SÃ©curitÃ© des comptes, mieux vaut une phrase qu'un mot de passe
Internet
PostÃ© par : JulieM
PubliÃ©e le : 16/7/2012 14:00:00

On vous en parle souvent de la sÃ©curitÃ© de vos comptes et des mots de passeÂ pour y accÃ©der. Aujourdâ□□hui Yahoo, hier Linkedin, le piratage des**mots de passe et leur sÃ©curitÃ© est au cÅ□ur de lâ□□actualitÃ©.**

Ces sites majeurs ont dÃ©plorÃ© des fuites avec mise en ligne de millions de mots de passe dâ□□utilisateurs, alors faites **preuve d'imagination**.

Le jeu League of Legend a connu Ã©galement des failles, entraÃ®nant une divulgation de donnÃ©es clients (et de mots de passe notamment).

Que nous enseignent ces incidents en matiÃ¨re de sÃ©curitÃ© des mots de passe ? Que, malheureusement, les gens continuent Ã utiliser des mots de passe non sÃ©curisÃ©s, et que nous sommes encore trop nombreux Ã nous contenter de mots de passe incroyablement simples tels que Â« **1234** Â», ou des mots de passe faciles Ã deviner (comme travail ou linkedin).

MÃªme des **mots passes**, a priori plus Ã©laborÃ©s, ont Ã©tÃ© piratÃ©s (comme davidlinkedin qui associe un prÃ©nom Ã un nom de site, ou les jeux de mots relatifs aux sites utilisÃ©s tels que leakedin et linkedout).

Mais les utilisateurs peuvent Ã©galement renforcer la sÃ©curitÃ© de leurs mots de passe.

Voici quelques conseils Ã ce propos :

â□¢ Des phrases plutÃ´t que des mots.

Il est devenu essentiel de rallonger ses mots de mots de passe. Dix Ã douze caractÃ¨res Ã minima, et encore plus long pour vos sites les plus sensibles (comptes bancaires en ligne par exemple). Le traditionnel mot de passe se transforme donc en Â« phrase Â» de passe. Mais attention, des mots trop longs â□□ **supercalifragilisticexpialidement** par exemple - sont difficiles Ã retenir, et prÃ©sentent un risque dâ□□erreur de frappe.

Choisissez plutÃ´t des phrases au hasard (mÃªme dÃ©pourvues de sens) dont vous pouvez vous

souvenir pour des raisons personnelles et abstenez-vous dâ□□utiliser le nom de votre film favori ou des termes trop Ã la mode. Par exemple, Starwars est Ã Ã©viter. En revanche, **OrdiNagerMelonLampe** est plus indiquÃ©, car il fait rÃ©fÃ©rence Ã des objets et activitÃ©s usuels dont vous pouvez vous rappeler.

â□¢ Surtout ne rÃ©utilisez pas vos mots de passe.

Tous ceux qui ont Ã©tÃ© piratÃ©s seront, Ã minima, ajoutÃ©s Ã une liste des mots de passe connus et rÃ©utilisÃ©s par les pirates pour commettre leurs exactions. Si un identifiant dâ□□utilisateur a Ã©tÃ© Ã©galement piratÃ©, le pirate dispose alors dâ□□une paire identifiant+mot de passe quâ□□il peut utiliser pour dâ□□autres sites. En clair, nâ□□utilisez pas le mÃªme mot de passe pour plusieurs sites.

â□¢ Utiliser un gestionnaire de mots de passe

Ces astuces se limitent bien sÃ»r Ã la facultÃ© de tout un chacun de pouvoir se souvenir des mots de passe. Des gestionnaires de mots de passe comme DirectPass peuvent aussi simplifier la tÃ¢che des utilisateurs. Ces outils stockent les multiples mots de passe des utilisateurs, en environnement sÃ©curisÃ© et dans le Cloud permettant une utilisation Ã partir de plusieurs appareils : PC, Smartphones ou tablettes.