ASSEMBLÉE NATIONALE

13ème législature

Internet

Question écrite n° 74297

Texte de la question

M. Philippe Plisson attire l'attention de Mme la secrétaire d'État chargée de la prospective et du développement de l'économie numérique sur le phénomène de la cyber-escroquerie qui touche déjà des dizaines de milliers de citoyens français. Depuis l'ouverture du réseau Internet au trafic commercial au début des années 1990, les cyber-escroqueries n'ont cessé d'augmenter et sont un vrai fléau international. Les services comme paypal ou moneybookers sont régulièrement clonés pour faire de faux sites à ces enseignes. Les banques françaises et européennes font aussi l'objet d'usurpation. De faux courriels à enseigne de ces banques sont envoyés par centaines de milliers aux internautes dans le but d'obtenir l'identifiant et le mot de passe de leur compte bancaire en ligne. Des faux documents à l'enseigne de grandes banques internationales se multiplient. Il en va de même pour les abonnements des internautes. Des faux courriels à en-tête de Orange, Free, Club Internet, Alice-adsl, etc., circulent chaque jour. Très récemment, la SACEM, la CAF, mais également l'administration fiscale française faisaient l'objet d'usurpation, dans le cadre d'une tentative d'escroquerie visant à récupérer des numéros de cartes bancaires. Les internautes se voient proposer de fausses offres d'emploi ou des stages rémunérés. Les candidats sont invités à envoyer un dossier de candidature et devront s'acquitter des frais de dossier de 100 à 350 euros. Les victimes, qui bien souvent auront avisé « Pôle emploi » de ce nouvel emploi, ne sont plus indemnisées pendant un certain temps. Ce phénomène prend aussi la forme d'annonces de gain à une loterie, d'héritage ou de don *via* le courrier électronique. Se référant à l'ordonnance n° 2009-104 du 30 janvier 2009 article 19, le Crédit agricole d'Aquitaine a récemment demandé par courrier électronique à ses clients la transmission de la copie de leur pièce d'identité et d'un justificatif de domicile, proposant de retourner les documents scannés par voie électronique. Il s'agissait là d'une demande réelle mais, pour le consommateur, il est de plus en plus difficile de faire la part entre le vrai et le faux, tant ils sont peu ou mal informés des risques et des pratiques. Eu égard à ces observations, il lui demande quelles mesures elle compte prendre pour protéger les internautes français des cyber-escroqueries.

Texte de la réponse

Le développement de l'Internet offre de nouvelles opportunités à une criminalité en constante évolution. Pour y répondre, les moyens humains et juridiques des forces de sécurité sont renforcés et leurs méthodes d'investigation modernisées. Un vaste plan d'action de lutte contre la cybercriminalité a été engagé en 2008, qui incombe à titre principal à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire. Le Gouvernement a présenté le 6 janvier 2009 un plan de lutte contre les escroqueries et les abus de confiance, dans le cadre duquel d'importants moyens d'actions sont mobilisés. Ce plan a permis d'intensifier la lutte contre les escroqueries, commises notamment par le biais d'Internet. Une campagne de sensibilisation de grande ampleur a ainsi été mise en oeuvre, avec, par exemple, la mise en place de plaquettes d'information et la diffusion via Internet de mises en garde. Par ailleurs, une plate-forme téléphonique « Info escroqueries », rattachée à l'OCLCTIC, a été créée en 2009. Elle permet à toute personne craignant d'être victime d'une escroquerie de contacter des policiers ou des gendarmes pour disposer d'informations sur le risque et de conseils sur les démarches à suivre.

Au 1er juin 2010, près de 30 000 appels ont déjà été enregistrés. Depuis le mois de janvier 2009, une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), composée de policiers et de gendarmes, permet en outre de traiter les informations des fournisseurs d'accès et du public concernant les contenus illicites sur l'Internet (www.internet-signalement.gouv.fr). Près de 80 000 signalements ont été reçus. Les capacités de détection et d'investigation ont également été accrues par le dispositif, pleinement opérationnel depuis un arrêté du 30 mars 2009, des « cyberpatrouilles ». Le MIOMCT coopère avec la plate-forme nationale de signalement des « spams » (www.signal-spam.fr) qui s'est récemment renforcée avec le soutien de la CNIL et du secrétariat d'État. Ce dispositif offre aux citoyens des outils d'information et de prévention concrets contre les escroqueries sur l'Internet et facilite les investigations des forces de sécurité. Au-delà, la lutte contre la cybercriminalité exige une approche globale, fondée en particulier sur la coopération internationale. La France a ainsi favorisé d'importantes avancées durant sa présidence de l'Union européenne. À son initiative, il a été décidé de créer une plate-forme européenne de signalement des infractions relevées sur l'Internet, dont l'élaboration est en cours. Une active coopération internationale est également menée, par le canal d'INTERPOL ou dans le cadre de relations bilatérales avec les pays « sources ».

Données clés

Auteur : M. Philippe Plisson
Circonscription : Gironde (11e circonscription) - Socialiste, radical, citoyen et divers gauche
Type de question : Question écrite
Numéro de la question : 74297
Rubrique : Télécommunications
Ministère interrogé : Prospective et économie numérique
Ministère attributaire : Prospective et économie numérique

Date(s) clée(s)

Question publiée le : 16 mars 2010, page 2878
Réponse publiée le : 23 novembre 2010, page 12973