“El Phising, Pharming y Spoofing”

Presentado por:

Kriss A. Ríos Quintero

Eduardo Lagarón Martín

14 de Febrero de 2011

I. SUPUESTO TEÓRICO Y TÍPICO DE "PHISING".

Juan recibe un email de un banco denominado bancosantanderes, el cual le aparece como remitente. Resulta que Juan, posee una cuenta corriente con un nombre muy parecido, y a su parecer dicha referencia tan sólo le hace indicar que es el banco que le escribió el email, es el conjunto de sus sedes bancarias. Dicha página web le informa de lo siguiente:

> *"Posiblemente Usted notó que la semana pasada nuestro sitio www.bancosantanderes.es funcionaba inestable y se observaban frecuentes intermitencias.*
> *Hemos renovado nuestras instalaciones bancarias y ahora el problema está resuelto.*
> *Pero para activar un sistema nuevo de protección de los datos y una capacidad de trabajo correcta de sus cuentas bancarias, le pedimos a usted introducir los detalles completos de la cuenta para que podamos renovar nuestra base de los clientes y comprobar la capacidad de trabajo de nuestro nuevo sistema de protección de los datos.*
> *Si Usted no active su cuenta bancaria durante 5 días, las posibilidades complementarias de la defensa de seguridad no serán establecidas en su cuenta.*
> *Si Usted tiene una cuenta bancaria personal, pase a la referencia: https://www.bancosantanderes.es/particulares/*
> *htttps://www.bancosantanderes.es/empresas/*
> *Esta carta es enviada automáticamente a todos los clientes de nuestro banco, no hay necesidad de contestar a ella."*

Juan, al ver que su periodo de actuación para resolver el problema es de 5 días, se dispone a realizar con celeridad lo dispuesto en el email, sin percatarse de lo sospechoso del email (incluso dicho email, puede tener errores gramaticales).

Al cabo de 3 días, Juan va a retirar dinero, y el banco le informa de que su cuenta se encuentra al descubierto. ¿Qué ha ocurrido? ¿Donde está su dinero? ¿Ha sido víctima de un fraude? La contestación a dicha preguntas es un nuevo delito informático de estafa denominado "phising".

II. ¿QUÉ ES EL "PHISING", "PHARMING" Y EL "SPOOFING"?

Se trata de un delito informático consistente en enviar de modo masivo correos electrónicos, a miles de potenciales víctimas. Aquellos que se caracterizan porque su contenido, su aspecto, su diseño y su logo, crean la apariencia de estar realmente remitidos por una entidad bancaria, y si el destinatario del correo pertenece a la entidad bancaria, y es lo suficientemente ingenuo, accederá a remitir lo solicitado en el e-mail, aportando las claves de acceso a la cuenta bancaria.

Los medios utilizados pueden ser muy diversos. Desde que se le informa al titular de la cuenta de que su datos personales están bloqueados junto con su cuenta de acceso, o bien, que la contraseña aportada para entrar en su cuenta corriente está a punto de expirar. Ante dicha situación el internauta ingenuo, accede a aportar sus datos de carácter personal a la página web de la entidad ficticia. No sólo existe esta técnica de "phising". Este delito informático también puede llevarse a cabo a través de programas informáticos instalados en la víctima. En este caso, la víctima es informada de que se necesita instalar una herramienta de Internet en su ordenador con el fin de que pueda utilizar herramientas informáticas (normalmente, se le informa de que tanto como la herramienta que se instala en su ordenador como la herramienta informática son gratuitas, y así

poder defraudar a la víctima) y posteriormente instalar en el ordenador de la víctima un troyano o un "keyloger". Este último, es un tipo de software que se encarga de registrar las pulsaciones que se realizan en el teclado, para memorizarlas en un fichero y/o enviarlas a través de Internet, es decir, se trata de un programa que graba todos los datos introducidos a través de Internet, con el fin en este caso, de que el timador pueda observar a que cuentas accede, el nombre de los bancos a los que accede y que contraseñas utiliza.

Una variación del "phising" que se ha venido practicando en los últimos años es el "pharming". Dicho delito es algo más complicado, y más difícil de identificar. El "pharming" básicamente consiste en reemplazar una página web por una clonada, con el fin de obtener los datos que el usuario ingrese en ella.

Por último el "spoofing", consiste básicamente en sustituir la dirección IP origen de un paquete por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UPD o TCP. En definitiva, se trata de una suplantación de identidad del protocolo TCP/IP. En este caso es el denominado "IP spoofing".

III. Protección penal para el "phising" en el Derecho Comparado.

Este delito informático es actualmente, uno de los delitos más utilizados en Internet. Por ese motivo, y ante la alarma social creada por este tipo de delitos, numerosos países han introducido leyes realmente duras en algunos países con el fin de frenar dicha alarma social, ya que esta estaba generando en los ciudadanos una gran desconfianza a la hora de usar sus datos de carácter personal en Internet, y no sólo eso, sino que dichos datos implicaban grandes cantidades de dinero. Ante esta situación, los Gobiernos al ver que esta conducta hostil de los ciudadanos ante esta nueva utilidad de Internet, que podría potenciar el desarrollo tecnológico y económico, han reaccionado con duras penas para este tipo de delitos.

En los Estados Unidos, se introdujo el *Acta Anti-Phishing de 2005,* el 1 de Marzo de 2005. Esta ley federal de anti-phising establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de e-mail con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 y penas de cárcel por un término de hasta cinco años.

En Marzo del 2005, también se consideró la asociación entre Microsoft y el gobierno de Australia para educar sobre mejoras a la ley que permitirían combatir varios crímenes cibernéticos, incluyendo el "phishing".

En Gran Bretaña, debido a un caso de "hacking" en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización.

IV. Protección Penal para el "phising" en nuestro Código Penal.

En nuestro ámbito penal, dada la seguridad jurídica de nuestro ordenamiento jurídico en detrimento de la flexibilidad jurídica, hemos de adaptar aquellos tipos penales antiguos a tipos penales nuevos derivados de una nueva generación de delitos informáticos. Por ella la doctrina familiarizada con este tipo de delitos es muy dispar, pues algunos autores ven imposible "encuadrar" en los tipos penales antiguos, los nuevos delitos informáticos, y en este caso, el "phising".

Si bien dependiendo del supuesto de "phising" concreto, podemos abarcar tipos penales distintos. Abarcando en algunos supuestos, mayor número de delitos, y en otros un menor número. En el presente trabajo se pretende analizar aquellos que resulten más típicos en el tipo penal, pero sin descartar otros, que puedan aparecer en supuestos concretos. Generalmente se da cuando el estafador infecta nuestra computadora con un troyano, el cual manipula las direcciones DNS (Domain Name Server) de las páginas web que solemos visitar, de tal modo que cuando ingresemos, por ejemplo, a la página web de nuestro Banco seamos redirigidos a una página clonada de éste. Por lo tanto, ya se trata no sólo de un tipo avanzado de "phising" (en el que se incluye un troyano simple o un "keyloger"), sino que dicho troyano, aún más peligroso, cambia los parámetros básicos de acceso a Internet del usuario.

Artículo 248, 249 y 250 del Código Penal: Delito de estafa

En realidad, dicha norma no regula expresamente el delito de "phising", pero actualmente, los Tribunales vienen considerando el delito de "phising" como un delito de estafa. El artículo 248, su apartado 1 y su apartado 2, señala claramente la estafa mediante delitos informáticos (Art.248.2 a) y también señala el fraude por tarjetas de crédito (Art.248.2 c).

La combinación de ambos apartados, parece no dar lugar a dudas de que el delito de "phising" corresponde a este tipo penal. En cuanto a la atenuante de devolución del importe estafado al cliente, el Tribunal Supremo se ha pronunciado al respecto señalando que se deben estimar los mismos elementos que una estafa tradicional. Así una vez más se enmarca el "phising" y la existencia de sus particularidades, en un delito de estafa tradicional, lo que puede generar en algún caso concreto, ciertas incompatibilidades.

Artículo 401: Usurpación del Estado Civil: Suplantación de identidad.

Dicho delito no sólo se comete en el caso de delitos de "phising", sino que también se comete en redes sociales y "blogs". Por ello, la doctrina ha puntualizado que la suplantación de identidad sólo se da cuando la conducta consiste en una "verdadera" suplantación de identidad, que no se limite al nombre y apellidos, sino a todas las características o datos que integran la identidad de una persona.

Ante esta situación, cabría preguntarse qué datos, y qué combinación de estos integra la identidad de la persona, en cuyo caso, habría que analizar el caso concreto. Parte de la doctrina opina que la suplantación de identidad en Internet sólo se comete cuando existe una suplantación de la firma electrónica. En nuestra opinión, es claro que en el caso del "phising", para cometer el delito hace falta más que los nombres y apellidos de la persona, sino que también hace falta su número de cuenta, contraseña, y en algunos casos DNI; para poder cometer el delito; y la suplantación de identidad estará compuesta por aquellos elementos que resulten mínimos para realizar una transacción dineraria, según la herramienta que utilice la entidad bancaria para dichas transacciones.

Aún así la suplantación de identidad en el "phising", es algo complicado de valorar, pues esta puede darse en la víctima o en la entidad bancaria; y como se indicó anteriormente, habrá que ir al caso concreto.

Artículo 197 y siguientes: Revelación de secretos.

El mencionado delito suele ser en estos casos de delitos informáticos, consecuencia del delito anterior. En el ámbito del "phising" es menos frecuente que en otros ámbitos como es el

acceso a cuentas de correo electrónico o redes sociales, pues en estos últimos casos puede cometerse un delito a la intimidad.

En el caso del "phising", este puede cometerse si los datos bancarios referentes a la cuenta accedida mediante fraude, puedan ser obtenidos por cualquier persona (existe mucha jurisprudencia y doctrina, en cuanto donde está el límite de lo que se considera una revelación y lo que no). Si bien la revelación de secretos apenas se da en delitos como el "phising", cierta información personal en casos muy concretos, si se difunde puede haber un delito de revelación de secretos.

V. Análisis de la jurisprudencia en delitos de "phising".

5.1. Sentencia núm. 242/2008 de 23 julio por la Audiencia Provincial de Burgos: Responsabilidad de la Entidad Bancaria

Supuesto de hecho: Inexistencia de responsabilidad bancaria por operaciones fraudulentas mediante banca "online". El cliente facilitó sus claves a terceros al recibir un correo electrónico con un enlace falso. Se realizaron las advertencias oportunas por el Banco y diligencia en la anulación de transferencias posteriores al aviso del actor.

Comentario: En este caso no se pretende sólo actuar contra el autor material del delito de "phising", sino que el demandante pretende imputar una responsabilidad subsidiaria civil derivada de un delito penal a la entidad bancaria por no adoptar las medidas necesarias derivadas de un delito de "phising". El demandante alega que el software utilizado por la banca "online" de la entidad bancaria no cumplía las medidas de seguridad necesarias, y ha de ser responsable civilmente por ello, ya que es la entidad bancaria la obtiene grandes beneficios en el uso de la "banca online". En nuestra opinión, existen beneficios tanto económicos como organizativos por parte de la entidad bancaria, pero por otro lado, el cliente también ser beneficia de los servicios en cuanto existe una mayor flexibilidad y celeridad en el acceso a sus cuentas y la gestión de las mismas. Por lo tanto, habrá que considerar una vez más el deber de diligencia por la entidad bancaria para garantizar las medidas de seguridad informáticas con el fin de evitar el "phising". Dadas las pruebas aportadas en el proceso, creemos que el deber de diligencia fue óptimo, distinto es la responsabilidad que se le pueda atribuir al banco por aceptar transferencias (y en este caso, electrónicas) por encima del límite establecido por el cliente, pero en este caso, se trata otras medidas de seguridad, distintas de prevenir el hecho delictivo concreto del phising (mandar emails suplantando a la entidad bancaria, o elaborar páginas web clonadas).

5.2. Sentencia núm.556/2009 de 16 de marzo por el Tribunal Supremo (Sala de lo Penal, Sección 1ª): "Phising" y "Spoofing" en un mismo delito.

Supuesto de hecho: Existencia de un grupo organizado que emplea la red informática para la captación de datos confidenciales de titulares de las cuentas on-line y efectuar transferencias mediante el empleo de las claves suministradas por el titular., en este caso, abusando de la firma de otro, o sustrayendo, ocultando o inutilizando algún proceso.

Comentario: Dicha sentencia tiene mayor dificultad por su contenido técnico, como por su contenido jurídico-penal.

En cuanto al primer apartado, se trata de un delito en el cual unos estafadores mandan de

manera masiva correos electrónicos con virus troyano incluido "phising", que contienen un enlace o URL, que direcciona directamente con una página web clonada "spoofing". Dicha website ha sido creada por los propios estafadores. De este modo se aseguran en mayor medida la consecución del delito, ya que por un lado incluyen un troyano con "keyloger", con lo que pueden obtener los datos personales de acceso y contraseña, los cuales volverán a ser incluidos en la website clonada junto con mayores datos personales.

En cuanto la cuestión jurídico-penal, se plantea la punibilidad del delito por existencia o no de culpabilidad (además de vulnerar la presunción de inocencia y la tutela judicial efectiva de uno de los demandados). En este supuesto de hecho, el "phising" es más complejo ya que los estafadores utilizan a una persona como mediadora para cometer sus delitos, con o sin desconocimiento de esta, de la comisión del delito (y es aquí lo que se cuestiona del caso). En este caso, los estafadores celebran un contrato de servicio por el cual, una parte contratante cede sus datos bancarios a los estafadores para posteriores ingreso por parte de la víctima para que posteriormente esa parte contratante envíe esa cantidad de dinero a otra cuenta menos el 7% de comisión que obtiene la parte contratante, como contra-prestación al servicio, evidentemente los ingresos por parte de la víctima a ese contratante son con desconocimiento (o no) de la existencia de un delito de estafa.

En nuestra opinión, la valoración de la coautoría del delito depende de las circunstancias concretas de cada caso, y el conocimiento legal y técnico de los intervinientes. Como bien indica el tribunal *"la adecuación del engaño ha de medirse por el conjunto de las circunstancias del caso singular, comprendiendo tanto la atención a módulos objetivos como a las condiciones personales de los intervinientes"*.

Pero en todo caso, creemos que en ningún caso puede considerarse cooperadora necesaria del delito, pues no forma parte fundamental del delito cometido, es decir, el contrato celebrado por los estafadores con la contratante no existe en base a sus circunstancias o cualidades personales, ya que estas eran perfectamente sustituibles por los de otra persona, su cuenta bancaria no se diferencia de ninguna otra. En la misma línea, aunque con argumentos algo diferenciados lo indica el recurso al señalar que: *"Ángeles no puede ser considerada autora o inductora, ya que quien ideó, puso en marcha y ejecutó el plan criminal fue un tercero, y tampoco cooperadora necesaria, pues no participó en el mecanismo por el que se consiguieron las claves de acceso bancarias de Fátima o en la orden de transferencia desde la cuenta de aquélla"*. Respecto a las alegaciones, no estamos del todo de acuerdo, ya que la cooperación necesaria ha de evaluarse no únicamente en el mecanismo para la consecución de los datos personales, sino como bien indica anteriormente, en el plan criminal en su conjunto.

VI. Bibliografía y Anexo.

1) Http://www.proteccionlegal.com/delitos-en-la-red/articulos/158-delitos-informaticos-phishing.html.

2) Http://www.scribd.com/doc/18670332/COMENTARIOS-A-SOBRE-LA-EXPANSION-DEL-DERECHO-PENAL-Y-SU-VINCULACION-CON-LA-FIGURA-DEL-PHISHING.

3) Http://falsaspaginasweb.blogspot.com/

4) Http://www.recoverylabs.com/informes/Recovery_Labs_pharming.pdf