ASSEMBLÉE NATIONALE

14ème législature

Internet

Question écrite n° 35116

Texte de la question

M. Christophe Castaner attire l'attention de Mme la ministre déléguée auprès du ministre du redressement productif, chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, sur la multiplication de tentatives de fraude *via* courriel par l'usurpation d'identité d'entreprises (banques, assurances) dans le but de récolter des informations confidentielles. Les techniques utilisées par les fraudeurs s'avèrent de plus en plus poussées (imitation du nom de domaine, même charte graphique, appel téléphonique) et mettent en dangers de nombreux citoyens, notamment ceux qui sont les plus fragiles, et les plus crédules. La divulgation des données (codes confidentiels et numéros de comptes) entraîne des conséquences désastreuses pour les particuliers. Aussi il souhaiterait savoir comment elle envisage de lutter contre ces pratiques, de coordonner les actions de lutte avec les entreprises concernées, et de mieux informer les internautes.

Texte de la réponse

La sécurité de l'espace numérique constitue pour la société (acteurs économiques, particuliers...) et pour l'Etat un enjeu majeur alors que le développement d'Internet et des systèmes d'information offre de nouvelles occasions à une criminalité, souvent internationale, qui sait tirer profit des structures de l'environnement numérique (anonymisation, etc.). Parmi les manifestations les plus visibles de cette délinquance figure le « phishing » (« hameçonnage »), qui vise à recueillir des informations personnelles confidentielles par des envois de mels falsifiés qui se présentent comme des messages provenant d'organismes familiers. Les victimes, trompées par la qualité supposée de l'expéditeur, fournissent leurs données bancaires. Banques, grandes sociétés et organismes publics sont la cible de fréquentes campagnes de « phishing ». Comme d'autres acteurs publics et privés, les forces de sécurité de l'Etat consacrent d'importants moyens, humains et techniques, à la lutte contre la cybercriminalité sous toutes ses formes. L'action de la police et de la gendarmerie nationales s'appuie sur un réseau de plus de 600 enquêteurs spécialisés dans le numérique. Au sein du ministère de l'intérieur, cette mission 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. Composé de policiers et de gendarmes, cet office central anime et coordonne l'action des services centraux et territoriaux de la police judiciaire, conduit des actes d'enquête et des travaux techniques d'investigation en appui de nombreux services, aussi bien de police et de gendarmerie que d'autres administrations (direction générale des douanes et droits indirects, etc.). La collaboration est particulièrement développée avec la gendarmerie nationale, dont le service technique de recherches judiciaires et de documentation est doté d'une division de lutte contre la cybercriminalité. La gendarmerie dispose aussi d'une expertise judiciaire avec son département informatique et électronique de l'institut de recherche criminelle de la gendarmerie nationale, à l'instar du service central de l'informatique et des technologies de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire. La cybercriminalité étant largement un phénomène transnational, les coopérations bilatérales avec les pays « sources » sont renforcées et la coopération se développe dans les enceintes européennes et internationales (Union européenne, Conseil de l'Europe, G8, Interpol...). L'OCLCTIC dispose aussi d'un groupe d'enquête mixte police-gendarmerie spécialisé dans la répression des principales

infractions de cybercriminalité. Sur le plan juridique, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a créé une incrimination pénale d'usurpation d'identité sur Internet. Une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) a été mise en place en 2009 pour exploiter le site www. internet-signalement. gouv. fr, qui offre des conseils de prévention et permet aux internautes et aux professionnels de signaler, de manière simple, tout contenu illicite de l'Internet. Ces signalements peuvent être le point de départ de l'ouverture d'une enquête pénale. La plate-forme, composée de policiers et de gendarmes et placée au sein de l'OCLCTIC, a reçu en 2012 près de 120 000 signalements, dont des milliers ont été transmis pour enquête aux services répressifs français et à Interpol. 60 % de ces signalements concernent des escroqueries commises sur Internet. Au cours des sept premiers mois de 2013, PHAROS a reçu plus de 80 000 signalements, dont près de 20 000 concernaient des faits de « phishing ». Le nombre de signalements reçus par PHAROS témoigne d'une réelle visibilité du site www. internet-signalement. gouv. fr, dont l'existence est signalée sur de nombreux sites publics ou privés, et qui est immédiatement identifiable via les grands moteurs de recherche. Une plate-forme téléphonique d'information et de prévention du public sur toutes les formes d'escroqueries existe également. Appelée « Info escroqueries » et composée de policiers et de gendarmes, elle reçoit plus de 40 000 appels par an. Il convient à cet égard de rappeler que le « hameçonnage » relève dans la plupart des cas de la qualification pénale d'escroquerie ou de tentative d'escroquerie. De nombreux organismes publics et privés mènent des campagnes de sensibilisation face aux risques du « phishing » et certains ont mis en place un dispositif de signalement. PHAROS demeure toutefois le point central national unique de recueil des signalements. PHAROS et l'association Phishing Initiative préparent une convention de partenariat qui permettra une transmission réciproque des signalements pour en assurer un traitement plus efficace, avec en particulier la mise à disposition des internautes d'un formulaire en ligne permettant le signalement facile des URL qui dirigent vers des sites de phishing. Les organismes sociaux et les autres acteurs privés ciblés par des campagnes de « phishing » pourront s'associer à ce dispositif. Par ailleurs, le Gouvernement a engagé une adaptation du dispositif de lutte contre la cybercriminalité. A la suite du séminaire gouvernemental sur le numérique du 28 février dernier, il a été décidé de mettre en place un groupe de travail interministériel (Justice/Economie et Finances/ Intérieur/ Economie numérique). Ce groupe de travail a commencé à se réunir en juillet 2013 et devrait rendre son rapport d'ici à la fin de l'année. Il est chargé d'élaborer une stratégie globale de lutte contre la cybercriminalité, prenant en compte la dimension internationale et européenne du phénomène, et portant notamment sur le développement des dispositifs d'aide aux victimes et de sensibilisation des publics. Une prévention efficace contre les fraudes de type « hameçonnage » passe en effet d'abord par une sensibilisation des internautes, ainsi que par l'emploi de navigateurs intégrant par défaut des systèmes de contre-mesures.

Données clés

Auteur : M. Christophe Castaner
Circonscription : Alpes-de-Haute-Provence (2e circonscription) - Socialiste, écologiste et républicain
Type de question : Question écrite
Numéro de la question : 35116
Rubrique : Télécommunications
Ministère interrogé : PME, innovation et économie numérique
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 30 juillet 2013, page 8079
Réponse publiée au JO le : 19 novembre 2013, page 12117