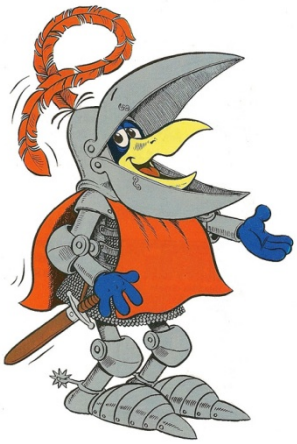
Comment protéger l'accès à vos services informatiques



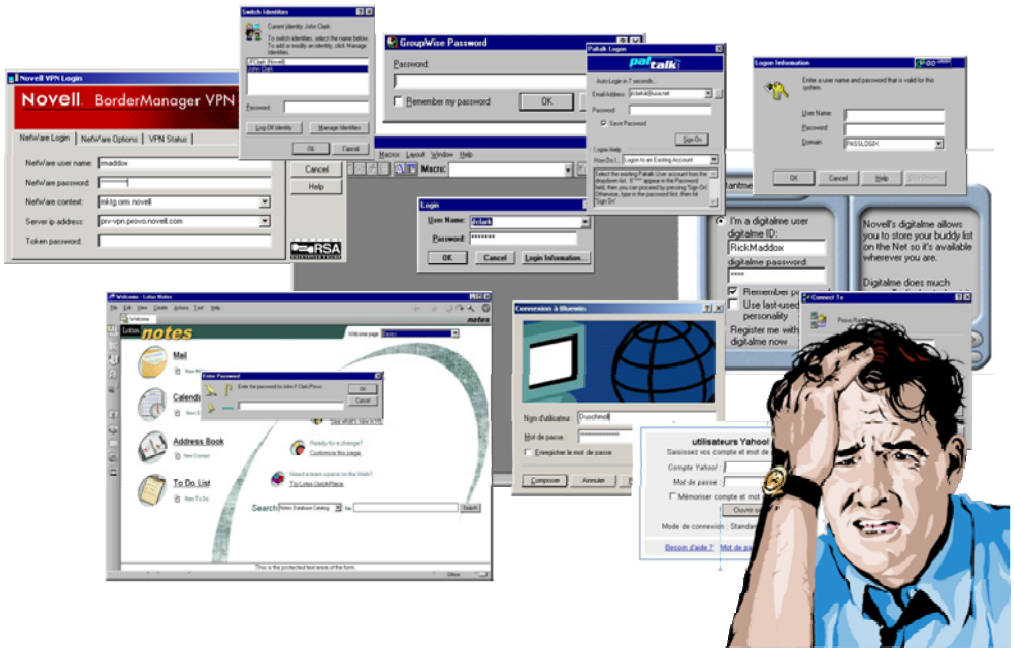
Suite à la mésaventure de plusieurs personnes de mon entourage qui se sont fait pirater leur messagerie, elles m'ont demandé comment bien sécuriser l'accès à leur messagerie. La plupart des services de messagerie étant gratuits, le niveau de sécurité d'accès est beaucoup plus faible qu'un service e-banking. La responsabilité incombe à l'utilisatrice ou à l'utilisateur qui doit s'assurer de la robustesse de son mot de passe.

Alors la question est : qu'est-ce qu'un mot de passe robuste ?

Si sur internet vous effectuez la recherche « *casser un mot de passe* », vous aurez environ 524'000 résultats proposant des méthodes ou des téléchargements de logiciels permettant de casser un mot de passe !!

La plupart des hackers ont des logiciels qui utilisent des dictionnaires pour d'abord détecter tous les mots existants dans notre langue ainsi que dans toutes autres langues étrangères, ce que les performances des PCs actuels permettent de faire en très peu temps. Ensuite, ces hackers vont essayer de trouver sur le Net des informations personnelles : noms et prénoms de vos proches, nom du chien ou du chat, marque ou n° de plaque de la voiture, vos activités favorites, vos clubs, etc. Puis ils pourront agir en envoyant à tout votre répertoire d'adresses un message de détresse demandant en votre nom une aide financière suite à une agression grave lors de votre pseudo voyage à l'étranger où vous auriez tout perdu

Il faut donc créer un mot de passe complexe non significatif (exemple : Mv1B9V7jk). Mais comment le créer et surtout s'en souvenir sans l'inscrire sur un post-it collé sur l'écran ou sous le clavier de votre ordinateur ?



Avant de vous dire comment le faire, voici une petite explication : la robustesse d'un mot de passe dépend du nombre de caractères et de chiffres indépendants uniformément distribués. Plus le mot de passe en contient, plus cela prendra du temps pour le casser et lorsque cela prend trop de temps, le hacker abandonne généralement au vu de l'effort et des moyens à mettre en œuvre.

Si le mot de passe contient N caractères indépendants et uniformément distribués, le nombre maximum d'essais nécessaires se monte alors à :

- 10^N si le mot de passe ne contient que des chiffres. Exemple : il faudra 10 puissance 4 essais pour casser un PIN code de 4 chiffres. 10^4 essais = 10'000 essais, ce qu'un ordinateur peut faire en quelques secondes !!
- 26^N si le mot de passe ne contient que des lettres de l'alphabet totalement en minuscules ou en majuscules ;
- 52^N si le mot de passe ne contient que des lettres de l'alphabet, avec un mélange de minuscules et de majuscules ;
- 62^N si le mot de passe mélange des majuscules et des minuscules ainsi que des chiffres. Dans ce cas, il faudra 40'105'584'896 essais pour trouver un mot de passe composé de 8 caractères, ce qui est mieux qu'un PIN code de 4 chiffres.

Alors, comment créer un mot de passe de N caractères indépendants uniformément distribués et facile à retenir ? Une technique simple est l'utilisation de chevilles phonétiques - suite de lettres et de chiffres qui phonétiquement forment un mot. Exemple de mots de passe de 7 à 8 caractères comme souvent requis pour l'accès différent services informatiques:

- Ght19kC – J'ai acheté un œuf cassé,
- lnrstNRV – Hélène est restée énervée,
- RVetoqp – Hervé est occupé

Attention : Les mots de passe circulent en clair sur les réseaux, sauf si l'adresse de la connexion commence par **https://**. Des techniques simples (sniffers, espions, chevaux de Troie, etc.), peuvent être mises en œuvre pour capter le couple (identifiant et mot de passe) à l'insu des utilisateurs. Ces dispositifs peuvent rester en place pendant des mois avant d'être découverts. Pendant ce temps, tapis à l'écoute du réseau, les hackers captent tous les mots de passe qui circulent. C'est pourquoi, même robuste, un mot de passe doit être modifié régulièrement.

Cordialement – Claude Maury