Les mots de passe

Introduction

Source: FlickR

Outil clé d'identification sur les différents services en ligne, le mot de passe est souvent la seule barrière de protection contre les intrusions indésirables aux conséquences potentiellement désastreuses.

Cependant, il s'agit souvent d'un outil mal géré, car de nombreux utilisateurs n'hésitent pas, par exemple, à utiliser des mots de passe très simples. Ils sont donc plus faciles à deviner et à pirater. Il est important d'être conscient des enjeux des mots de passe et de savoir comment les sécuriser facilement tout en les gardant en mémoire.

Identification de l'utilisateur

L'utilisation de l'ordinateur implique souvent l'identification des internautes. La technique la plus courante est basée sur le couple "login/mot de passe". Selon la situation, l'identifiant peut être public ou privé, mais il est souvent mal protégé. Le mot de passe est l'outil qui assure la sécurité essentielle.

Source: FlickR

Erasmus+

Risque majeur : vol d'identité

Définition de Wikipedia:
Le vol d'identité est l'utilisation délibérée de l'identité d'une autre personne, habituellement comme moyen d'obtenir un avantage financier ou un crédit ou d'autres avantages au nom de l'autre personne, et peut-être au détriment ou à la perte de l'autre personne.

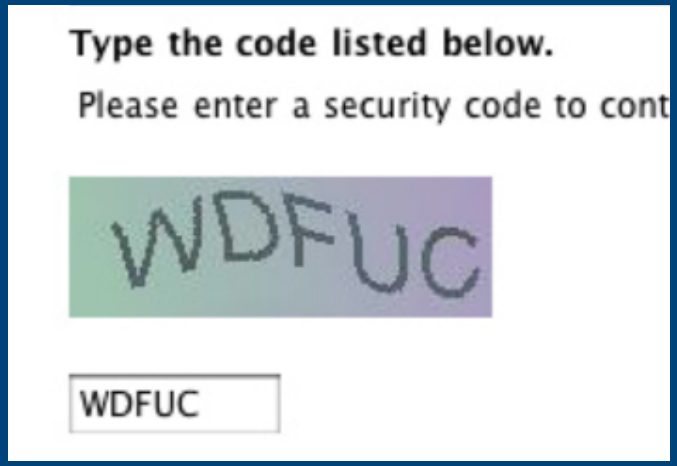
Problème:
Il est difficile de déterminer le lien entre les atteintes à la protection des données et le vol d'identité, surtout parce que les victimes de vol d'identité ne savent souvent pas comment leurs renseignements personnels ont été obtenus et que le vol d'identité n'est pas toujours détectable par les victimes individuelles.

Donc...

Les opérateurs qui demandent une identification doivent mettre en place de nombreuses mesures de sécurité pour gérer les mots de passe. C'est une question très importante, mais sur laquelle nous avons peu de contrôle.

➔ Utiliser un mot de passe qui ne peur pas être facilement deviné par un hacker

- *Evitez les mots de passe de base tels que 12345, azerty, date de naissance, même mot de passe que login, etc.*
- *Le mot de passe doit être long (au moins 14 lettres/chiffres)*
- *Il doit être diversifié (lettres majuscules, minuscules, chiffres, caractères spéciaux, etc.)*
- *Un opérateur sérieux mettra en œuvre certaines mesures de sécurité telles qu'un nombre limité de tentatives ou un captcha.*



Source: FlickR

Erasmus+

Mais...

La plupart des gens ont plusieurs comptes et il est fondamental de diversifier vos mots de passe. Par conséquent, il est compliqué de les mémoriser tous. Conserver des mots de passe sur un post-it est également risqué.

Alors, comment s'attaquer à ce problème ?

Pour limiter ce problème de mémorisation, trois méthodes complémentaires sont disponibles :

- Utilisez des "mots de passe - phrase" faciles à mémoriser mais difficiles à deviner.
- Utiliser des méthodes d'identification mixtes
- Utiliser un gestionnaire de mots de passe

Erasmus+

« Mots de passe - phrase »

Plutôt que de devoir mémoriser des mots de passe complexes comme "Mç9@X###Kl", nous vous conseillons d'adopter des "mots de passe phrase", plus faciles à mémoriser mais plus complexes à pirater.

Il s'agit de conserver plusieurs termes inspirés d'éléments connus uniquement par l'utilisateur. Au lieu de la date et du lieu de naissance, on pourrait mettre un "Né à onze heures 27 un jeudi". Cette phrase peut être liée ou non au service utilisé (d'une manière non évidente) afin qu'on puisse s'en souvenir.

Ceci permet de concilier les avantages d'un mot de passe complexe tout en le mémorisant plus facilement !

Erasmus+

Méthodes d'identification mixtes

Les opérateurs fournissent des méthodes d'identification mixtes où un élément supplémentaire au mot de passe sera demandé à l'utilisateur. Pour les grandes opérations, l'identification se fait souvent avec une vérification supplémentaire. Il s'agit le plus souvent d'indiquer un code éphémère transmis par SMS.

Le mauvais point de cette amélioration de la protection des comptes est la transmission de données supplémentaires (numéro de téléphone dans l'exemple donné, validation par e-mail, validation d'une carte à puce ; les données biométriques peuvent également être utilisées dans des cas similaires).

Faites attention !
donner votre numéro de téléphone à votre banque peut être justifié mais donner vos données biométriques pour un achat sur Internet ne l'est pas !

Erasmus+

Source: FlickR

Gestionnaires de mots de passe

Peu importe la façon dont vous créez vos mots de passe, se souvenir d'eux est toujours le plus grand défi ! Une bonne solution peut être d'utiliser un gestionnaire de mots de passe.

Presque tous les navigateurs offrent la possibilité de mémoriser vos mots de passe. Cette possibilité, même si elle simplifie la vie, peut être dangereuse. Certains navigateurs, comme Firefox, conservent les mots de passe par défaut et en texte clair !
Si vous voulez vraiment utiliser cette option, le mieux est de créer un mot de passe maître. Il protégera alors l'accès aux mots de passe enregistrés.

Erasmus+

Gestionnaires de mots de passe (2)

La meilleure solution est d'utiliser un gestionnaire de mots de passe externe. Ce logiciel doit être installé sur votre ordinateur. Il gérera la mémorisation de vos mots de passe pour vous. Les logiciels les plus sérieux chiffrent les mots de passe qui ne deviennent accessibles qu'en donnant le mot de passe maître qui est donc le seul dont l'utilisateur doit se souvenir.

Exemples de logiciels: Lastpass, Onepassword, Dashlane...

Important à noter, ils sont gratuits !

MERCI!

Avez-vous des questions?