ASSEMBLÉE NATIONALE

12ème législature

Internet

Question écrite n° 113116

Texte de la question

M. Thierry Mariani appelle l'attention de M. le ministre d'État, ministre de l'intérieur et de l'aménagement du territoire, sur les escroqueries bancaires liées à l'utilisation d'internet. Le mode opératoire de l'escroquerie est le suivant : 1. Tout d'abord, des personnes mal intentionnées envoient en grand nombre d'E-mails à des particuliers, en leur demandant de mettre à jour leurs informations bancaires confidentielles, via un faux lien internet d'un grand établissement bancaire. 2. Ensuite, les réponses des particuliers répondant par manque de méfiance, sont ensuite transférées via le faux lien internet sur l'email des auteurs de l'escroquerie. Ces derniers disposant ainsi, d'un accès total aux comptes de leurs victimes. Il se trouve qu'il existe aujourd'hui un nombre de plus en plus important de personnes victimes de cette escroquerie. C'est pourquoi, il le prie de bien vouloir lui indiquer quelles sont les mesures en vigueur afin de limiter au maximum ce type d'agissement.

Texte de la réponse

Au sein de la criminalité informatique, le « phishing » est un phénomène qui se développe en France. Contraction des mots anglais « fishing » et « phreaking », qui signifient respectivement « pêche » et « piratage de lignes téléphoniques », il s'agit d'une méthode de captation de données bancaires en vue de leur utilisation au détriment des clients de banques ou de sites marchands. Plus précisément, les pirates usurpent l'identité d'une entreprise (banque ou site de commerce électronique, par exemple) et invitent les internautes à mettre à jour des informations qui les concernent par le biais d'une page « web » factice, copie conforme du site original. Grâce aux données confidentielles (identifiants, mot de passe, numéro de compte bancaire, notamment) ainsi récupérées, les escrocs sont ensuite capables de transférer directement l'argent sur un autre compte ou de mettre ces données à disposition sur des sites de « hacking » qui proposent des conseils de piratage. Cette escroquerie, apparue dans le monde anglo-saxon, pose le problème de la sécurité des relations dématérialisées « banque-client ». Elle fragilise la confiance dans les nouveaux systèmes de transactions ou de communication et porte atteinte au développement des « e-banques » et des « e-commerces ». Pour lutter contre cette menace, plusieurs actions ont été impulsées sous la coordination de 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. La Fédération bancaire française et le Groupement d'intérêt économique cartes bancaires, en partenariat avec l'OCLCTIC, ont élaboré, dès 2004, un dispositif d'alerte en direction des établissements bancaires. Il vise à détecter, dans les meilleurs délais, les courriels qui contiennent les adresses de sites Internet qui contrefont de véritables sites de banque, à organiser une veille sur Internet afin d'y rechercher les adresses qui présentent des similitudes suspectes avec celles d'établissements financiers et bancaires et, enfin, à prévoir des mécanismes de contrôle qui permettent le dépistage rapide de virements frauduleux en vue de leur blocage. Une procédure de fermeture des sites litigieux, y compris quand ils sont situés à l'étranger, est également prévue par l'intermédiaire des différents computer emergency response team (CERT). Cette procédure démontre que ces sites de fausses « banques » sont installés fugacement et que leur localisation est compromise en raison de leur grande mobilité programmée par leur concepteur. Parallèlement, les établissements visés sont invités à déposer plainte systématiquement. Ainsi, l'OCLCTIC est en charge de

plusieurs affaires de « phishing » qui nécessitent l'activation des réseaux de coopération internationale, notamment avec la Russie. Afin d'augmenter les capacités de réponse des enquêteurs dès le dépôt de plainte effectué par les internautes, un accent particulier est porté sur la lutte contre ce nouveau mode opératoire lors des sessions de formation des référents « cybercriminalité » des services territoriaux de police judiciaire et de sécurité publique. Enfin, le réseau bancaire en coordination avec l'OCLCTIC déploie de nombreux efforts en matière de communication et de prévention auprès de ses clients afin de les sensibiliser sur les risques potentiels encourus et les inviter au respect des règles de sécurité.

Données clés

Auteur : M. Thierry Mariani
Circonscription : Vaucluse (4e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 113116
Rubrique : Télécommunications
Ministère interrogé : intérieur et aménagement du territoire
Ministère attributaire : intérieur et aménagement du territoire (II)

Date(s) clée(s)

Question publiée le : 12 décembre 2006, page 12885
Réponse publiée le : 10 avril 2007, page 3602