

VeriSign Authentication, Les statistiques de la fraude sur Internet
Internet

Post   par : JPilo

Publi  e le : 16/11/2010 12:00:00

VeriSign Authentication, filiale de Symantec, publie la deuxi  me   dition de son barom  tre de la fraude sur Internet qui, chaque semestre, dresse **le bilan de la fraude sur Internet en France**.

Cette derni  re   dition fait appara  tre les   l  ments suivants :

   Le nombre de victimes de la fraude reste stable, avec 9 % de victimes de la cybercriminalit   sur l  ensemble de la population des internautes fran  sais au cours des 12 derniers mois ;

   La perte financi  re moyenne par victime de la fraude sur Internet s  l  ve    752    ;

   L  indemnisation des victimes suite    une fraude s  est am  lior  e : 79 % des personnes ayant r  pond   d  clarent que l  argent perdu leur a   t   totalement rembours  , soit une augmentation de 25 % depuis mars 2010 ;

   Le nombre de personnes qui pensent que l  argent qu  elles ont perdu sur Internet ne leur sera jamais rembours   a   t   divis   par deux, pour passer de 16 % en mars 2010    8 % en novembre ;

   En France, ce sont les hommes qui sont les plus susceptibles d    tre victimes de fraude : 10 % des r  pondants masculins d  clarent avoir   t   victimes d  une usurpation d  identit   en ligne au cours des 12 derniers mois, contre 7 % des femmes ;



   Les habitants de la r  gion Nord-ouest sont les moins prudents : seulement 77 % d  entre eux affirment effectuer leurs achats uniquement sur des sites    s  curit   renforc  e, contre une moyenne nationale de 80 %. Les Parisiens sont les plus m  fiants : ils affirment    84 % n  acheter que sur des sites s  curis  s.

D  clarations :

Danilo Labovic, directeur de l'activité SSL chez VeriSign Authentication, Symantec, rappelle :
« Les cybercriminels ont seulement besoin de trois informations pour dérober une identité numérique. Bien que l'usurpation d'identité en ligne n'entraîne pas obligatoirement une perte financière immédiate et que les victimes soient indemnisées plus facilement, les internautes ne doivent pas oublier que les fraudeurs exploitent les e-mails et les sites des réseaux sociaux pour collecter des informations qui leur permettent de dérober une identité. Ils peuvent également revendre ces données à des personnes qui pourront les utiliser de manière frauduleuse. Les consommateurs doivent rester vigilants en permanence, lire les politiques de sécurité des sites qu'ils consultent, vérifier leurs paramètres de confidentialité et prêter attention aux certificats et cachets de sécurité.

Les entreprises peuvent sortir du lot dans le climat économique actuel en renforçant la sécurité de leurs sites Web et en démontrant aux consommateurs qu'elles appliquent des règles de sécurité rigoureuses, à l'instar de l'authentification renforcée ou l'EV SSL qui permet d'afficher en vert la barre d'adresse d'un site sécurisé, pour permettre aux consommateurs de réaliser leurs transactions en ligne en toute quiétude. »

Pour surfer sans risque, VeriSign Authentication recommande les mesures suivantes :

1. Protégez votre ordinateur à l'aide d'un pare-feu personnel et d'un logiciel antivirus. Déconnectez-vous d'Internet quand vous n'êtes pas en train de surfer. Si vous utilisez un ordinateur portable, créez un mot de passe bloquant l'accès à vos informations.

2. Conservez vos mots de passe en lieu sûr. Ne choisissez pas des mots de passe faciles à deviner, ne les communiquez à personne. Modifiez fréquemment vos mots de passe. Dans la mesure du possible, utilisez une authentification renforcée ou bifactorielle qui, pour vérifier votre identité ou une transaction, couple une information que vous connaissez (identifiant et mot de passe) à un objet que vous possédez (une carte, un jeton ou un téléphone portable).

3. Vérifiez si le site Web que vous consultez est sûr. Avant de saisir vos informations de paiement, quel que soit le site Web consulté, vérifiez que l'URL commence par https (le « s » signifie « sécurisé »). Évitez tous les sites qui présentent des fautes d'orthographe évidentes et qui ne peuvent pas prouver leur sécurité. En cas de doute, cliquez sur l'icône VeriSign pour vérifier l'identité d'un site. Si possible, utilisez un navigateur Web à haute sécurité qui affiche la barre d'adresse verte Extended Validation (EV, Validation étendue).

4. Ne téléchargez pas les pièces jointes des e-mails et ne cliquez pas sur un lien indiqué dans un e-mail, sauf si celui-ci est envoyé par une personne de confiance. Ne communiquez aucune information confidentielle par e-mail. N'oubliez pas que les sites Web financiers ne vous demandent jamais de fournir votre identifiant, votre mot de passe, votre numéro d'identification personnelle ou toute autre information confidentielle par e-mail. En revanche, un fraudeur vous les demandera !

5. Vérifiez que vous utilisez un réseau WiFi sécurisé. Définissez un mot de passe pour sécuriser votre réseau sans fil domestique et évitez d'effectuer des achats en ligne ou de consulter un site financier sur un réseau WiFi public.