Zone-Alarm : Les Mots de Passe, maillon faible sur Internet
Internet
PostÃ© par : JulieM
PubliÃ©e le : 22/12/2010 14:30:00

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

Check PointÂ® Software Technologies Ltd, leader mondial de la sÃ©curitÃ© sur Internet, annonce aujourd'hui les rÃ©sultats d'un sondage ZoneAlarm1. Celui-ci rÃ©vÃ¨le que 79 % des consommateurs utilisent des mots de passe Ã risque, qu'ils construisent Ã partir d'informations personnelles et de mots courants.

Le sondage montre Ã©galement que **26 %** des personnes interrogÃ©es utilisent le mÃªme mot de passe pour plusieurs comptes clÃ©s, comme leur messagerie, leur compte bancaire, les portails d'achat en ligne et les rÃ©seaux sociaux. De plus, prÃ¨s de **8 %** des personnes interrogÃ©es avouent avoir copiÃ© leur mot de passe sur des listes trouvÃ©es sur Internet, supposÃ©es recenser les mots de passe les plus Â« fiables Â». On ne s'Ã©tonnera donc pas d'apprendre que **29 %** des personnes interrogÃ©es ont Ã©tÃ© victimes de piratages visant leur messagerie ou leur profil sur un rÃ©seau social, et que plus de la moitiÃ© de ces personnes (**52 %**) connaissent quelqu'un ayant vÃ©cu une expÃ©rience similaire.

Quâ□□il sâ□□agisse dâ□□accÃ©der Ã un compte sÃ©curisÃ© ou de s'infiltrer dans un ordinateur, la premiÃ¨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 automatisÃ©s qui Â« devinent Â» les mots de passe en essayant systÃ©matiquement tous les Ã©lÃ©ments d'information ou mots courants rÃ©pertoriÃ©s dans une base de donnÃ©es.

Autre enseignement du sondage ZoneAlarm :

22 % des personnes interrogÃ©es se sont dÃ©jÃ fait pirater leur messagerie Ã©lectronique et prÃ¨s de 46 % dâ□□entre elles connaissent quelqu'un ayant vÃ©cu pareille mÃ©saventure. De plus, 22 % des personnes interrogÃ©es dÃ©clarent avoir dÃ©jÃ Ã©tÃ© victimes d'un piratage de leur profil sur un rÃ©seau social, et 32 % connaissent quelqu'un ayant subi un dÃ©sagrÃ©ment similaire. Une fois qu'un pirate obtient l'accÃ¨s Ã un compte, il parvient dans prÃ¨s de 30 % des cas Ã rÃ©utiliser l'information obtenue pour accÃ©der Ã d'autres sites contenant des donnÃ©es financiÃ¨res, comme le numÃ©ro d'un compte bancaire ou d'une carte de crÃ©dit.

Â« *En cette pÃ©riode de fÃªtes, le nombre d'achats effectuÃ©s en ligne est plus Ã©levÃ© 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 sophistiquÃ©s pour les â□□craquerâ□□* Â», dÃ©clare **Bari Abdul**, vice-prÃ©sident en charge du service Ventes grand public chez Check Point. Â« *En crÃ©ant un mot de passe unique pour chaque compte clÃ©, les consommateurs bÃ¢tissent une premiÃ¨re ligne de dÃ©fense contre les cybercriminels qui n'ont qu'une idÃ©e en tÃªte : faire*

main basse sur les donnÃ©es critiques de leurs victimes dans un but lucratif. Â»

Pour permettre de rÃ©aliser des achats sur Internet en toute sÃ©curitÃ© et profiter sereinement des fÃªtes de fin d'annÃ©e, voici quelques conseils pour choisir un mot de passe hautement sÃ©curisÃ© :

â Choisir un mot de passe contenant au moins 8 Ã 10 caractÃ¨res.

Cette longueur devrait suffire Ã prÃ©venir les attaques par force brute. Une telle attaque consiste Ã essayer tous les codes, combinaisons et mots de passe imaginables jusqu'Ã identifier l'Ã©lÃ©ment qui sert de sÃ©same.

Â â Veiller Ã choisir un mot de passe difficile Ã deviner.

Ãvitez d'utiliser un nom, particuliÃ¨rement votre identifiant, le nom d'un membre de votre famille ou le nom d'un animal domestique. Gardez-vous Ã©galement d'utiliser des donnÃ©es personnelles, par exemple un numÃ©ro de tÃ©lÃ©phone, une date d'anniversaire ou le nom de la ville oÃ¹ vous Ãªtes nÃ©.

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

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

â Ãviter d'utiliser plusieurs fois le mÃªme caractÃ¨re ou des sÃ©quences faciles Ã deviner.

Exemple : 77777, 12345 ou abcde.

â Choisir un mot de passe qui associe des chiffres, des lettres et des caractÃ¨res spÃ©ciaux.

Plus votre mot de passe sera complexe et alÃ©atoire, et plus il sera difficile Ã un cybercriminel de le Â« craquer Â».

â Utiliser des fragments de mots, qui ne pourront pas Ãªtre trouvÃ©s 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 ssÃ©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.**