ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 24394	De **M. Alain Rousset** (Socialiste, républicain et citoyen - Gironde)	**Question écrite**

Ministère interrogé > Économie et finances	**Ministère attributaire** > Intérieur

Rubrique >télécommunications	**Tête d'analyse** >Internet	**Analyse** > escroqueries. lutte et prévention.

Question publiée au JO le : **16/04/2013**
Réponse publiée au JO le : **24/09/2013** page : **10112**
Date de changement d'attribution : **07/05/2013**

Texte de la question

M. Alain Rousset attire l'attention de M. le ministre de l'économie et des finances sur la problématique de la multiplication des courriels frauduleux émanant d'individus se présentant comme opérateurs publics ou privés. Cette pratique est en effet en pleine croissance : l'usurpateur envoie à sa victime un message et récupère ses informations personnelles et bancaires pour accéder à des comptes et effectuer des opérations sous son identité. Si la DGCCRF (Direction générale de la concurrence de la consommation et de la répression des fraudes) assure la protection économique et la sécurité des consommateurs, il n'existe cependant aucun moyen direct de signaler la fraude à l'opérateur en question. Certains organismes, comme la CAF, ont initié une campagne de sensibilisation en direction de leurs usagers pour l'instauration d'une procédure de signalement automatique des courriels et sites internet frauduleux. C'est pourquoi il s'interroge sur l'opportunité de généraliser cet outil, et de créer sur la page d'accueil des sites de paiement en ligne un onglet « signalement de fraudes », qui permettrait d'alerter le consommateur. En conséquence il le remercie de bien vouloir lui préciser la position du Gouvernement, et les dispositions qu'il entend prendre afin de remédier à cette situation.

Texte de la réponse

La question de la multiplication des courriels frauduleux émanant d'individus se présentant comme opérateurs publics ou privés afin de récupérer des informations personnelles et bancaires pour accéder à des comptes et effectuer des opérations sous de fausses identités fait référence à la technique dite du « hameçonnage » (en anglais « phishing ») utilisée par les cyberdélinquants pour capter les données personnelles liées plus particulièrement aux moyens de paiement. Suivant le développement des techniques modernes d'information, cette nouvelle forme de déviance constitue une menace sérieuse qui se développe et doit être combattue avec la plus grande fermeté, notamment en généralisant le signalement des fraudes. A cette fin, le ministère de l'intérieur a d'ores et déjà mis en place un portail officiel généraliste de signalement des contenus illicites de l'Internet (www. internet-signalement. gouv. fr), géré par des policiers et des gendarmes placés auprès de la plateforme « PHAROS », rattachée à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Cette plateforme assure le traitement centralisé des signalements émanant d'internautes comme de professionnels et les oriente utilement vers les services et unités d'investigation. Ces derniers, dans le cadre des enquêtes initiées, sont appelés à rentrer en contact avec les opérateurs concernés et donc à leur diffuser l'information. Tout opérateur Internet peut ensuite retransmettre ces éléments à l'ensemble de ses clients en les invitant à adresser des courriels de signalement sur une adresse électronique au format « abuse@ », suivi du nom de domaine. Parallèlement à ces actions, il convient aussi de souligner l'existence de deux associations de professionnels, qui viennent par ailleurs de signer entre elles une convention de partenariat pour lutter contre ce phénomène. La première, Signal Spam

(www. signal-spam. fr), a été créée en 2004 et regroupe la plupart des organisations françaises concernées par la lutte contre les « pourriels ». Elle compte parmi ses partenaires la gendarmerie et la police nationales. Elle recueille les signalements relatifs aux « pourriels » eux-mêmes, quel que soit l'objet du message indésirable et les retransmet aux forces de sécurité. La seconde, Phishing Initiative (www. phishing-initiative. com), a été créée fin 2010 entre le CERT-LEXSI, Microsoft et Paypal. Elle est spécialement dédiée à la lutte contre les hameçonnages. Son blog (http ://blog. phishing-initiative. com/) donne tous les conseils utiles à leur signalement. Ce recueil de signalements peut déboucher, après vérification, sur le blocage des sites suspects dans les navigateurs (Explorer, Firefox, Chrome et Safari), voire à leur fermeture définitive. C'est plus de 25.000 sites qui ont ainsi été traités en 2012. L'ensemble de ces dispositifs publics et privés permet dés à présent de répondre aux besoins des utilisateurs d'Internet. Il n'apparait dés lors ni nécessaire, ni opportun de créer une nouvelle procédure de signalement. Pour autant, cela n'exclut pas que des campagnes de sensibilisation soient menées à l'instar de celles réalisées par les banques et les services de paiement en ligne auprès de leurs clients. Cet aspect sera utilement examiné dans le cadre du groupe de travail interministériel relatif à la lutte contre la cybercriminalité que les ministères de l'économie numérique, de la justice et de l'intérieur viennent de constituer pour renforcer la lutte dans ce domaine.