

Zone-Alarm : Les Mots de Passe, maillon faible sur Internet **Internet**

Posté par : JulieM

Publié le : 22/12/2010 14:30:00

Selon un sondage **Zone Alarm**, 50% des internautes interrogés se sont fait pirater leur messagerie ou leur profil sur un réseau social. Pourtant, les consommateurs persistent à utiliser le même mot de passe pour tous leurs comptes en ligne essentiels.

Check Point® Software Technologies Ltd, leader mondial de la sécurité sur Internet, annonce aujourd'hui les résultats d'un sondage ZoneAlarm1. Celui-ci révèle que 79 % des consommateurs utilisent des mots de passe à risque, qu'ils construisent à partir d'informations personnelles et de mots courants.

Le sondage montre également que **26 %** des personnes interrogées utilisent le même mot de passe pour plusieurs comptes clés, comme leur messagerie, leur compte bancaire, les portails d'achat en ligne et les réseaux sociaux. De plus, près de **8 %** des personnes interrogées avouent avoir copié leur mot de passe sur des listes trouvées sur Internet, supposées recenser les mots de passe les plus « fiables ». On ne s'étonnera donc pas d'apprendre que **29 %** des personnes interrogées ont été victimes de piratages visant leur messagerie ou leur profil sur un réseau social, et que plus de la moitié de ces personnes (**52 %**) connaissent quelqu'un ayant vécu une expérience similaire.



Quand il s'agit d'accéder à un compte sécurisé ou de s'infiltrer dans un ordinateur, la première chose que fait un pirate informatique est d'essayer de deviner le mot de passe de sa victime. Pour ce faire, il dispose de programmes automatisés qui « devinent » les mots de passe en essayant systématiquement tous les éléments d'information ou mots courants répétés dans une base de données.

Autre enseignement du sondage ZoneAlarm :

22 % des personnes interrogées se sont déjà fait pirater leur messagerie électronique et près de 46 % d'entre elles connaissent quelqu'un ayant vécu pareille mésaventure. De plus, 22 % des personnes interrogées déclarent avoir déjà été victimes d'un piratage de leur profil sur un réseau social, et 32 % connaissent quelqu'un ayant subi un désagrément similaire. Une fois qu'un pirate obtient l'accès à un compte, il parvient dans près de 30 % des cas à utiliser l'information obtenue pour accéder à d'autres sites contenant des données financières, comme le numéro d'un compte bancaire ou d'une carte de crédit.

« En cette période de fêtes, le nombre d'achats effectués en ligne est plus élevé que jamais, et les consommateurs doivent prendre conscience de l'importance des mots de passe et du fait que les pirates disposent de moyens de plus en plus sophistiqués pour les craquer », déclare **Bari Abdul**, vice-président en charge du service Ventes grand public chez Check Point. « En créant un mot de passe unique pour chaque compte clé, les consommateurs battissent une première ligne de défense contre les cybercriminels qui n'ont qu'une idée en tête : faire

main basse sur les données critiques de leurs victimes dans un but lucratif. »



ZONEALARM®
by Check Point®

Pour permettre de réaliser des achats sur Internet en toute sécurité et profiter sereinement des fêtes de fin d'année, voici quelques conseils pour choisir un mot de passe hautement sécurisé :

Choisir un mot de passe contenant au moins 8 à 10 caractères.

Cette longueur devrait suffire à prévenir les attaques par force brute. Une telle attaque consiste à essayer tous les codes, combinaisons et mots de passe imaginables jusqu'à identifier l'élément qui sert de sésame.

À veiller à choisir un mot de passe difficile à deviner.

Évitez d'utiliser un nom, particulièrement votre identifiant, le nom d'un membre de votre famille ou le nom d'un animal domestique. Gardez-vous également d'utiliser des données personnelles, par exemple un numéro de téléphone, une date d'anniversaire ou le nom de la ville où vous êtes né.

Ne pas utiliser les termes que l'on peut trouver dans le dictionnaire.

Les dictionnaires en ligne permettent à n'importe quel pirate d'exécuter un programme capable de tester tous les mots du dictionnaire jusqu'à tomber sur le bon.

Éviter d'utiliser plusieurs fois le même caractère ou des séquences faciles à deviner.

Exemple : 77777, 12345 ou abcde.

Choisir un mot de passe qui associe des chiffres, des lettres et des caractères spéciaux.

Plus votre mot de passe sera complexe et aléatoire, et plus il sera difficile à un cybercriminel de le « craquer ».

Utiliser des fragments de mots, qui ne pourront pas être trouvés dans un dictionnaire.

â **SÃ©parer un mot en insÃ©rant un caractÃ¨re spÃ©cial en son milieu.**

â **Utiliser des mots de passe diffÃ©rents et uniques pour tous les sites les plus importants.**

â **Changer souvent vos mots de passe.**

En admettant que quelqu'un parvienne Ã accÃ©der au fichier systÃªme contenant les mots de passe, le mot de passe obtenu ne pourra pas lui servir bien longtemps.

â **Utiliser une solution**

ZoneAlarm vous propose un produit partenaire, [Password Manager](#) De plus, ZoneAlarm vous offre une vaste gamme de sÃ©curitÃ©, essentielles pour

protÃ©ger le consommateur des menaces sophistiquÃ©es du Web.

[Pour en savoir plus.](#)

Â« Quand vous crÃ©ez un mot de passe, vous devez tenir compte de l'importance du compte que vous souhaitez protÃ©ger, et des consÃ©quences qui s'ensuivraient si jamais ce compte Ã©tait piratÃ©. Autre point important : lorsque vous vous inscrivez sur un site grand public pour tÃ©lÃ©charger gratuitement un jeu vidÃ©o, ne choisissez pas le mot de passe vous permettant de consulter votre compte bancaire Â», conclut **M. Abdul.**