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

www.uoc.edu/idp

RESEÑA

Jornada sobre Riesgos Penales de la Banca *On-line*

Rosa Fernández Palma

Resumen

Reseña de la jornada celebrada en diciembre del 2005 sobre los nuevos riesgos a los que está sometida la banca *on-line* y el comercio electrónico debido al aumento de ataques de tipo *phishing* y otras defraudaciones semejantes.

Palabras clave

phishing, *pharming*, delincuencia informática, seguridad en Internet, banca *on-line*, estafa informática

Tema

Derecho penal y sociedad de la información

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 día 16 de diciembre del 2005 los Estudios de Derecho y Ciencia Política de la UOC, bajo la dirección académica de los profesores Óscar Morales García y Rosa Fernández Palma, organizaron la jornada **Riesgos Penales de la Banca *On-line*. Pesca electrónica y tarjetas de crédito**. La sesión tuvo lugar en la sede central de la Universidad en la Avda. de Tibidabo y a ella asistieron presencialmente profesionales de diversos sectores y estudiantes de Derecho; pero también, a través de videoconferencia, el contenido de las ponencias fue retransmitido a la sede de la Universidad de Cádiz, desde donde participaron un grupo de estudiantes y diversos sectores del entorno jurídico.

La jornada se planteó con el objetivo de analizar algunas modalidades delictivas, cercanas a las defraudaciones penales más clásicas, que en los últimos tiempos tienen, en los clientes de la banca y del comercio electrónico, a sus objetivos prioritarios. La pesca electrónica (*phishing*), el empleo de troyanos, las páginas web falsas o el *pharming* son algunas de las modalidades defraudatorias que han ido ganado intensidad.

La finalidad de todas estas conductas es común: los ataques tienen como objeto la captura del nombre de usuario y la contraseña, que permiten al particular el acceso a páginas web sensibles, como su entidad financiera virtual, comercios electrónicos, etc. El atacante se vale normalmente de la creación de páginas falsas (fenómeno que es conocido como *web spoofing*), que simulan aquélla a la que el usuario pretende acceder. Una vez allí, la víctima, confiada en encontrase en sitio seguro, introduce su nombre de usuario y contraseña, que son inmediatamente capturadas por el espía.

De entre los sistemas de atracción de que se vale el atacante para conducir a la víctima a la página web falsa, el

más conocido es el *phishing* o pesca del incauto: el usuario recibe un correo electrónico, aparentemente de su entidad bancaria, en el que se le advierte que se están realizando comprobaciones de seguridad, comunicándole que, si no sigue las instrucciones que se detallan (enviar su nombre de usuario y contraseña), sus cuentas bancarias quedarán bloqueadas (o ¡canceladas!). El *phishing* se sirve del correo electrónico para captar *internautas* y conseguir que voluntariamente se desprendan de datos personales, con la excusa de la promoción de productos o sorteos, la realización de un examen de seguridad o su inclusión en alguna base de datos de la entidad bancaria, que le permitirá acceder a sus cuentas bancarias de modo virtual.

Junto al *phishing* clásico, la captura de datos personales se viene realizando también a través de troyanos especialmente destinados al robo de claves bancarias. El troyano espía resulta, por su permanencia, si cabe, más peligroso, porque permite, hasta el momento en que es detectado y desactivado, la recopilación de información sensible y, en no pocas ocasiones, el control de la máquina atacada. Su instalación puede producirse por el acceso a una página web o la apertura de un correo electrónico –aunque éste se encuentre en blanco–, y, una vez operativo, puede monitorizar las pulsaciones del teclado o el *cliqueo* del ratón.

La pesca electrónica, por más llamativa que pueda parecer, posee un efecto limitado: no siempre es fácil obtener una buena pesca, porque el número de incautos cada vez es más reducido gracias a la difusión de estas conductas y porque requiere con frecuencia de medios de ingeniería social para su activación, del tipo de mensajería instantánea, anuncios virtuales o contactos telefónicos (el porcentaje de víctimas *reales* de *phishing* se cifra en un cinco por ciento). Mayor peligro y eficacia encierra la nueva amenaza conocida como *pharming*, cuya base de actuación la constituye la alteración de las direcciones DNS, que permiten conducir al usuario, de nuevo, a una página web falsa y no a la que ha solicitado realmente al teclear la dirección. El sistema de ataque puede ser general, si el objeto de asalto son los servidores DNS, en cuyo caso, cualquier usuario que pretenda acceder a la entidad bancaria, cuyo DNS se haya modificado fraudulentamente, en realidad recabará en la página web falsa creada para la recogida de sus credenciales bancarias. Pero también resulta altamente eficaz el ataque local, a través de la modificación del fichero *hosts*, que se encarga de *recordar* las DNS más frecuentes a las que se conecta el usuario, una vez alterado, el usuario es remitido a una página web que imita a la que realmente quería acceder. La modificación del fichero puede hacerse tras lograr el control de la máquina aprovechando alguna vulnerabilidad o a través del empleo de virus o troyanos con esa funcionalidad.

La mañana de la sesión se dedicó a analizar en profundidad las modalidades de ataque descritas desde un punto de vista técnico, también los sistemas de prevención arbitrados por las entidades financieras afectadas, y sus consecuencias para la mayor o menor facilidad de acceso por parte del usuario al servicio prestado. Para ello contamos con profesionales de los diversos sectores implicados, públicos y privados, así como con un representante de la Unidad de delitos tecnológicos del Cuerpo Nacional de Policía, según puede consultarse en el programa de la jornada.

La segunda de las mesas se dedicó al estudio de las dificultades que las modalidades delictivas descritas presentan en el ámbito de la investigación penal y policial, proyectando los modelos de investigación a cada una de las conductas y otorgando especial atención a la eficacia y el respeto a las garantías constitucionales. En esta ocasión las ponencias corrieron a cargo de D. José Vicente Rubio, inspector jefe de la Unidad de Delitos Tecnológicos del Cuerpo Nacional de Policía y el Ilmo. Sr. Daniel de Alfonso Laso, magistrado de la Sección Décima de la Audiencia Provincial de Barcelona.

La tarde permitió ofrecer el aspecto más jurídico de la sesión, mediante el estudio del tratamiento jurídico penal de las defraudaciones bancarias en línea. Los problemas derivados del uso ilícito y falsificación de tarjetas bancarias, y la propuesta de subsunción jurídica, fueron desarro-

llados por el Dr. Ruiz Rodríguez, profesor titular de la Universidad de Cádiz. El estudio del régimen jurídico penal de las conductas conocidas como *pharming* o *phishing* fue desarrollado por el Excmo. Sr. José Manuel Maza Martín, magistrado del Tribunal Supremo (Sala Segunda).

Las conclusiones fundamentales de la jornada resultaron muy interesantes, tanto desde el punto de vista técnico, como jurídico. Está prevista su publicación en el próximo número de esta revista.

Cita recomendada

FERNÁNDEZ, Rosa (2006). «Reseña de la Jornada sobre Riesgos Penales de la Banca *On-line*» [reseña en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 2. UOC. [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/2/dt/esp/fernandez.pdf>
ISSN 1699-8154

Rosa Fernández Palma
mfernandezpa@uoc.edu

Licenciada en Derecho (Universidad Complutense de Madrid). Doctora en Derecho (Universidad Autónoma de Barcelona).

Ha sido becaria del Plan de formación de personal investigador de la Comunidad de Madrid y profesora de Derecho penal en la UCM, UAB. Actualmente, es profesora de Derecho penal de la UOC y coordina el Seminario de doctorado *Internet, Dret i Política* del Programa de doctorado de la UOC.

Es autora de publicaciones relacionadas con delitos contra el honor y la intimidad.

En la actualidad el ámbito de interés de su investigación se centra en la delincuencia relacionada con las tecnologías de la información y la comunicación, habiendo participado en proyectos de investigación sobre la materia, másteres, cursos de doctorado y jornadas, así como en diversas publicaciones sobre este ámbito.

Magistrada suplente en la Audiencia Provincial de Barcelona.

UOC
www.uoc.edu