Internet: attention aux mots de passe trop simples!

Technologie

Posté par: Visiteur

Publié le : 15-03-2010 23:49:02

"1234", "password", "azerty", "harrypotter"... Les internautes, qui doivent entrer un mot de passe sur chacun de leurs comptes, en choisissent souvent de trop simples, peu conscients des risques de vols de données personnelles ou bancaires

"Il y a un manque de vigilance" des utilisateurs, reconnaît Bernard Ourghanlian, directeur sécurité de Microsoft France, estimant nécessaire un travail de "pédagogie" à ce sujet. Nom de l'enfant, du chat, date de naissance, mots du dictionnaire, suite de chiffres: "80% des mots de passe sont très facilement détectables", note Jean-Philippe Bichard, de l'éditeur de logiciels de sécurité Kapersky Lab.

L'enjeu est pourtant important : les cybercriminels qui parviennent à les détecter peuvent avoir accès à la messagerie des usagers, leurs comptes sur les réseaux sociaux ou encore leur banque en ligne. Libres à eux ensuite de faire des achats en ligne, de vendre les informations trouvées ou de se faire passer pour l'usager en envoyant des messages à ses amis pour leur demander, par exemple, de leur virer de l'argent. "Casser" les mots de passe est souvent un jeu d'enfant pour les pirates. L'attaque "par dictionnaire" consiste par exemple à passer en revue, via un logiciel, tous les mots du dictionnaire. Celle "par force brute" essaie, elle, tous les mots de passe possibles : succession de lettres, de chiffres, etc. Du fait de la rapidité des logiciels, il faut seulement "une seconde pour casser un mot de huit caractères simples", affirme un porte-parole de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Conséquence : il est impératif de bannir les mots de passe trop courts, les noms propres et communs, ceux de proches ou relatifs à notre environnement immédiat. Les pirates consultent en effet les réseaux sociaux, type Facebook, pour tenter de les deviner (lieux de villégiature, amis, etc.). Un bon mot de passe, explique M. Ourghanlian, doit être "long", et donc comporter "au moins huit caractères et dans l'idéal 14 ou plus". Il faut également "mélanger les caractères, en associant des lettres, avec des minuscules et des majuscules, des chiffres, des symboles (point d'interrogation, tiret...)". "La difficulté de casser le mot de passe varie de façon exponentielle avec le nombre de caractères : plus on rajoute de caractères différents, plus c'est difficile pour l'attaquant", note-t-il. Selon le porte-parole de l'Anssi, si le mot de passe comporte des minuscules et des majuscules, il ne pourra ainsi pas être trouvé avant "une semaine". "Et si on ajoute en plus des caractères spéciaux (tiret, etc.), on va dépasser le mois". Face à la difficulté de retenir un mot de passe d'une telle complexité, M. Ourghanlian conseille "d'utiliser plutôt une phrase comme MonfilsOliviera-de3ans, beaucoup plus simple à mémoriser" qu'une suite illogique. En aucun cas, le mot de passe ne doit en effet être écrit quelque part. Autre conseil : en changer pour chaque site, car s'il est découvert, tous les comptes de l'usager sont compromis. Pour éviter un casse-tête, la même phrase peut être conservée, mais en y ajoutant un élément se référant au site consulté. Par exemple: "AmazMonfilsOliviera-de3ans", sur Amazon. Des outils sur internet permettent, en cas de doute, de mesurer la force du mot de passe, à l'image de Password Meter. Et pour ceux que l'idée de retenir des dizaines de mots de passe effraie, des éditeurs, comme Kapersky Lab et Symantec (Norton), vendent des logiciels qui, via un mot de passe unique, en gèrent pour chaque site.
afp.com