IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

RESSENYA

Jornada sobre Riscos Penals de la Banca en Línia

Rosa Fernández Palma

Resum

Ressenya de la jornada organitzada el desembre de 2005 sobre els nous riscos a què la banca en línia i el comerç electrònic estan sotmesos a causa de l'augment d'atacs de tipus pesca electrònica o *phishing* i altres defraudacions semblants.

Paraules clau

phishing, *pharming*, delinqüència informàtica, seguretat a Internet, banca en línia, estafa informàtica

Tema

Dret penal i societat de la informació

Abstract

Review of the Seminar held in December 2005 concerning the new risks that online banking and e-commerce now face due to the rising number of attacks such as phishing and similar fraudulent acts.

Keywords

phishing, pharming, computer crime, Internet security, online banking, computer fraud

Topic

Penal law and Information Society

El dia 16 de desembre de 2005 els Estudis de Dret i Ciència Política de la UOC, sota la direcció acadèmica dels professors Óscar Morales García i Rosa Fernández Palma, van organitzar la jornada **Riscos Penals de la Banca en Línia. Pesca Electrònica i Targetes de Crèdit**. La sessió va tenir lloc a la seu central de la universitat a l'avinguda Tibidabo i hi van assistir de manera presencial professionals de diversos sectors i estudiants de Dret; però també, mitjançant videoconferència, el contingut de les ponències va ser retransmès a la seu de la Universitat de Cadis, des d'on hi van participar un grup d'estudiants i diversos sectors de l'entorn jurídic.

La jornada es va plantejar amb l'objectiu d'analitzar algunes modalitats delictives, properes a les defraudacions penals més clàssiques, que en els darrers temps han fixat els clients de la banca i del comerç electrònic com els seus objectius prioritaris. La pesca electrònica, l'ús de cavalls de Troia, les pàgines web falses o el *pharming* són algunes de les modalitats defraudatòries que han anat guanyant intensitat.

La finalitat de totes aquestes conductes és comuna: els atacs tenen com a objecte la captura del nom d'usuari i la contrasenya, que permeten al particular l'accés a pàgines web sensibles, com la seva entitat financera virtual, comerços electrònics, etc. L'atacant es val normalment de la creació de pàgines falses (fenomen que és conegut com a *falsejament d'identitat* o *web spoofing*), que simulen aquella pàgina a la qual l'usuari pretén accedir. Una vegada allà, la víctima, confiada de trobar-se en lloc

segur, introdueix el nom d'usuari i la contrasenya, que són immediatament capturats per l'espia.

D'entre els sistemes d'atracció de què es val l'atacant per conduir la víctima a la pàgina web falsa, el més conegut és la pesca electrònica de l'incaut: l'usuari rep un correu electrònic, aparentment de la seva entitat bancària, en què se l'adverteix que s'estan fent comprovacions de seguretat i se li comunica que si no segueix les instruccions que es detallen els seus comptes bancaris quedaran bloquejats (o cancel·lats!). La pesca electrònica se serveix del correu electrònic per a captar internautes i aconseguir que de manera voluntària es desprenguin de dades personals, amb l'excusa de la promoció de productes o sortejos, la realització d'un examen de seguretat o la seva inclusió en alguna base de dades de l'entitat bancària, cosa que li permetrà accedir als seus comptes bancaris de manera virtual.

Juntament amb la pesca electrònica clàssica, la captura de dades personals també es fa mitjançant cavalls de Troia especialment destinats al robatori de claus bancàries. El cavall de Troia espia és, per la seva permanència, si és possible, més perillós perquè permet, fins al moment en què es detecta i es desactiva, la recopilació d'informació sensible i, no poques vegades, el control de la màquina atacada. La instal·lació pot produir-se per l'accés a una pàgina web o l'obertura d'un correu electrònic –encara que aquest es trobi en blanc– i, una vegada operatiu, pot monitoritzar les pulsacions del teclat o els clics del ratolí.

La pesca electrònica, per més vistosa que pugui semblar, té un efecte limitat: no sempre és fàcil obtenir una bona pesca, perquè el nombre d'incauts cada vegada és més reduït gràcies a la difusió de conductes com aquestes i perquè requereix amb freqüència mitjans d'enginyera social per a ser activada, del tipus de missatgeria instantània, anuncis virtuals o contactes telefònics (el percentatge de víctimes reals de pesca electrònica se xifra en un cinc per cent). Més perill i eficàcia inclou la nova amenaça coneguda com a *pharming*, la base d'actuació de la qual la constitueix l'alteració de les adreces DNS, que permeten conduir l'usuari, de nou, a una pàgina web falsa i no a la que ha sol·licitat realment en escriure l'adreça. El sistema d'atac pot ser general si l'objecte d'assalt són els servidors DNS; en aquest cas, qualsevol usuari que pretengui accedir a l'entitat bancària, el DNS del qual s'hagi modificat de manera fraudulenta, en realitat anirà a la pàgina web falsa creada per a recollir les seves credencials bancàries. Però també és molt eficaç l'atac local, mitjançant la modificació del fitxer amfitrió, que s'encarrega de recordar les DNS més freqüents a què es connecta l'usuari. Una vegada alterat, es remet l'usuari a una pàgina web que imita la pàgina a la qual realment volia accedir. La modificació del fitxer pot fer-se després d'aconseguir el control de la màquina aprofitant alguna vulnerabilitat o mitjançant l'ús de virus o cavalls de Troia amb aquesta funcionalitat.

El matí de la sessió es va dedicar a analitzar en profunditat les modalitats d'atac descrites des d'un punt de vista tècnic, també els sistemes de prevenció arbitrats per les entitats financeres afectades, i les seves conseqüències per a facilitar més o menys l'accés al servei prestat a l'usuari. Per a això vam comptar amb professionals dels diversos sectors implicats, públics i privats, i també amb un representant de la Unitat de Delictes Tecnològics del Cos Nacional de Policia, tal com pot consultar-se en el programa de la jornada.

La segona de les taules es va dedicar a l'estudi de les dificultats que les modalitats delictives descrites presenten en l'àmbit de la investigació penal i policíaca, projectant els models d'investigació a cada una de les conductes i atorgant especial atenció a l'eficàcia i el respecte a les garanties constitucionals. En aquesta ocasió les ponències van ser a càrrec del senyor José Vicente Rubio, inspector en cap de la Unitat de Delictes Tecnològics del Cos Nacional de Policia, i l'il·lustríssim senyor Daniel de Alfonso Laso, magistrat de la Secció Desena de l'Audiència Provincial de Barcelona.

La tarda va permetre oferir l'aspecte més jurídic de la sessió, mitjançant l'estudi del tractament jurídic penal de les defraudacions bancàries en línia. Els problemes derivats de l'ús il·lícit i falsificació de targetes bancàries i la proposta de subsumpció jurídica van ser desenvolupats pel doctor Ruiz Rodríguez, professor titular de la Universitat de Cadis. L'estudi del règim jurídic penal de les conductes conegudes com a *pharming* o pesca electrònica va ser desenvolupat per l'Excel·lentíssim Senyor José Manuel Maza Martín, magistrat del Tribunal Suprem (Sala Segona).

Les conclusions fonamentals de la jornada van ser molt interessants, tant des del punt de vista tècnic, com jurídic. Es preveu que es publiquin en el proper número de la revista.

Citació recomanada

FERNÁNDEZ, Rosa (2006). «Ressenya de la "Jornada sobre Riscos Penals de la Banca en Línia"» [ressenya en línia]. *IDP. Revista d'Internet, Dret i Política.* Núm. 2. UOC. [Data de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/2/dt/cat/fernandez.pdf>
ISSN 1699-8154

Rosa Fernández Palma
mfernandezpa@uoc.edu

Llicenciada en Dret (Universitat Complutense de Madrid). Doctora en Dret (Universitat Autònoma de Barcelona).

Ha estat becària del Pla de formació de personal investigador de la Comunitat de Madrid i professora de Dret penal a la UCM i la UAB. Actualment és professora de Dret penal a la UOC i coordina el seminari de doctorat *Internet, dret i política* del programa de doctorat de la UOC.

És autora de publicacions relatives a delictes contra l'honor i la intimitat.

En l'actualitat l'àmbit d'interès que investiga se centra en la delinqüència relacionada amb les tecnologies de la informació i la comunicació, i ha participat en projectes d'investigació sobre la matèria, màsters, cursos de doctorat, jornades, i també ha fet diverses publicacions sobre aquest àmbit.

Magistrada suplent de l'Audiència Provincial de Barcelona.