

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

Post   par : JulieM

Publi  e le : 22/12/2010 14:30:00

Selon un sondage **Zone Alarm**, 50% des internautes interrog  s se sont fait pirater leur messagerie ou leur profil sur un r  seau social. Pourtant, les consommateurs persistent    utiliser le m  me mot de passe pour tous leurs comptes en ligne essentiels.

Check Point   Software Technologies Ltd, leader mondial de la s  curit   sur Internet, annonce aujourd'hui les r  sultats d'un sondage ZoneAlarm1. Celui-ci r  v  le que 79 % des consommateurs utilisent des mots de passe    risque, qu'ils construisent    partir d'informations personnelles et de mots courants.

Le sondage montre   galement que **26 %** des personnes interrog  es utilisent le m  me mot de passe pour plusieurs comptes cl  s, comme leur messagerie, leur compte bancaire, les portails d'achat en ligne et les r  seaux sociaux. De plus, pr  s de **8 %** des personnes interrog  es avouent avoir copi   leur mot de passe sur des listes trouv  es sur Internet, suppos  es recenser les mots de passe les plus   « fiables   ». On ne s'  tonnera donc pas d'apprendre que **29 %** des personnes interrog  es ont   t   victimes de piratages visant leur messagerie ou leur profil sur un r  seau social, et que plus de la moiti   de ces personnes (**52 %**) connaissent quelqu'un ayant v  cu une exp  rience similaire.



Qu  il s  agisse d  acc  der    un compte s  curis   ou de s'infiltrer dans un ordinateur, la premi  re 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 automatis  s qui   « devinent    les mots de passe en essayant syst  matiquement tous les   l  ments d'information ou mots courants r  p  rt  s dans une base de donn  es.

Autre enseignement du sondage ZoneAlarm :

22 % des personnes interrog  es se sont d  j   fait pirater leur messagerie   lectronique et pr  s de 46 % d  entre elles connaissent quelqu'un ayant v  cu pareille m  saventure. De plus, 22 % des personnes interrog  es d  clarent avoir d  j     t   victimes d'un piratage de leur profil sur un r  seau social, et 32 % connaissent quelqu'un ayant subi un d  sagr  ment similaire. Une fois qu'un pirate obtient l'acc  s    un compte, il parvient dans pr  s de 30 % des cas    r  utiliser l'information obtenue pour acc  der    d'autres sites contenant des donn  es financi  res, comme le num  ro d'un compte bancaire ou d'une carte de cr  dit.

  « En cette p  riode de f  tes, le nombre d'achats effectu  s en ligne est plus   lev   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 sophistiqu  s pour les   craquer     », d  clare **Bari Abdul**, vice-pr  sident en charge du service Ventes grand public chez Check Point.   « En cr  ant un mot de passe unique pour chaque compte cl  , les consommateurs b  tissent une premi  re ligne de d  fense contre les cybercriminels qui n'ont qu'une id  e en t  te : 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.

■ 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'écriter 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 systÃ¨me 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.**