5 astuces AVG pour se protÃ©ger contre le vol d'identitÃ© sur Internet
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 20/7/2010 0:00:00

AVG Technologies, dÃ©veloppeur de l'antivirus gratuit le plus utilisÃ© dans le monde, donne **ses 5 astuces pour aider les internautes Ã se protÃ©ger du vol dâ□□identitÃ©** sur Internet.

L'aspect le plus inquiÃ©tant au-delÃ du vol de lâ□□identitÃ© est que cela semble Ãªtre relativement simple Ã faire, et que les consÃ©quences peuvent Ãªtre Ã©pouvantables dans le monde d'aujourd'hui qui est entiÃ¨rement connectÃ© numÃ©riquement.

En fait, la fraude liÃ©e Ã l'identitÃ© permet Ã des criminels d'utiliser des informations personnelles pour obtenir de l'argent, mais Ã©galement pour ouvrir des comptes bancaires au nom de la personne piratÃ©e, de rediriger son courrier vers une autre adresse, voire d'obtenir un passeport en utilisant ses donnÃ©es personnelles. Voici donc ce quâ□□il faut faire pour empÃªcher ces fraudeurs de subtiliser suffisamment

d'informations, pour cloner son identitÃ©, ruiner ses finances mais aussi sa vie !

AVG Technologies propose une liste d'astuces qui aidera les internautes Ã rester en sÃ©curitÃ© et Ã tenir les fraudeurs Ã distance.

1- Ne jeter aucun des documents personnels suivants, Ã moins de ne les avoir dÃ©chirÃ© ou passÃ© dans un destructeur de documents afin qu'ils soient le moins utilisables possible : relevÃ©s de banque, factures de

services publics, formulaires d'inscription, talons de chÃ¨ques, tickets de cartes bancaires et lettres qui

contiennent des informations personnelles.

2- Prendre garde au hameÃ§onnage par tÃ©lÃ©phone, si quelqu'un demande des informations personnelles par tÃ©lÃ©phone, vÃ©rifier leurs informations et demander un numÃ©ro de tÃ©lÃ©phone afin de pouvoir rappeler

l'organisation et vÃ©rifier qu'elle est bien rÃ©elle.

3- Faire trÃ¨s attention lorsque lâ□□on est sur Internet, les attaques par hameÃ§onnage reprÃ©sentent un problÃ¨me en dÃ©veloppement constant, ne pas renseigner son adresse e-mail dans n'importe quel formulaire, et ne pas se faire avoir par les e-mails demandant des informations personnelles comme les informations relatives Ã son compte bancaire, ses noms d'utilisateur, ses mots de passe ou ses numÃ©ros de carte bancaire. Utiliser des mots de passe plus compliquÃ©s Ã trouver. L'annÃ©e derniÃ¨re, 20 000 comptes Yahoo, AOL et Hotmail ont Ã©tÃ© piratÃ©s et il s'est avÃ©rÃ© que pour ces comptes, lâ□□un des mots de passe les plus populaires avait Ã©tÃ© utilisÃ© : 123456.

Essayer d'utiliser une combinaison de lettres et de chiffres, puis changer ses mots de passe rÃ©guliÃ¨rement. Faire Ã©galement attention lorsque lâ□□on utilise les sites des rÃ©seaux sociaux, ce peut Ãªtre un moyen trÃ¨s simple de rÃ©cupÃ©rer des donnÃ©es.

4- Surveiller rÃ©guliÃ¨rement le statut de sa situation de crÃ©dit. De cette faÃ§on, il est possible de savoir qui fait des recherches sur ses crÃ©dits et si de nouveaux comptes ont Ã©tÃ© ouverts Ã son nom.

5- Lors dâ□□un dÃ©mÃ©nagement, faire suivre son courrier pendant au moins six mois, afin d'Ã©viter que des courriers importants contenant des informations personnelles nâ□□arrivent dans la boite aux lettres de quelqu'un d'autre.

Si lâ□□on suspecte une activitÃ© frauduleuse, il faut rÃ©agir vite et contacter sa banque, ses organismes de crÃ©dit auxquels on est inscrit, les magasins pour lesquels on a des cartes de paiement, les services publics et ses compagnies de tÃ©lÃ©phone pour qu'ils puissent dÃ©tecter toute activitÃ© anormale. Contacter Ã©galement des agences telles quâ□□Experian ou Equifax afin quâ□□ils vous aident Ã rÃ©soudre la situation. La CIFAS, qui est un service de prÃ©vention des fraudes, est une autre trÃ¨s bonne source de conseils pour le Royaume-Uni.

Si lâ□□on suit ces conseils simples et que lâ□□on est vigilant, cela peut nous faire Ã©conomiser beaucoup d'argent et d'heures passÃ©es Ã faire opposition Ã des cartes et Ã relancer les banques pour qu'elles nous remboursent l'argent volÃ©.

Il est Ã©galement possible dâ□□acheter AVG Identity Protection, qui, en plus de son antivirus, protÃ¨ge des curieux ses mots de passe, numÃ©ros de cartes bancaires et autres informations numÃ©riques de valeur.