe !

Vous arrêtez de tenir des listes tout de suite, sinon je vais me fâcher tout rouge !

## F. *Pratique à éviter :* Mémoriser les mots de passe dans le navigateur

C'est très pratique, mais plutôt risqué. On ne sait pas vraiment où ces données sont stockées, qui y a accès, et de toute façon c'est forcément stocké soit en clair, soit crypté de manière réversible.

Personnellement, et sans être complotiste, je n'ai pas spécialement envie que Google (navigateur Chrome), Microsoft (Edge) ou Apple (Safari) etc., connaissent tous mes mots de passe.

## G. *Pratique à éviter :* Utiliser le remplissage automatique des formulaires

Là aussi, c'est pratique, mais plutôt risqué pour les mêmes raisons qu'au paragraphe précédent.

# Partie 3 : les bonnes pratiques

## A. *Bonne pratique :* Utiliser des mots de passe compliqués

➔ Dans l'absolu, le meilleur mot de passe est celui dont vous êtes incapable de vous souvenir tant il est compliqué.

Au début, les mots de passe étaient un peu comme les anciens PIN des cartes bancaires… une suite de quelques chiffres. Cela s'est compliqué rapidement, justement pour des raisons de sécurité.

Actuellement, un mot de passe « fort » contient une suite de caractères aussi divers que variés, des chiffres, des lettres, des minuscules et des majuscules.

- Chiffres : « 1234567890 »
- Lettres : « abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ »
- Caractères : « §+*ç%&/()= ?!éèöäüà$£€ » (et j'en oublie certainement).

Forcément, avoir « ***Gu*PN2&rsZX)Az48a*9pjy§CH6rçzE(JQuEKa*** » comme mot de passe est un tantinet plus fort que « ***mistigri*** » ou « ***1870*** ».

Cela peut vous sembler totalement absurde car impossible à mémoriser (bien que rien ne vous empêche de renommer le chat « *Gu*PN2&rsZX)Az48a*9pjy§CH6rçzE(JQuEKa* »), mais c'est justement dans cette direction que vous devez aller. Pour cela il y a des outils, appelés gestionnaires de mots de passe, dont je vous parlerai dans un prochain paragraphe.

## B. *Bonne pratique :* Utiliser des mots de passe longs

Je ne pense pas avoir à l'expliquer, vous conviendrez sans le moindre doute qu'un mot de passe de 36 caractères aléatoires est forcément plus sûr qu'un mot de passe de 12 caractères.

## C. *Bonne pratique :* Utiliser un mot de passe différent pour chaque accès

➔ C'est vraiment la base : chaque mot de passe ne devrait être utilisé **que pour un accès** (site, application, carte bancaire, carte SIM, code de porte etc.).

➔ Au pire, si un hacker trouve un de vos mots de passe, il n'aura accès qu'au site (ou appli) correspondant à celui-ci.

Avoir un mot de passe par accès limite considérablement les risques.

## D. *Bonne pratique :* Utiliser le login à la manière d'un mot de passe

Comme chacun le sait, le mot de passe accompagne quasi toujours un login. C'est exactement comme avoir une double serrure sur une porte.

➔ La plupart du temps, **le login est en fait votre adresse email ; ce qui est facile à trouver**. Ainsi, la double serrure n'en est en fait qu'une seule, si on part du principe que votre adresse email est connue.

Ma recommandation est donc la suivante :

- Utilisez une adresse email « **privée** » pour tous vos logins privés.
- Utilisez une adresse email « **pro** » pour tous vos logins professionnels.
- Utilisez un login « **très compliqué** » et unique pour les accès particulièrement sensibles.

Par exemple, en tant qu'entreprise ayant plusieurs clients dans une base de données, j'utilise comme login ce qui est en fait un second mot de passe, et non une adresse email.

Exemple : *Login : JA623na*6An&am(J9%36)&a3G9*
*Password : 3Kn&2C9=s&w*ms23&J81D)*d78*

Ainsi, les hackers n'ont pas un seul mot de passe à trouver, mais deux ! C'est quasi impossible à cracker.

## E. *Bonne pratique :* Renouveler ses mots de passe

➔ Changez vos mots de passe de temps en temps. Une fois par année n'est pas très contraignant, et c'est déjà pas mal du tout. Deux fois par an, c'est encore mieux.

Au-delà serait fantastique, mais cela tient plus de la paranoïa que de la sécurité… pour autant que vous utilisiez des mots de passe compliqués comme décrits précédemment, car si vous utilisez le prénom de belle-maman, votre code postal ou le nom du chat, changer le mot de passe chaque semaine serait encore insuffisant !

## F. *Bonne pratique :* Utiliser l'indentification à plusieurs facteurs

Vous utilisez probablement déjà la reconnaissance à plusieurs facteurs pour votre e-banking, via votre Smartphone.

C'est quelque chose de très sécuritaire ; car cela commence à faire beaucoup pour un hacker : il doit déjà connaitre votre login, cracker votre mot de passe, et il devrait en plus de tout cela vous voler votre Smartphone (et avoir votre empreinte pour le déverrouiller). Je veux bien admettre que certains pirates soient spécialement doués, mais il y a des limites.

Je ne peux donc que vous encourager d'activer l'indentification à multiples facteurs lorsque cela vous est proposé.

## G. *Bonne pratique :* Utiliser un gestionnaire de mot de passe

J'ai pleinement conscience qu'en arrivant à ce point, vous vous dites que je suis complètement fou car personne n'est humainement capable de suivre mes recommandations (des mots de passe impossibles à retenir, uniques et différents pour chacun des sites et applis, et ce, sans tenir de liste).

Heureusement, **les gestionnaires de mots de passe sont là pour vous aider** !

Il y en a clairement deux dans lesquels vous pouvez avoir une confiance « absolue » ; il s'agit de **Kaspersky Password Manager**, et de **1Password**, tous deux chaudement recommandés (pas juste par moi, mais par de véritables spécialistes en sécurité de données), mais il en existe probablement d'autres tout aussi sûrs.

Pour ma propre entreprise, j'utilise depuis 2 ans **1Password** (et par le passé **Kaspersky**), qui gère un coffre-fort (de mots de passe) pour chacun de mes collaborateurs (on est 3). Ainsi, je ne connais pas leurs mots de passe, et eux ne connaissent évidemment pas les miens. Cela fonctionne très bien.

Je n'ai que 2 mots de passe dont je dois me souvenir : celui de mon PC (qui lui aussi ne doit pas être le nom du chat), et le mot de passe du gestionnaire de mot de passe (idem !).

A noter qu'un gestionnaire de mots de passe doit forcément être installés sur le PC (ou Smartphone) qu'il protège ; un hacker ne peut pas y avoir accès depuis son PC (et ne peut pas savoir que vous en utilisez un, ni duquel il s'agit).

Le gestionnaire de mot de passe vous met en garde lorsqu'un mot de passe n'est pas assez fort, il vous suggère des mots de passe sûrs pour les nouvelles entrées (lorsque vous créez un nouveau compte sur un site), il peut également gérer vos données de cartes de crédit, et sécurise le remplissage des champs de formulaire.

C'est quelque chose de sûr, simple à utiliser, vraiment efficace, et très recommandé par les spécialistes de la sécurité.

# Résumé :

## Pour minimiser les risques :

- ➔ J'arrête d'utiliser le nom du chat, la date de naissance de ma belle-mère, mon code postal, ou encore un nom commun comme mot de passe.
- ➔ Je n'utilise plus le même mot de passe pour tous mes accès.
- ➔ Je ne partage pas mes mots de passe.
- ➔ Je ne tiens pas de liste de mots de passe même si je ne sais pas comment les retenir.
- ➔ Je ne mémorise plus les mots de passe dans le navigateur.
- ➔ Je n'utilise plus le remplissage automatique de formulaires.

## Pour faire la nique aux hackers :

- ➔ J'utilise des mots de passe très compliqués de la mort qui tue, composés de caractères aléatoires et mélangés, que je suis totalement incapable de retenir, parce que je le vaux bien.
- ➔ J'utilise des mots de passe de minimum 20 caractères (36 pour faire plaisir à Lionel).
- ➔ J'ai un mot de passe différent pour chaque accès pour éviter de perdre toutes mes données d'un seul coup, pour minimiser mes risques si un pirate cracke un de mes mots de passe.
- ➔ Pour les données de tiers ou très à risque, j'utilise le login comme un mot de passe, car je suis pénalement responsable de la protection des données qui me sont confiées par mes contacts.
- ➔ Je renouvelle mes mots de passe une fois par année.
- ➔ Lorsqu'on me le propose, j'utilise l'identification à plusieurs facteurs, même si j'en ai marre de devoir entrer un code reçu par SMS à chaque fois que je commande des croquettes pour le chat.
- ➔ Comme je suis incapable de me rappeler les 98392 mots de passe qui ne veulent rien dire car j'ai écouté ce *&%ç&* de Lionel à qui j'avais rien demandé, j'utilise un gestionnaire de mots de passe.