



CASES articles

De nombreux mots de passe ne sont pas sûrs

XpS4;rIV1 – Votre mot de passe ressemble-t-il à cela ?

Pour plus de sécurité, adoptez les réflexes CASES !

Une règle d'or de la sécurité informatique : de bons mots de passe

« Des mots de passe compliqués ? Mais personne ne peut les mémoriser ! » C'est ainsi que réagissent nombre de personnes lorsqu'on les interroge au sujet des mots de passe. Les mots de passe font aujourd'hui partie intégrante de notre vie quotidienne : que ce soit pour l'e-banking, utiliser sa carte de crédit, consulter ses e-mails ou sécuriser l'accès à son ordinateur. Cette importante méthode d'authentification, qui existe depuis des siècles, a été remise au goût du jour grâce aux technologies de l'information modernes. La quantité d'informations privées disponibles sous forme numérique ne cesse d'augmenter. De nombreux services sont de nos jours proposés par l'intermédiaire d'Internet. Afin d'interdire les accès non autorisés, les mots de passe sont devenus un composant essentiel des mécanismes d'authentification actuels. Ils peuvent être considérés comme les clés du monde virtuel et leur bonne utilisation figure parmi les règles d'or de la sécurité informatique. Cependant, les mots de passe ne sont sûrs que si certaines règles sont appliquées.

De nombreuses techniques d'authentification reposent sur un secret : le code d'identification. Ce code est seulement connu de la personne qui souhaite s'authentifier et de la personne qui demande cette authentification. Il peut adopter différentes formes et combinaisons : il peut s'agir d'objets tangibles, comme d'une carte ou d'un document par exemple, il peut également s'agir de caractéristiques propres à son détenteur, comme une empreinte digitale. Le code repose également souvent sur un savoir propre à l'utilisateur – les mots de passe font partie de cette dernière catégorie. L'authentification à l'aide d'un mot de passe compte parmi les plus anciennes techniques de sécurité.

Si une tierce personne découvre le mot de passe d'un utilisateur, le vol et l'utilisation de l'identité de ce dernier ne peuvent être exclus. Un cybercriminel peut ainsi se faire passer pour l'utilisateur et procéder en son nom à des virements d'argent sur d'autres comptes ou solliciter des crédits. Il peut également utiliser cette identité pour téléphoner, envoyer des e-mails, exploiter l'ordinateur de la victime à des fins criminelles ou encore espionner son poste de travail. Face à de tels agissements, il est bien souvent très difficile pour la victime de prouver son innocence.

Méthodes d'attaque des cybercriminels

Nombreux sont les utilisateurs qui ignorent la valeur des informations

et des applications présentes sur leur ordinateur, ils sous-estiment en particulier leur valeur pour des tiers. Lorsque des mots de passe sont utilisés pour protéger ces données et ces applications, les utilisateurs ont tendance à toujours utiliser le même mot de passe, facilement

21 % des personnes questionnées ont révélé leur mot de passe en échange d'une tablette de chocolat

En avril 2008, l'organisateur du Salon de la sécurité informatique Infosecurity Europe a effectué un sondage auprès de 576 personnes à Londres. Les personnes questionnées, disposées à révéler leur mot de passe, ont reçu une tablette de chocolat. 21 % des sondés étaient disposés à révéler leur mot de passe sans hésitation. 46 % des femmes et 10 % des hommes interrogés étaient disposés à échanger leur mot de passe contre une tablette de chocolat. La moitié des sondés a déclaré connaître les mots de passe des collègues. 58 % des personnes étaient disposées à communiquer leur mot de passe au téléphone, sur demande du service informatique de leur société. 35 % des sondés déclaraient connaître une personne dans la société ayant connaissance des mots de passe de membres de la direction. 31 % des personnes utilisent le même mot de passe pour toutes leurs applications. 43 % indiquent ne jamais changer de mot de passe ou ne le changer que très rarement.

mémorisable. « Qui n'a encore jamais utilisé les prénoms des enfants, une date de naissance ou le nom d'un animal de compagnie en tant que mot de passe ? Dans ce cas, il est très facile pour un tiers de deviner le mot de passe d'un utilisateur. Il suffit de collecter quelques informations à son sujet, et ceci est très facile, notamment grâce à l'Internet et à l'attitude désinvolte adoptée par les utilisateurs lorsqu'il s'agit de leurs données personnelles. De nombreuses personnes sous-estiment la valeur des informations présentes sur leur ordinateur », explique Pascal Steichen, du portail de sécurité luxembourgeois CASES, fort de son expérience de formateur.

En outre, les cybercriminels utilisent des moyens techniques afin de découvrir les mots de passe. Certains programmes procèdent ainsi à l'essai systématique de tous les mots d'un vocabulaire. Il leur est ainsi possible de découvrir un mot de passe. Ce procédé est qualifié d'attaque par dictionnaire. Les mots d'usage courant sont donc inadaptés en tant que mots de passe sécurisés. Les pirates emploient également des outils informatiques permettant d'essayer toutes les combinaisons de signes, de chiffres, de caractères ou de lettres possibles. C'est ce que l'on nomme une attaque par force brute. Plus un mot de passe est long et plus les signes, chiffres, caractères et lettres qui le composent sont variés, plus l'outil du pirate mettra de temps à découvrir la bonne combinaison.

La rapidité des attaques par force brute

Combien de combinaisons un ordinateur acheté dans le commerce peut-il vérifier en une seconde ? Lors d'une attaque par force brute, 1 000 000 de combinaisons sont vérifiées par seconde. Le programme d'attaque utilisé est alors un

programme que l'on peut trouver gratuitement sur Internet.

Si un réseau est utilisé pour l'attaque plutôt qu'un seul ordinateur, le nombre de combinaisons vérifiées peut énormément augmenter. Les pirates utilisent des botnets à cet effet, constitués d'ordinateurs zombies. Il s'agit en l'occurrence d'ordinateurs télécommandés par les pirates. Les utilisateurs de ces machines ne savent pas qu'elles sont exploitées pour perpétrer une attaque par force brute. Si des pirates utilisent un botnet constitué par exemple de 2 500 ordinateurs zombies, ils sont en mesure d'essayer quelque 2 500 000 000 combinaisons de mots de passe par seconde. Les botnets atteignant cette taille sont courants.

Lors d'une attaque par force brute effectuée sur un ordinateur standard, un mot de passe constitué de 10 chiffres ne résiste ainsi guère plus de 60 minutes.

Un mot de passe constitué d'une combinaison de lettres capitales et minuscules, de chiffres, de caractères spéciaux et de signes de ponctuation, mais ne comprenant que 6 caractères, ne résistera que 3 jours, toujours sur un ordinateur standard et en utilisant un programme d'attaque gratuit disponible sur le net. Toutefois, si la longueur du mot de passe est augmentée pour atteindre 8 caractères, il faudrait environ 80 ans à un ordinateur standard pour découvrir la bonne combinaison.

Les caractéristiques d'un bon mot de passe

Sur la base des méthodes d'attaque actuelles, un bon mot de passe devrait être constitué d'une série aléatoire d'au moins huit caractères regroupant des chiffres, des lettres capitales et minuscules, ainsi que des caractères spéciaux.

Un mot présent dans le dictionnaire ne devrait en aucun cas être utilisé en tant que mot de passe. En outre, le mot de passe ne doit jamais reprendre des données personnelles.

Les mots de passe constituent les clés du monde virtuel ; à ce titre, ils doivent disposer des mêmes caractéristiques que leurs homologues dans le monde réel. Porte d'entrée, voiture, lieu de travail, garage ou boîte aux lettres – autant de lieux pour lesquels différentes clés sont utilisées, assurant différents niveaux de sécurité. Cette approche doit également être appliquée dans le monde virtuel : chaque application doit disposer de son propre mot de passe. L'importance des informations ou des applications à protéger déterminera le niveau de sécurité du mot de passe à utiliser. Le mot de passe de connexion à un chatroom sur la cuisine nécessite par exemple un niveau de sécurité moins élevé que celui utilisé pour protéger son poste de travail ou celui gardant l'accès à l'entreprise.

Les mots de passe peuvent être découverts par le biais d'attaques par force brute, c'est une question de temps. Ils devraient donc être modifiés fréquemment, au moins tous les trois à six mois, selon leur niveau de sécurité.

Comment choisir un bon mot de passe et le mémoriser ?

La question est pertinente : comment mémoriser deux, trois et même quatre mots de passe ou plus, tout en tenant compte de l'obligation de combiner au moins huit caractères constitués de chiffres, de lettres capitales et minuscules et de caractères spéciaux ? Une astuce simple permet de surmonter cette difficulté : *la phrase magique*.

La phrase magique est un procédé mnémotechnique et il suffit à l'utilisateur de formuler et de mémoriser une phrase simple. L'utilisateur

utilise ensuite la première lettre de chaque mot, ainsi que les signes et chiffres présents dans la phrase afin de constituer son mot de passe. Voici un exemple : **3 petits cochons: PIM, PAM et POUM!** Le mot de passe sécurisé ainsi obtenu est le suivant : **3pc:P,PeP!**. L'utilisateur pourrait également lire la phrase de droite à gauche ou utiliser la deuxième lettre de chaque mot afin de constituer son mot de passe. Cela donnerait les mots de passe suivants, tout aussi sécurisés : !PeP,P:cp3 et 3eo:l,AtO!

Mesures de sécurité relatives aux mots de passe

Un utilisateur ne devrait en aucun cas noter son mot de passe sur une feuille de papier et fixer celle-ci sur l'écran de son ordinateur ou sous son clavier. Cela équivaudrait à laisser la clé de la maison sur la porte d'entrée ou sous le paillasson. Les voleurs se verraient offrir une très belle opportunité de cambriolage. Les mots de passe ne devraient pas non plus être cachés dans le portefeuille, même camouflés en tant que numéros de téléphone. Les personnes malintentionnées connaissent ces astuces.

L'endroit le plus sûr pour conserver un mot de passe reste la mémoire. Si l'utilisateur oublie son mot de passe, il peut en référer et un nouveau mot de passe lui sera attribué par le système. Si ce nouveau mot de passe est un mot de passe standard, celui-ci devrait être immédiatement modifié par l'utilisateur. Les applications Internet mettent généralement à la disposition de l'utilisateur une fonction de récupération du mot de passe. Il suffit pour cela de s'identifier et de communiquer une adresse e-mail, le nouveau mot de passe est ensuite envoyé à cette adresse par e-mail. Ce dernier devrait être effacé après utilisation.

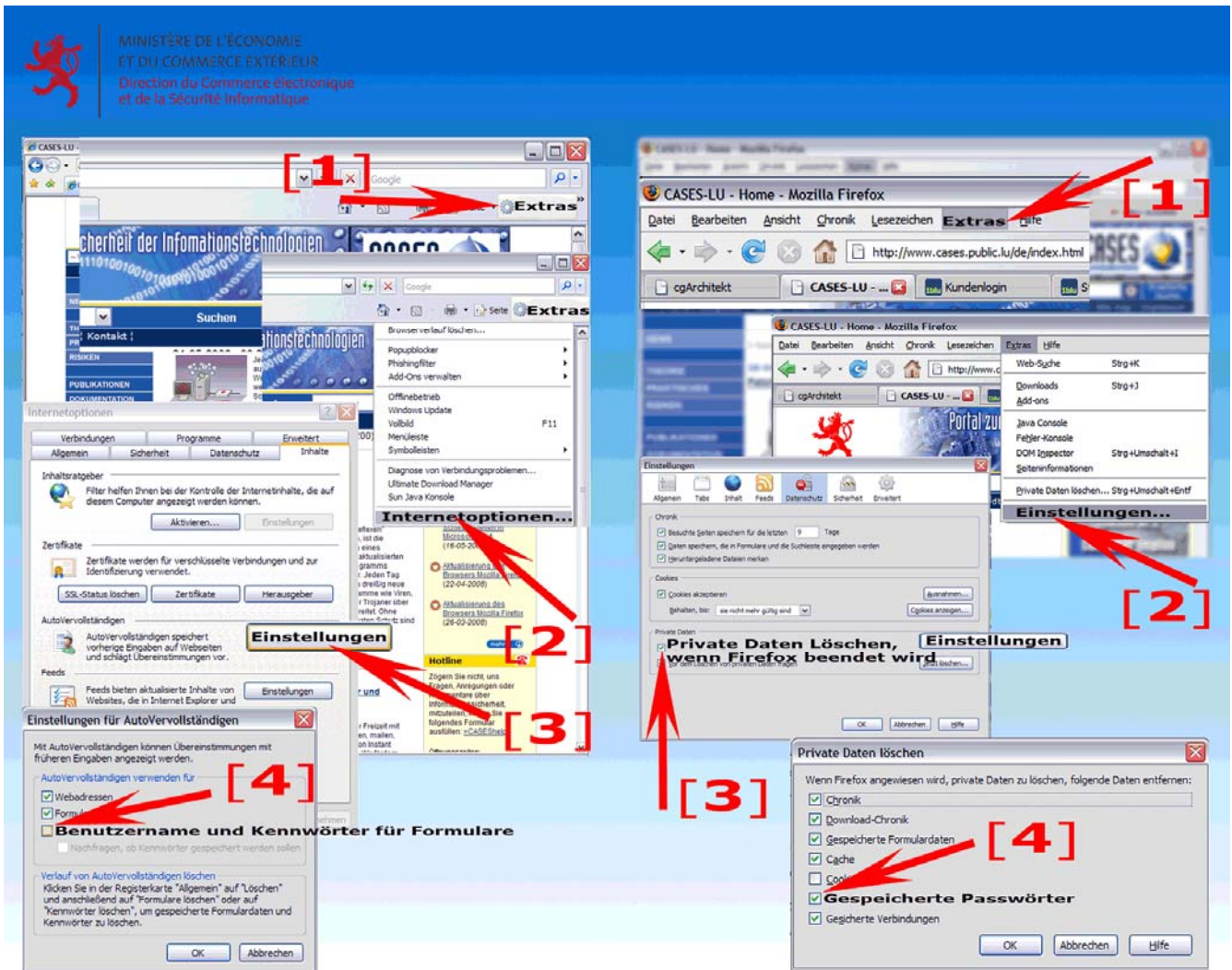
De nombreuses applications Internet proposent de mémoriser le mot de passe d'accès. L'utilisateur n'a ensuite plus besoin de le saisir pour accéder au service. Il est fortement déconseillé d'avoir recours à ce genre de fonctionnalité.

L'enregistrement automatique du mot de passe facilite en effet également l'accès d'autres personnes. Un pirate peut en outre attaquer cette application et obtenir le mot de passe qui y serait mémorisé.

Les choses peuvent devenir encore plus faciles pour le pirate si l'utilisateur utilise de surcroît ce même mot de passe pour plusieurs applications. Cela correspondrait à un voleur ayant obtenu une seule clé permettant d'ouvrir la porte de la maison, de démarrer la voiture et de pénétrer dans la société.

Dans certaines sociétés et professions, l'utilisateur doit employer un grand nombre de mots de passe différents. Dans ce cas, l'utilisation d'un logiciel spécifique de gestion des mots de passe peut s'avérer judicieuse. Cette application sera alors, à son tour, protégée par un mot de passe général. Il convient alors de choisir ce dernier avec soin et de le modifier fréquemment, ceci afin de préserver efficacement les mots de passe mémorisés par l'application.

COMMENT EFFACER LES MOTS DE PASSE DANS LE NAVIGATEUR



INTERNET EXPLORER

Désactiver l'enregistrement de nouveaux mots de passe est simple : dans la barre des menus du navigateur, cliquer sur [Outils] et [Options Internet], puis cliquer sur l'onglet [Contenu] et dans la rubrique [Saisie semi-automatique], cliquer sur le bouton [Paramètres]. Dans la fenêtre qui s'ouvre ensuite, l'option [Noms d'utilisateur et mots de passe sur les formulaires] doit être décochée. Il suffit ensuite de cliquer deux fois sur [OK].

Pour effacer les mots de passe déjà enregistrés, il suffit de cliquer sur [Outils] et [Options Internet] dans la barre des menus du navigateur, puis, dans l'onglet [Général], sous la rubrique [Historique de navigation], cliquer sur le bouton [Supprimer...]; dans la nouvelle fenêtre qui s'ouvre et sous la rubrique [Mots de passe], cliquer sur [Supprimer les mots de passe...] puis [Oui].

FIREFOX

Effacer des mots de passe est simple. Dans la barre des menus du navigateur, cliquer sur [Outils] et [Options...], cliquer ensuite sur [Vie privée]. Sous la rubrique [Vie privée], l'option [Toujours effacer mes informations personnelles à la fermeture de Firefox] devrait être cochée. Il faut ensuite cliquer sur le bouton [Paramètres...] et vérifier que l'option [mots de passe enregistrés] est également cochée. Il faut ensuite confirmer en cliquant sur [OK]. Ensuite, toujours sous la rubrique [Vie privée], cliquer sur le bouton [Effacer mes traces maintenant...], puis dans la fenêtre qui s'ouvre, cliquer sur [Effacer mes traces maintenant] puis sur [OK].

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu