Phising, una visión tecno del fallo -Comentario a Fallo-(*)

Por Raúl Alejandro Farías (**)

Normalmente los abogados tratamos de hacer un análisis jurídico de los fallos que nos interesan. Para los que nos especializamos en Derecho de Alta Tecnología es igualmente importante analizar lo que ocurre con las tecnologías implicadas en estos casos. Ello nos permitirá evaluar adecuadamente los perjuicios ocasionados, elegir las vías de reclamo, delimitar el alcance y conveniencia de las normas a invocar y proyectarnos sobre los demás delitos involucrados que, por la propia forma en que se despliegan las tecnologías aplicadas, pueden afectar otros actores y bienes en juego fuera del principal. En tal sentido se advierte fácilmente que no solo el damnificado (ERR) es sujeto pasivo de este delito, sino que también lo es el banco al haberse clonado sus páginas y afectando así una variedad de derechos que van desde la imagen a las marcas con su consiguiente perjuicio económico.-

¿Qué deja este fallo?

Como primera medida, conviene aclarar los detalles fácticos relevantes que de él surgen:

El engaño

Una ventana que contiene un formulario pidiendo los números de tarjeta de debito y código de transferencia del damnificado, con la vana promesa de obtener "mejor atención y seguridad en la operación" se despliega en forma paralela a la que contiene el sitio web legítimo de banca on-line que consulta la víctima.-

El error

Como consecuencia directa del engaño y teniendo aquel formulario la misma apariencia que el sitio legítimo y habiéndose abierto en el mismo instante de la consulta on-line, cree que efectivamente pertenece al banco e introduce la información requerida.-

La disposición patrimonial

Al día siguiente el damnificado descubre faltantes de dinero tanto en su caja de ahorros como en su cuenta corriente. Sin perjuicio de señalar que el damnificado no dispuso por sí de sus fondos inducido por el engaño sino que directamente se ha realizado una sustracción del dinero con destino a otra cuenta, como si alguien se hiciera de la llave de una casa para entrar contra la voluntad de su dueño y sustraer bienes, este perjuicio no deja de ser una consecuencia directa de los dos pasos previos.-

Formulado el reclamo ante el banco, se hace de las constancias que acreditan que los montos faltantes de sus cuentas se transfirieron a la caja de ahorros de uno de los imputados.-

Ambos imputados (RMGG y MJR) afirman que esos montos proviene de la venta que el titular de la cuenta destino (RMGG) hizo a un tercero (MB) del que no aportan datos. Tampoco acreditan la operación que, según dicen, realizaron mediante una página de Facebook. Los montos transferidos, por excesivos, no guardan verosimilitud con el objeto de la pretendida venta (camiseta de fútbol).-

Todas las transferencias se realizan entre cuentas del mismo banco de personas que no se conocían.-

Respondiendo entonces a la pregunta inicial, se advierte en primer lugar que el phishing es una técnica delictiva informática que está efectivamente entre nosotros. Pasó de ser algo que reconocía la mayor cantidad de registros[1] en USA para cohabitar con los delitos locales.-

A fin de conocer que elementos tenemos que evaluar los abogados para encausar correctamente un caso similar, es necesario saber en qué consiste el Phishing.-

¿Qué es el phishing?

Se lo ha definido como la práctica de engañar a una víctima para que revele contraseñas u otros datos personales que permiten que el ladrón pueda acceder o modificar las sus cuentas existentes.2[2]

En mi visión, se trata de una forma de estafa que mediante engaños en base a técnicas de ingeniería social, intenta obtener ilícitamente los datos de acceso a cuentas de todo tipo, desde las de correo hasta una cuenta de banca on-line como en el caso comentado.-

Los métodos de phisihng han ido evolucionando en la medida que la gente se ha informado de su existencia.-

En un primer momento se enviaban e-mail a las posibles víctimas pidiéndoles que respondieran incluyendo nombres de usuario y contraseña de cuentas.-

El destinatario simulaba ser oficial de cuentas del banco de la posible víctima incluyendo parte del nombre de la institución en el dominio del e-mail.-

Las excusas generalmente eran del tipo *"estamos haciendo mantenimiento de las cuentas", o "actualizando nuestro sistema de seguridad y si no contamos con estos datos no podrá volver acceder a la suya".* Los textos eran planos sin más aditamentos.-

Luego evolucionaron dando mayor verosimilitud al engaño con imágenes propias de las instituciones bancarias insertas en el cuerpo del email y pidiendo esos mismos datos con excusas similares. Para ingresar los datos daban una dirección web que *linkeaba* con un formulario para llenar.-

Un paso más adelante, las propias imágenes comerciales de los bancos estaban vinculadas a estos sitios falsos. Esto se advertía al deslizar el puntero del mouse por encima de ellas y ver en la barra de estado, al pie del mensaje, la verdadera dirección que, por cierto, nada tenía que ver con la institución bancaria que decía ser.-

Por su parte, los formularios a los que se vinculaba eran exactamente iguales a los de los bancos, con la salvedad que la dirección web era levemente distinta dado que, claro está, vinculaba a otro servidor. Incluso se han usado servidores seguros y código JavaScript para enmascarar la dirección falsa con una imagen superpuesta de la legítima en la barra de direcciones del navegador a fin de hacer creer a las víctimas que se encuentran en el sitio correcto. El desarrollo de aplicaciones específicas, ha profesionalizado el engaño.-

El ultimo grito de esta "moda" consiste en la creación de páginas paralelas que mediante la técnica conocida como *cross site scripting* confunden a los usuarios que entran normalmente en una página original de banca on-line al requerirles mediante un mensaje en pop-up que realicen la verificación de usuario y contraseña momento en que se los redirige a una página clonada donde se consuma la apropiación de los datos o, como en fallo comentado, directamente induce a dejar esos datos en la página paralela, sin redirigir hacia otras; algo mucho más dañino.-

Otro factor directamente relacionado con el phishing, aunque no necesario, es la existencia de "mulas" que hacen el lavado del dinero obtenido de cuentas a las que se accedió mediante estas técnicas. Los "mulos" son por lo general incautos que aceptan realizar un trabajo, por ejemplo enviando e-mail de publicidad. Su salario consiste en un porcentaje del dinero que recibió en transferencia desde la cuenta víctima y que supuestamente, para ellos, proviene de los beneficios logrados con su trabajo. Hecha la retención que le corresponde, transfiere el grueso de la suma a otra cuenta, la del verdadero *phisher*.-

Como quiera que sea y conociendo la forma en que funciona, siempre tendremos que fijarnos en la vinculación que existe entre la cuenta víctima y del supuesto victimario. Es importante ver montos, fechas y horas de las operaciones. Eventualmente si hubiera "mulas" en el circuito de esta estafa, se deberán investigar las transferencias hechas desde la cuenta del presunto victimario a cuentas de terceros. Su historial, periodicidad y porcentajes constantes serán datos relevantes.-

Protección contra el phishing.-

Como dije más arriba estas técnicas delictivas evolucionan junto con los remedios que ponen los bancos basados principalmente en la difusión de este tipo de amenazas y apelando al conocimiento como principal anticuerpo lo cual, sin dudas, no es poco. No obstante ello, los casos se repiten como en el comentado ya que aunque sean pocos, siempre resultarán rentable para los estafadores.-

Por lo pronto, existen técnicas más robustas de protección de datos sensibles y consecuentemente de las cuentas bancarias, tal el caso de la firma digital. Pero parece ser que puestos a evaluar costos-beneficios, a las instituciones bancarias les sigue saliendo más barato cubrir los eventuales perjuicios de sus clientes producidos por estas estafas antes que instrumentar medidas de protección serias.-

El punto fuerte del phishing es que se basa en la llamada ingeniería social[3], donde el humano es la variable débil directamente enfocada porque es ahí donde el delincuente encuentra una puerta de acceso, ya sea por descuido de la persona, buena fe o desconocimiento de factores informáticos básicos e incluso por haber pasado a formar parte del paisaje todas las advertencias precedentes.-

Han venido en auxilio de esta debilidad los llamados *sitemas multifactor de seguridad* que básicamente constituyen una barrera de seguridad compuesta por tres aspectos principales a) uno memorizado por el individuo, como lo es una contraseña; b) otro basado en biometría, por ejemplo mediante la lectura de huellas dactilares, c) y un tercero material, normalmente desempeñado por un Token[4] o llave usb.-

Qué sé (clave), *que* soy (biometría), *que tengo* (Token) resume el concepto de *sitemas multifactor de seguridad* que es capaz de brinda un nivel de protección sobresaliente.-

Actualmente los bancos utilizan un doble nivel de protección basado en las variables a) y b) referidas es decir, sé una clave y tengo una tarjeta de coordenadas.-

Aun así existen casos de phishing registrados en España, en los que se han obtenido los números de estas tarjetas de coordenadas, tal los sufridos en 2005 por clientes de Bankinter, el 6º mayor banco Español, donde se les pedía que introdujeran en un formulario web los números de las tarjetas de coordenadas, o los padecidos por clientes de La Caxia (Caixa d'Estalvis i Pensions de Barcelona) a quienes se les pedía que enviaran por fax copia de la tarjeta.-

Según se desprende del Report 42 Spam & Phishing[5] del mes de junio de 2010, elaborado por la empresa Symantec, si bien USA tiene el record en la detección de señuelos phising con el 56% del total mundial, nuestro vecino Brasil empata en el 2% con países como Rusia y China, siendo los objetivos principales el sector financiero, con el 86% de los ataques seguido del sector de servicios de información con el 14%.-

Como lo señalé más arriba el phishing se ha acercado y ya está entre nosotros. El hecho que aun no figuremos o que pudiéramos representar bajos valores estadísticos, no debe hacernos bajar la guardia dado que las estadísticas provienen de millones de casos y, llevadas a los hechos en relación a nuestra población conectada, pude representar una alta probabilidad de sufrir uno de estos fraudes. El fallo comentado es un claro ejemplo de ello.-

---

(*) Causa Nro.39.779 - "G. R. y otro s/ procesamientos" – CNCRIM Y CORREC - SALA VI 03/08/2010 (elDial.com - AA2EC)

(**)Abogado. Cursando la Carrera de posgrado de Derecho de Alta Tecnología, Pontificia Universidad Católica Argentina (finalización, diciembre de 2011). Especializado en temas de informática jurídica, seguridad informática y Tecnologías de la Información y de la Comunicación (TICs). Desde el año 2008 a la actualidad es Director Académico del PEA Programa de Entrenamiento para Abogados de FORES, Foro de Estudios para la Administración de Justicia. Director IT del PEA, profesor y responsable del área de TICs Tecnologías del la Información y la Comunicación. Coordinador del equipo de derecho laboral del PEA y de los alumnos en su intervención en la columna "Consultorio Laboral" del Diario La Nación. Representante del PEA en gran cantidad de eventos académicos.

[1] *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised,*
please click the link below and confirm your identity."
"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
How Not to Get Hooked by a 'Phishing' Scam. Federal Trade Commission Bureau of Consumer Protection Offi ce of Consumer & Business Education (2006)

[2] "*the practice of tricking a victim into revealing passwords or other personal data that allow the thief to access or alter the victim's existing accounts*" Harvard Journal of Law & Technology - Volume 21, Number 1 Fall 2007 - IDENTITY THEFT: MAKING THE KNOWN UNKNOWNS KNOWN - Chris Jay Hoofnagle*

[3] Social engineering / Definitions: "the art and science of getting people to comply to your wishes", "an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system" (Palumbo), or "getting needed information (for example, a password) from a person rather than breaking into a system" (Berg). In reality, social engineering can be any and all of these things, depending upon where you sit. The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system. http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

[4] En sistemas de seguridad, pequeño dispositivo del tamaño de una tarjeta de crédito que muestra un código de ID que constantemente cambia. Primero un usuario ingresa una clave y luego la tarjeta muestra un ID que puede ser usado para ingresar a una red. Generalmente las IDs cambian cada 5 minutos. Un mecanismo similar para generar IDs es una smart card. http://www.alegsa.com.ar/Dic/token.php

[5] State of Spam & Phishing - A monthly report - (2010) Symantec.
http://www.symantec.com/content/en/us/enterprise/other_resources/b-state_of_spam_and_phishing_report_06-2010.en-us.pdf

Citar: **[elDial.com - DC147D]**

Publicado el 13/10/2010