Bien choisir son mot de passe sur le net

Gk!(b8*3£)° Un mot de passe sans doute idéal pour contrer les attaques de pirates informatique. Même si vous vous contentez de lettres – majuscules et minuscules – et de chiffres, un mot de passe de 10 caractères représente plus 839 000 000 000 000 000 combinaisons possibles !

En ajoutant des signes de ponctuation ou autres, le nombre de combinaisons explose encore plus. Il est quasiment inviolable. A condition de ne le notre nulle part, ce qui est difficile en ce cas.

Choisir un mot de passe suffisamment compliqué pour ne pas être découvert mais assez simple pour le mémoriser.

Les sites internet demandent de créer un mot de passe pour vos comptes et pour pouvoir vous identifier par la suite et vous donner accès à vos données ou vous autoriser certaines actions (accéder à votre messagerie, faire vos opérations bancaires en ligne, lire le journal online auquel vous êtes abonné, commander des livres sur un site où vous êtes client,…)

L'accès à vos données, c'est justement ce qui intéresse les fraudeurs et c'est pourquoi vous avez tout intérêt à les protéger avec un mot de passe difficile à découvrir.

Les fraudeurs recherchent des données soit pour commettre eux-mêmes des escroqueries dont vous serez la victimes (comme détourner de l'argent de votre compte), soit pour vendre vos données à des malfaiteurs qui pourront alors vous nuire ou nuire à d'autres en agissant sous votre identité (p. ex. envoyer depuis votre messagerie des mails que vous n'avez pas écrits).

Qui dit vol de données informatiques pense avant tout à des attaques d'ordre technique.

Attaques techniques : pas de mots de passe courts : ne descendez pas en dessous de 6 caractères

Evitez les mots qui ont un sens courant, en ce compris les prénoms, lieux, célébrités,…

Mêlez au moins majuscules, minuscules, lettres, chiffres;

Si possible, ajoutez un ou plusieurs caractères spéciaux (ponctuation ou symboles). Utilisez tout le clavier.

Evitez les suites logiques (ex: lettres voisines sur le clavier azerty).

Plus le mot de passe est long et plus les caractères sont variés, plus nombreuses seront les possibilités que l'appareil du voleur devra passer en revue et plus l'attaque prendra du temps.

Un simple PC peut trouver un mot de passe de 8 lettres en environ 1 heures mais il lui faudra près d'un mois pour casser une combinaison de 8 caractères mêlant majuscules, minuscules et chiffres. Avez du matériel plus puissant, la recherche peut toutefois être plus rapide.

Attaques par ruse : vous avez choisi un mot de passe fort. Est-ce suffisant ? Non, il vous reste encore à prendre d'autres précautions au moins aussi importantes, car si le second danger qui guette un mot de passe est sa faiblesse, le premier est sa divulgation par vous-même ! C''e sont les attaques les plus fréquentes.

Attaque par hameçonnage : pour la fraude bancaire : En vous orientant vers un site imitant celui de votre banque ou en vous envoyant un mail émanant soi-disant de celle-ci, les fraudeurs vous demandent d'introduire vos données personnelles, code bancaire et mot de passe. S'ils arrivent à vous mettre en confiance, ils disposeront alors du moyen de subtiliser de l'argent de votre compte.

Méfiez vous de tout mail, appel téléphonique ou site suspect. Partez de l'idée qu'aucune personne bien intentionnée ne vous demande de lui confier ces informations secrètes, ne les donnez JAMAIS et avertissez votre banque de vos soupçons de malversation.

Attaque sociale : amis, ex-amis, collègues… Nombreuses sont les personnes qui possèdent beaucoup d'informations à votre sujet. Ajoutez à cela les renseignements qui ont été mis sur les réseaux sociaux, par vous ou par d'autres. En rassemblant ces données, il est possible de deviner vos mots de passe s'ils font référence à votre vécu. En matière de mot de passe, votre premier ennemi est votre premier cercle !

Soyez discrets dans les informations que vous mettez en ligne. Et ne choisissez pas un mot de passe relatif à des renseignements plus ou moins publics. Et bien sûr, ne notez pas le mot de passe sur un post-it collé à votre écran !

Attaque par keylogger : il existe des logiciels qui peuvent être installés à votre insu sur votre ordinateur et qui enregistre tout texte que vous tapez. Ces oublis espions peuvent être véhiculés par des mails suspects, des téléchargements dont vous n'êtes pas sûr, des logiciels et des applications inconnus… Soyez vigilant, même un peu paranoïaque.

Le mot que vous utilisez pour un petit site qui n'a pas les moyens technologiques d'être bien sécurité n'est pas important si les données qu'il protège ne sont pas intéressants pour autrui. Mais attention : une des techniques des escrocs est de partir à la pêche aux mots de passe sur ce type de sites et de les tester ensuite sur des comptes importants comme les messageries électroniques ou les sites web financiers. Si vous utilisez le même mot de passe pour tous les sites, ce n'est donc pas d'une seule clé d'accès que la personne malhonnête disposera, mais un passe partout !

C'est surtout pour les sites importants que vous devez absolument trouver un mot de passe fort : en tout cas les sites bancaires et tout ce qui touche à l'argent (paypal, ebay…) ainsi que les messageries. Pour ne pas avoir de maux de tête, vous pouvez garder un seul mot de passe fort pour tous les sites sensibles et le personnaliser par un ou deux caractères en rapport avec le site en question.

Pour mémoriser ses mots de passe

Partez d'une citation, d'un diction, d'un film, d'une chanson qui vous est propre. Gardez les premières lettres en mêlant majuscules et minuscules, ajoutez chiffres et signes qui font sens pour vous. EX : un consommateur averti en vaut d'eux! "ucaevd" - "UCAevd" – "U1CAevd2" – "U1CA:evd2!

Collez quelques mots dont l'association a du sens pour vous seul et mettez des majuscules par exemple à la première lettre.

Fautes d'orthographe et/ou de grammaire sont les bienvenues ! Ajoutez signe et/ou chiffre sans trop compliquer.

Les style sms : écrire les sons comme on les entend ex: cette fois, j'ai acheté un vélo plus neuf " 7X,ght1vlO+9

Sur les comptes critiques, changez de mot de passe au moins tous les 6 mois, même que quelques éléments.

Supprimez vos historiques si vous avez utilisé un ordinateur public.

N’utilisez pas le même mot pour votre identifiant login, et votre mot de passe, password.

Ayez le courage de ne pas cochez les cases se souvenir de moi ou connexion automatique dans vos formulaires d’identification en ligne, surtout si votre PC à plusieurs utilisateurs. Et tapez votre mot de passe à l’abri des regards.

N’envoyez jamais de mot de passe par mail, chat ou SMS.

Verrouillez vos Smartphones, tablette, ordinateur portable…) aussi soigneusement que votre ordinateur de bureau, pour autant bien sûr que ce soit possible. Ne perdez en effet pas de vue qu’un accès à vos comptes mail, facebook voire mobile banking est aussi possible depuis ces outils-là.

Dans une interview accordée à l'émission Last Week Tonight de John Oliver, Edward Snowden, ancien employé de la CIA et de la NSA qui a révélé le vaste programme d'espionnage " PRISM ", s'est entretenu au sujet des mots de passe utilisés sur Internet. Lorsqu'Oliver lui a demandé s'il était actuellement important d'avoir un mot de passe adéquat, Snowden a expliqué que les mauvais mots de passe, des mots de passe simplistes, étaient facilement vulnérables par les systèmes informatiques.

Mauvais mots de passe

Selon Snowden, un mauvais mot de passe est par exemple celui qui contient moins de huit caractères. " Les mots de passe de moins de huit caractères sont très courants. Un logiciel peut venir à bout d'un tel mot de passe en moins d'une seconde ", explique Snowden. Par ailleurs, un mot de passe ne doit jamais correspondre au nom d'un utilisateur ou à un numéro de téléphone.

Les phrases mot de passe ou " passphrases "

Selon Edward Snowden, une des meilleures manières d'obtenir un mot de passe sûr est de repenser notre approche de ceux-ci. Parmi les méthodes les plus efficaces, l'expert cite les " phrases mot de passe " ou " passphrases " qui consistent à choisir un morceau de chanson, la phrase d'un livre ou d'un film, un syntagme assez long qui n'a du sens que pour l'utilisateur en tant que mot de passe. .

Snowden cite en exemple le mot de passe " margaretthatcheris110%SEXY ", une phrase facilement mémorisable et que seul l'utilisateur emploierait. En outre, cette phrase contient un mélange de majuscules, de minuscules, de numéros et de symboles, détails très difficiles à déchiffrer par un logiciel de piratage informatique.

Varier les mots de passe

Enfin, l'ancien agent de la CIA recommande de ne pas utiliser toujours le même mot de passe pour plusieurs programmes ou pages internet. Ne pas varier ses mots de passe peut être, selon Snowden un arme à double tranchant, raison pour laquelle il est préférable d'avoir en mémoire trois mots de passe qui peuvent être utilisés selon les contextes.