La combinaison de plusieurs mots permet de générer un « mot de passe » plus long, donc **plus sécuritaire**, tout en étant **facile à mémoriser**. Selon l'Office québécois de la langue française, on parle alors de phrase de passe au lieu de mot de passe.

L'important, c'est d'utiliser une « phrase » dont vous vous **souviendrez** facilement.

Avec ou sans espaces

La plupart des systèmes supportent des « mots de passe » comportant des espaces, cependant, certains systèmes pourraient ne pas les accepter. Si les espaces sont utiles afin de distinguer les mots dans un texte, ils ne sont pas nécessaires pour que nous puissions les distinguer dans une phrase. L'utilisation de majuscules peut nous aider à distinguer les mots d'une phrase de passe.

Voici un exemple : « PourtantFacile » est une « phrase » composée de deux mots qui comporte 14 caractères, ce qui est difficile à déchiffrer pour un ordinateur dans un temps « raisonnable », alors qu'un mot de passe de 5 caractères tel @$%## qui est difficile à mémoriser par une personne, peut-être décodé en quelques secondes, sinon quelques minutes par un logiciel de décryptage sur un ordinateur possédant un processeur « récent ».

« Pourtant » et « Facile » sont deux mots faciles à décoder non ? Oui, mais l'encodage des deux mots pris séparément ne permet pas de « trouver » la combinaison des deux mots par les logiciels de décryptage.

Éviter l'utilisation de phrases populaires

Vous devriez cependant éviter les phrases populaires, citations ou extraits de texte connus : par exemple « Je Me Souviens » « Je Pense Donc Je Suis » etc., car tout comme les mots communs, des dictionnaires de phrases populaires sont ou seront disponibles pour faciliter le décodage de celles-ci par les fraudeurs.

Utilisation de préfixe ou suffixe dans vos mots de passe

Pour des raisons de sécurité, vous devriez utiliser des mots de passe différents pour les services auxquels vous accédez (Banque, PayPal, Gmail, Facebook, Dropbox etc.).

Vous pouvez utiliser des mots de passe complètement différents ou utiliser une méthode telle que celle-ci :

En utilisant l'exemple précédent, on pourrait utiliser un préfixe à notre phrase :

PayPourtantFacile pour votre compte PayPal

GMPourtantFacile pour votre compte Gmail

Ou un suffixe :

PourtantFacileAC pour votre compte UQAC

PourtantFacileT1 pour un compte sensible

Etc.

Si on prend les exemples précédents, on peut conclure que GMPourtantFacile et PourtantFacileT1 n'ont que 4 caractères différents. Pour une personne, c'est vrai, mais pour un logiciel, c'est une tout autre histoire, ils sont **totalement différents.** Si vous désirez en savoir plus, consulter le document : ***Encodage des phrases de passe***.

Pourquoi utiliser des mots de passe différents

Si vous possédiez un compte Yahoo avant le mois d'août 2013, votre mot de passe a été récupéré par des fraudeurs. Vous n'étiez pas seul, car 3 milliards de comptes ont été compromis dans cette entreprise. Ou peut-être un compte Equifax, Bell, Sony; ce ne sont que quelques exemples d'entreprises qui ont été victime de fuite d'informations des utilisateurs.

Oui, mais votre compte (adresse Yahoo) était Compte323@yahoo.com et votre compte (adresse) UQAC est Mon.Compte@uqac.ca, aucun lien direct entre les deux.

En fait, des informations personnelles sont peut-être rattachées à vos différents comptes sur différents médias. Vous avez peut-être donné votre adresse UQAC pour faire valider votre compte Yahoo.

Il existe plusieurs outils très puissants permettant de relier des informations entre elles en provenance d'une multitude de sources. Plusieurs renseignements personnels sont accessibles, entre autres, sur les réseaux sociaux qui pourraient éventuellement permettre de faire un lien entre vos deux adresses. Ou vous avez utilisé un accès sans fil dans un endroit public cible d'un fraudeur, les possibilités sont multiples n'en doutez pas.