BeaucouzéNet - Sécurité

Table des matières

LA SÉCURITÉ DES MOTS DE PASSE

Il n'y a pas de règle unique de gestion des mots de passe, que ce soit sur les sites ou chez l'utilisateur. Pour autant des bonnes pratiques sont parfois proposées ; l'agence nationale de sécurité préconise :*« Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux). ».*

Il semblerait que ce soit une bonne manière de définir un mot de passe. Mais quand plus loin ils disent : *« Utilisez un mot de passe unique pour chaque service...Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis ...Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis...Utilisez un mot de passe unique pour chaque service... »* ça nous semble excessif. Nous ne sommes pas la banque de France, et pour beaucoup d'utilisations que nous faisons, l'usurpation de notre identité n'est pas un drame en soi...

Après discussion, on pourrait préconiser les choses suivantes :

- Il existe des sites sensibles qui ont trait avec notre identité : site de gouvernement (impôts), messagerie, réseaux sociaux (facebook, twitter...). Il est important de d'y associer des mots de passe suffisamment sûrs et personnels, difficilement retrouvables
- Les sites marchands (Fnac, But, Darty, Boulanger, Amazon, LaRedoute, VentePrivée...) peuvent avoir le même utilisateur – mot de passe. Si on se les faisait voler, ce ne serait pas si grave ...
- Ne jamais noter ses mots de passe sur papier. Si on perd ou pire si on vous vole votre carnet ...
- Essayer d'avoir des mots de passe que vous pouvez retenir facilement – voir méthode plus loin
- Et surtout ne jamais écrire, ne jamais donner des mots de passe (ou codes) liés à vos activité bancaires...

OÙ SONT STOCKÉS LES MOTS DE PASSE

Les mots de passe servent essentiellement/exclusivement pour accéder à un site internet. Donc un des endroits où peuvent être enregistrés les mots de passe sont les navigateurs web. On a vu que pour les deux principaux navigateurs, on peut autoriser ou non l'enregistrement des mots de passe saisis, accepter/refuser qu'un nouveau mot de passe soit retenu et voir les mots de passe enregistrés. On lira la documentation pour Firefox et celle pour Chrome.

Mais on peut aussi sécuriser son propre ordinateur avec un mot de passe à l'ouverture d'une session. Je n'ai aucune assurance sur le sujet, il faut lire la documentation constructeur.

Gestionnaire de mot de passe.

Il y a beaucoup de littérature sur le sujet. Un article complet a été écrit par le site Le Monde. Pour les curieux, mes commentaires :

- Les logiciels qui stockent les mots de passe cryptés sur votre ordinateur. Exemple Keepass. Avantages : c'est en local. Inconvénient : si ne sécurise pas (cloud, duplication ailleurs...), quand on perd son ordinateur (ou qu'il est cassé) on perd tous ses mots de passe
- Les sites qui enregistrent vos mots de passe. Exemple Lastpass (celui que j'utilise). Avantages : accessible de n'importe où, même sur des ordinateurs/smartphone qui ne sont pas à vous. Inconvénient : c'est sur le Web . Donc si on vous pique votre mot de passe principal, on vous pique tout.
- Ceux en site web peuvent être communautaires – genre la famille, tout le monde à ses propres mots de passe mais on peut les partager0. Mais les options sont souvent payantes.
- Et ceux en site web peuvent être utilisés sur différents sources : ordinateur, smartphone … même si on n'en est pas proprétaire
- Et les outils de gestion de mots de passe sont souvent interfacés avec le navigateur. Donc les mots de passe sont remplis automatiquement.

Une méthode (parmi d'autres) pour choisir un mot de passe

Un mot de passe important (mail, banque, réseau social) doit être sécurisé mais son propriétaire doit le retenir facilement. On a évoqué plusieurs astuces :

- Changer certaines lettres d'un mot facile à retenir par d'autres lettres. Exemple
  - la lettre O devient le chiffre 0, le « i » devient « ! » (i inversé), le « a » se transforme en « @ », le « S » peut se transformer en chiffre 5, le « m » et le « n » passent la tête en bas en se transforman en « w » ou « u », voir l'inverse, etc etc
- se souvenir d'une phrase (poème, chanson) et ne mettre que les premières lettres de chaque mot. Exemple : « Maître corbeau sur un arbre perché Tenait en son bec un fromage » donne comme mot de passe Mcs1apTesb1f.
- Ou se souvenir d'une chanson de jeunesse, exemple Alexandrie de Claude François. « Ah Aaah Ah Aaah Voiles sur les filles Barques sur le Nil » donne 4AVslfBslN
- Ou d'une adresse. Pour la médiathèque de Beaucouzé se serait 2 rue du grand pin qui donne : 2RueDuGrandP1

POUR ESSAYER DE RÉSUMER

Ne jamais noter ses mots de passe sur un carnet ou un papier… sauf à bien le planquer chez soi …

Mettre un/des mots de passe bien sécurisés pour ces accès financiers et ses accès liés à l'identité numérique (mail, réseau sociaux).

Pour les sites marchands, on peut mettre le même mot de passe partout ; si on se le fait pirater, y'a pas mort d'homme…

Si on enregistre des mots de passe dans le navigateur internet, avoir bien conscience de ce qu'on fait.

Ne jamais noter nulle part les accès à votre banque, même pas dans un carnet.

Appliquer une méthode pour générer un mot de passe compliqué mais que vous retiendrez facilement.

LES SPAMS

Définition du Larousse : « *Courrier électronique non sollicité envoyé en grand nombre à des boîtes aux lettres électroniques ou à des forums, dans un but publicitaire ou commercial* ». Donc c'est un mail non désiré qu'on reçoit de quelqu'un qu'on ne connaît pas.

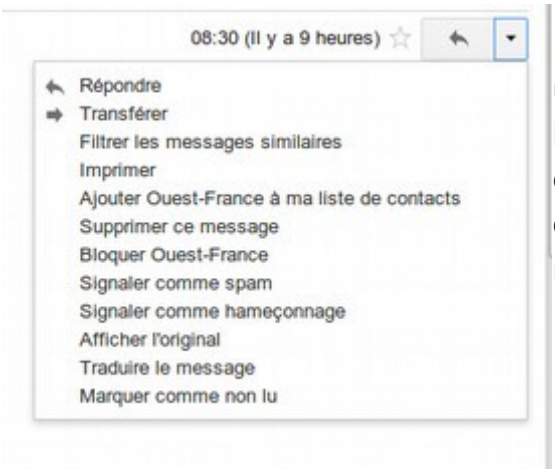
Mais malheureusement, on ne peut pas empêcher ces personnes de nous importuner ; il faut vivre avec.

COMMENT VIVRE AVEC

Sur les messageries il existe très souvent un anti-spam. C'est à dire qu'un courrier suspecté indésirable est mis de côté ; il est mis de côté soit parce qu'il est réputé comme indésirable par le fournisseur d'accès, soit que vous l'ayez déclaré vous-même indésirable.

Cas de Gmail.

Dans l'interface standard on peut voir plusieurs choses.



En haut à droite on peut déclarer un mail comme spam, hameçonnage (phishing) ou carrément le bloquer. Et à gauche on retrouve les spams dans un répertoire.

Pour les autres accès mail, il faudra compléter