

MOTS DE PASSE

et autres tracas

Julie est dégoûtée. En rentrant de l'école ce matin, elle a trouvé la porte de son armoire grande ouverte : on aurait dit que quelqu'un avait fouillé dans ses affaires personnelles. C'est fort pénible, car elle y conserve d'anciennes lettres, son journal intime et bien d'autres choses qui ne regardent personne d'autre. Julie a l'habitude de toujours bien verrouiller son armoire, mais il semblerait qu'elle ait laissé traîner sa clé ce matin. C'est certainement sa petite sœur qui en a profité. Ah si, tout comme dans l'histoire d'Ali Baba et les 40 voleurs, elle pouvait aussi utiliser le mot de passe «Sésame, ferme-toi» pour barricader son armoire ...

Bonne idée! Sauf que Julie oublie que les 40 voleurs, quand ils sont retournés dans la caverne, ils l'ont retrouvée complètement vide. En effet, Ali Baba avait entendu le fameux mot de passe et avait eu le temps de s'emparer des trésors cachés dans la caverne. Pour qu'une telle mésaventure ne t'arrive pas, voici quelques conseils :



SECURITÉ DE L'INFORMATION

Les mots de passe n'existent pas que dans les contes de fées, mais également en informatique. Tu en utilises un, chaque fois que tu te connectes à ton PC. Ton identifiant (user name) et ton mot de passe (password) sont pour ton ordinateur la preuve que c'est bien toi. Tout le monde pourrait lire tes e-mails s'il ne fallait pas encoder ton mot de passe avant de les télécharger du serveur. Tu dois aussi taper ton mot de passe avant de pouvoir entrer dans un chatroom. Imagine ce qui pourrait arriver si une autre personne utilisait ton mot de passe : Tout le monde parlerait de tes secrets ou quelqu'un d'autre se ferait passer pour toi dans un chatroom. En ayant une page perso, par exemple sur party.lu, tout le monde pourrait la modifier. Et si cette photo embarrassante de toi y était publiée...

Le seul remède est un mot de passe en béton qui ne peut pas être deviné même par quelqu'un qui te connaît bien. N'utilise donc pas ton prénom, ta date de naissance, le nom de ton animal ou ton numéro de mobile. Construis un mot de passe en utilisant la première lettre des mots d'une phrase, par exemple : «Ma sœur Olga - Tamara est nulle». Ceci donnerait : «**MsOTen**». Rajoutes-y l'un ou l'autre caractère spécial par sécurité : «**MsO-Ten!**». Un mot de passe ne devrait pas avoir moins de six caractères, huit ou dix sont encore mieux. Si tu remplaces finalement l'une ou l'autre lettre par un chiffre, le «O» par un zéro par exemple, tu auras déjà un mot de passe bien sécurisé : «**Ms0-Ten!**» - si tu arrives à le mémoriser. N'oublie pas de changer souvent de mot de passe. Mais le meilleur mot de passe ne sert à rien, si tu l'écris quelque part où tout le monde peut le lire, comme sur un Post-it collé sur l'écran de ton ordinateur ...

Souviens-toi qu'un mot de passe, c'est comme un chewing-gum : «Ne l'échange avec personne, prends-en un nouveau de temps à autre et ne le laisse jamais traîner!»

Une dernière remarque : Le vol de mots de passe existe aussi sur Internet. Cela s'appelle **phishing** (hameçonnage) et fonctionne avec des copies conformes de pages web très connues. L'internaute est appelé à encoder ses données personnelles sur ces pages web plus vraies que nature. Cela est particulièrement dangereux lors d'achats et d'opérations bancaires en ligne. Ça ne risque donc pas de t'arriver si tu ne fais pas de shopping sur Internet.

