SÃ©curitÃ© : Votre mot de passe est-il sÃ»r ?
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 5/10/2011 14:00:00

Une des faÃ§ons les plus courantes pour des tiers mal intentionnÃ©s de se procurer des mots de passe et autres informations personnelles est **le vol d'identitÃ©.**

Pour ce faire, un logiciel malveillant ou un virus sâ□□installe par inadvertance sur un ordinateur sans protection suffisante et utilise une Â«failleÂ» dans la sÃ©curitÃ© du systÃ¨me pour accÃ©der aux fichiers contenant ces donnÃ©es

sensibles et les renvoyer Ã lâ□□expÃ©diteur du logiciel malveillant.

Les cybercriminels peuvent Ã©galement installer des "keyloggers", logiciel dâ□□enregistrement de frappe clavier, qui enregistre les donnÃ©es saisies sur un ordinateur. Ces donnÃ©es sont Ã 95% inoffensives, pourtant elles

contiennent inÃ©vitablement des informations de connexion sur des sites sÃ©curisÃ©s tels que les banques en ligne et les sites marchands, avec nom, adresse, numÃ©ro de carte de crÃ©dit et les mots de passe eux-mÃªmes.

Le hameÃ§onnage est une autre faÃ§on courante de tromper les utilisateurs.

Cette mÃ©thode de fraude implique souvent des emails malhonnÃªtes qui semblent provenir d'une source lÃ©gitime demandant de fournir des renseignements personnels pour confirmer une transaction ou pour renouveler un service. Ces emails frauduleux sont souvent trÃ¨s habilement rÃ©digÃ©s et prÃ©sentÃ©s de faÃ§on Ã Ãªtre difficiles Ã dÃ©tecter.

La faÃ§on la plus simple pour se protÃ©ger contre ce genre de menaces est de s'assurer de disposer d'un logiciel de sÃ©curitÃ© moderne qui protÃ¨ge contre le vol d'identitÃ© et les tentatives dâ□□hameÃ§onnage, et de faire rÃ©guliÃ¨rement les mises Ã jour afin de contrer les

derniers virus et logiciels malveillants.

Comment choisir le bon mot de passe ?

Dâ□□aprÃ¨s un rÃ©cent sondage rÃ©alisÃ© par la sociÃ©tÃ© de sÃ©curitÃ© des donnÃ©es Imperva, qui a analysÃ© 32 millions de mots de passe afin de connaÃ®tre le classement des 10 mots de passe les plus couramment utilisÃ©s, cinq des

dix premiers Ã©taient simplement des suites de chiffres tels que "123456", ou le mot "password" (mot de passe en franÃ§ais) ou encore "abc123".

Bien que pratique et facile Ã retenir, il paraÃ®t Ã©vident que le choix dâ□□un tel mot de passe nâ□□est pas une bonne idÃ©e. De mÃªme, la plupart des experts en sÃ©curitÃ© informatique conseillent aux utilisateurs d'Ã©viter de fournir des

informations personnelles, telles que le nom de jeune fille d'une mÃ¨re, animal de compagnie prÃ©fÃ©rÃ©, lieu de naissance ou date de naissance.

Ceci pour deux raisons :

- premiÃ¨rement, parce que ce genre d'information est souvent utilisÃ© pour confirmer l'authenticitÃ© de lâ□□utilisateur avec les banques et services en ligne, et peut donc Ãªtre soumis Ã des escroqueries via la mÃ©thode du keylogging ou dâ□□hameÃ§onnage.

- DeuxiÃ¨mement, parce qu'il y a un risque quâ□□une personne que vous connaissez, ou quelqu'un qui aurait accÃ¨s Ã vos renseignements personnels, puisse Ãªtre celle ou celui qui essaie de se connecter sur votre compte.

La plupart des experts prÃ©conisent l'utilisation d'une combinaison alphanumÃ©rique (lettres et chiffres) dans un mot de passe. Prenez le nom dâ□□un joueur de foot prÃ©fÃ©rÃ©, par exemple Torres, et transformez-le en Tore32, ou bien le nom dâ□□un animal de compagnie, par exemple Tango, qui devient T4ng0. Une astuce qui permet dâ□□utiliser un mot familier tout en le rendant plus difficile Ã deviner. Cela peut sembler un peu compliquÃ©, mais

avec de la pratique, il devient presque naturel de tordre les mots courants de cette maniÃ¨re.

Il est Ã©galement important de changer rÃ©guliÃ¨rement un mot de passe, en particulier dans le cas de sites impliquant des transactions financiÃ¨res tels que les comptes bancaires, les services de paiement en ligne et les ecommerÃ§ants.

Toutefois, il vaut mieux Ã©viter dâ□□utiliser seulement une poignÃ©e de mÃªme mots de passe afin dâ□□Ã©viter que les cybercriminels se construisent une liste de mots et de phrases courantes sâ□□ils rÃ©ussissent Ã accÃ©der Ã un ordinateur.

D'autres moyens pour protÃ©ger les mots de passe et informations personnelles

Il est important de veiller Ã ce que les pages web qui demandent des dÃ©tails personnels utilisent bien un protocole de cryptage sÃ©curisÃ©, câ□□est Ã dire une page web qui affiche Â«https://Â». Cela indique que les informations

entrÃ©es seront cryptÃ©es et que des tierces parties ne pourront pas y accÃ©der.

De plus, de nombreux comptes de messagerie en ligne proposent aux utilisateurs de choisir de se connecter Ã partir de chez eux (donc un lieu sÃ©curisÃ©) ou Ã partir d'un lieu public, comme un cybercafÃ©. Il est important de toujours vÃ©rifier quâ□□une option ouvre une connexion avec une

sÃ©curitÃ© renforcÃ©e. En effet, certains dÃ©tails (comme le nom dâ□□utilisateur) peuvent Ãªtre conservÃ©s une fois la session terminÃ©e, ce qui signifie que ceux qui

utilisent ensuite lâ□□ordinateur public sont dÃ©jÃ Ã mi-chemin vers lâ□□accÃ¨s au compte.

MÃªme si les logiciels de sÃ©curitÃ© modernes sont trÃ¨s efficaces pour de protÃ©ger contre ce genre de menace, il est important d'Ãªtre bien informÃ© et de rester vigilant. Utiliser une combinaison des deux mÃ©thodes est encore la meilleure pratique pour garantir que les donnÃ©es personnelles restent hors dâ□□atteinte de mains malveillantes.