30/10/2015 11:56:16 | España - Estafa informática

Estafa informática. El denominado phishing y la conducta del “mulero bancario”: categorización y doctrina de la Sala Segunda del Tribunal Supremo

María Victoria Rodríguez Caro.
Licenciada en Derecho y en Criminología. Máster en Sistema penal, Criminalidad y Políticas de Seguridad. Abogada. Fiscal Sustituta

Todo comienza, por lo general, cuando un usuario de la banca on line recibe un correo que supuestamente procede de su banco, que tiene la finalidad de inducir al cliente para que clique en un enlace que le redirige a una web maliciosa mediante la que se suplanta la identidad del banco para obtener las claves de acceso del usuario engañado, sus datos bancarios, etc.

Los consejos para evitar ser una víctima de este tipo de fraudes son: 1. Cierre todas las aplicaciones antes de acceder a la web del banco. 2. Escriba directamente la url en el navegador, en lugar de llegar a la misma mediante enlaces disponibles en páginas de terceros o en correos electrónicos. 3. Asegúrese que la web comienza por https://, para que los datos circulen por la red cifrados. 4. Compruebe la legitimidad del sitio web empleando el navegador. 5. No acceda a los servicios de banca online desde ordenadores públicos, no confiables o que estén conectados a redes wifi públicas.

Normativa comentada

– Arts. 248 y 301 del Código Penal

I. Qué es el phishing

El término phishing proviene de la unión de los siguientes vocablos en inglés password, harvesting y fishing, con lo que se viene a hacer alusión a “cosecha y pesca de contraseñas”. A la persona que pone en práctica este delito se le conoce como phisher.

El origen de este delito data de la década de los noventa, y su operativa se centraba en el envío masivo de correos electrónicos fraudulentos a los clientes de entidades financieras (conocido como smishing, o incluso a través de llamadas telefónicas, el denominado vishing), con la finalidad de obtener de éstos los datos y las claves de usuario que les permitirán acceder fraudulentamente a la cuenta de la víctima. Al principio los mensajes consistían en una burda traducción al español, incluso estaban mal redactados o adolecían de errores ortográficos, pero en la actualidad la técnica se ha ido perfeccionando dotando al mensaje de mayor credibilidad aumentando así las posibilidades de éxito. Incluso la técnica del phishing ha evolucionado migrando hacia otras formas de comunicación online como, en particular, las redes sociales, mediante la colocación de posts en Facebook o Twitter, entre otros, con promociones y beneficios para cuyo disfrute se requiere el ingreso, también en este caso, de información personal y bancaria en las correspondientes webs clonadas.

Otra de las modalidades posibles de obtención de datos y contraseñas del usuario es el caso de phishing a través de malware (acrónimo de "malicious software"), es decir, la implantación de programas denominados maliciosos (entre los cuales, troyanos, virus, gusanos, etc.) en el sistema informático desde el que la víctima maneja sus cuentas bancarias.

Pero el método más usual de consecución de las claves de la cuenta bancaria en la práctica judicial es el denominado pharming (simulación de entidad bancaria). Los defraudadores simulan o copian una página web de un banco y en los correos anzuelo incluyen una URL en la que el cliente destinatario víctima ha de pinchar, teóricamente para acceder a la página de su banco pero que, en realidad les dirige a la página web simulada donde el destinatario introducirá sus datos de usuario y contraseñas, valiéndose de una excúsalo más verosímil posible (actualización del sistema, verificación de datos, etc.). Más modernamente, con el fin de evitar que quede al descubierto su verdadera URL y el usuario pueda percatarse del engaño, en lugar de contener un enlace en el correo remitido por la supuesta entidad bancaria, lo que se envía en el correo es un archivo adjunto HTML que el destinatario tiene que descargarse. El usuario bancario descarga y abre el archivo que consiste en un formulario de recogida de datos, el cual lo cumplimenta, proporcionándoselos al defraudador, dejando su cuenta expedita para que éste pueda operar libremente.

La averiguación de la titularidad del correo electrónico del remitente o de la página web fraudulenta no siempre es posible, lo que dificulta el descubrimiento de la identidad del phisher.

Una vez que el cliente ha picado y el phisher dispone de las claves de acceso, que han quedado registradas en la falsa página web, se introduce en el verdadero sistema informático de la entidad bancaria y está en disposición de retirar dinero de la cuenta bancaria de la víctima de manera fraudulenta e inconsentida.

Ahora bien, antes de efectuarlo es preciso que el defraudador cuente con una cuenta corriente bancaria de destino de la suma que se va a detraer ilícitamente y, lógicamente, ha de ser una cuenta que no levante sospechas (como sería el caso de una cuenta extranjera), que no provoque la alerta de la entidad bancaria y, además y fundamental, que pertenezca a un tercero, para proporcionar la impunidad al defraudador. Es aquí donde intervienen los conocidos en el argot policial como “muleros bancarios”, por analogía con lo que sucede en los delitos de tráfico de drogas.

Por tanto, es preciso desplegar la actividad conducente a encontrar a las personas que pongan a disposición del defraudador una cuenta bancaria para transferir a la misma el dinero que se va a detraer ilícitamente. El mulero bancario, proporciona, por tanto una aportación imprescindible para que el fraude pueda consumarse. En adelante se analizará la conducta del mulero, considerando si es una víctima del engaño o, al contrario, coopera de forma no tan “inocente” en el fraude.

En la captación de estos “colaboradores” se ha generalizado igualmente el método de envío de correo electrónico conteniendo una oferta de trabajo con generosas remuneraciones, por lo que la época de crisis ha contribuido al éxito de la misión. El trabajo consiste en efectuar labores de “auxiliar” o “intermediario financiero” de una empresa, generalmente internacional y que no exige grandes esfuerzos, proporcionando, en cambio, unos ingresos fijos o a modo de comisión. La excusa para el empleo de este inhabitual cauce se sitúa en razones fiscales. Si el destinatario “pica” y se interesa por esa oferta de empleo, le solicitan que envié sus datos y que suscriba un contrato. Entre otros datos intrascendentes para el defraudador (como número de la Seguridad Social) se encuentran el teléfono y, naturalmente, los datos de una cuenta bancaria donde le será ingresado el supuesto sueldo o la comisión por la prestación del servicio. En lugar de ello, el “mulero” lo que recibe en su cuenta bancaria es la transferencia que procede supuestamente de la víctima del phishing y su labor consiste en hacer llegar

el importe de la misma al defraudador, generalmente quedándose con un porcentaje de la cantidad transferida a su cuenta, en concepto de comisión por la gestión realizada; el grueso del dinero generalmente se envía al extranjero a favor de una persona desconocida cuyos datos se le han facilitado al “mulero”, a través de sistemas de envío postal como Western Union o MoneyGram, los más usados dado que estas empresas operan con códigos alfanuméricos que dificultan el rastreo del dinero.

Una vez que el “mulero” lleva a cabo el envío, el fraude queda consumado.

II. Regulación de los fraudes informáticos en el Código Penal español

La Decisión Marco del Consejo de Ministros de la Unión Europea sobre “la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo”, de fecha 28 de mayo de 2001, dispone en su art. 3º que “Cada estado miembro adoptará las medidas necesarias para garantizar que las siguientes conductas sean delitos penales cuando se produzcan de forma deliberada: realización o provocación de una transferencia de dinero o de valor monetario (...) mediante: la introducción, alteración, borrado o supresión indebidas de datos informáticos especialmente datos de identidad, y la interferencia indebida en el funcionamiento de un programa o sistema informáticos.”

El art. 248 del Código Penal en su regulación actual tras la reforma introducida por la LO 5/2010, de 22 de junio, dispone lo siguiente:

"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro."

El ámbito de aplicación del tipo es tan amplio como para englobar los desplazamientos patrimoniales inconsentidos que se producen por medios informáticos. En palabras del Tribunal Supremo: “Cuando la conducta que desapodera a otro de forma no consentida de su patrimonio se realiza mediante manipulaciones del sistema informático, bien del equipo, bien del programa, se incurre en la tipicidad del art. 248.2. También cuando se emplea un artificio semejante. Una de las acepciones del término artificio hace que este signifique artimaña, doblez, enredo o truco. El artificio es equivalente, a los efectos del contenido de la ilicitud, cuando el autor modifique materialmente el programa informático indebidamente o cuando lo utilice sin la debida autorización o en forma contraria al deber.” (STS 860/08, 17-12).

Las diferencias entre el tipo de la estafa informática y la clásica que recoge el art. 248.1 CP son evidentes, pues afectan a elementos tan característicos de este delito como son el engaño y el error que generan el acto de disposición en perjuicio de la propia víctima o de un tercero, en cambio subsisten los elementos subjetivos del dolo y el ánimo de lucro.

– En cuanto al engaño, es de destacar que la nueva figura pretende proteger el patrimonio de los ataques que propician las nuevas tecnologías, que se describen por el legislador como "manipulación informática o artificio semejante", incluyendo todos aquellos mecanismos que sean idóneos para

conseguir esa transferencia inconsentida de un activo patrimonial, que integra el acto de disposición y que provoca el enriquecimiento que el autor persigue. A diferencia de lo que ocurre respecto a la estafa prevista en el nº 1 del art. 248 del CP, el engaño ya no es un elemento básico ni su presencia es imprescindible, dado que la función que allí desempeñaba el uso de engaño, aquí es el recurso a la manipulación informática o un artificio fraudulento semejante, que son los que dan lugar al desplazamiento patrimonial que no ha consentido su titular. Dice la STS 533/2007, de 12 de junio, que “no es precisa la concurrencia de engaño alguno por el estafador, porque el acecho a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal.”

– Respecto al error, es de destacar que aquí ni siquiera se produce una relación intersubjetiva, ni es requisito imprescindible esa “colaboración” de la víctima del fraude informático, porque el desplazamiento patrimonial se produce, en realidad, por virtud de la manipulación informática. La acción no se dirige contra un sujeto que pueda ser inducido a error sino que se ejerce directamente al programa informático que actúa, sin error, según la información que le es suministrada. La STS 1476/2004, de 21 de diciembre ya destacaba: “En efecto, los aparatos electrónicos no tienen errores como los exigidos por el tipo tradicional de la estafa, es decir, en el sentido de una representación falsa de la realidad. El aparato se comporta según el programa que lo gobierna y, en principio, sin 'error'”. Y la STS 369/2007, de 9 de mayo pone de manifiesto que el tipo de la estafa informática admite diversas modalidades comisivas, “bien mediante la creación de órdenes de pago o de transferencias, bien a través de manipulaciones de entrada o salida de datos, en virtud de los que la máquina actúa en su función mecánica propia.”

En definitiva, “como en la estafa clásica, debe existir un ánimo de lucro; debe existir la manipulación informática o artificio semejante que es la modalidad comisiva mediante la que torticeramente se hace que la máquina actúe; y también un acto de disposición económica en perjuicio de tercero que se concreta en una transferencia no consentida. Subsiste la defraudación, y el engaño, que es propio de la relación personal, es sustituido como medio comisivo defraudatorio por la manipulación informática o artificio semejante en el que lo relevante es que la máquina, informática o mecánica, actúe a impulsos de una actuación ilegítima que bien puede consistir en la alteración de los elementos físicos, de aquellos que permite su programación, o por la introducción de datos falsos" (STS 369/07, de 9 de mayo).

Estas diferencias sustanciales determinan la no homogeneidad entre los apartados 1 y 2 del art. 248 (STS 185/06, 24 de febrero).

III. Calificación jurídica del phishing como estafa informática. La ignorancia deliberada

Debe anticiparse que el fenómeno complejo del phishing más común en la práctica de los tribunales comprende la actuación de al menos dos personas, el phisher y el "cyber-mula”, así como su desarrollo en diversos ámbitos territoriales, no sólo internos, sino de diferentes países, el lugar donde se encuentra el defraudador y desde el que lanza sus campañas de captación, el lugar donde la víctima recibe el ataque que puede o no coincidir con el domicilio de su cuenta bancaria, y el lugar donde el mulero desarrolla su contribución, recibiendo y extrayendo la suma defraudada que es enviada por él generalmente al extranjero, usualmente a países del este.

Esta circunstancia nos conduce a analizar la doctrina del Tribunal Supremo sobre la competencia,

porque para determinarla se hace preciso calificar la conducta criminal investigada o por investigar, y en este punto es unánime la posición contenida en los autos que resuelven los conflictos de competencia en virtud de la cual se caracteriza el ciberfraude del phishing como estafa informática.

Sabido es que a la estafa clásica se aplica la conocida como "Teoría de la Ubicuidad" que cristalizó en el Acuerdo no jurisdiccional del Peno del TS de fecha 3 febrero 2005, según el cual el delito se comete en todos los lugares en los que se desarrollan los elementos del tipo (en el caso de la estafa, donde se despliega el engaño o donde el sujeto pasivo realiza el acto de disposición patrimonial o donde se manifiesta el perjuicio) lo que implica que la competencia corresponde a aquel de los juzgados de dichos territorios que en primer lugar haya iniciado las actuaciones procesales.

La aplicación de esta teoría al caso del phishing precisa de matizaciones, pero en todos los casos el Alto Tribunal considera al mulero partícipe en un delito de estafa informática, “salvo que actúe bajo error”; a título de ejemplo el ATS de 19 de febrero de 2014 (nº de Recurso: 20768/2013) señala:

“Como ha dicho esta Sala en asuntos similares (vid. Auto de 6 de abril de 2011 citado por el Fiscal en la instancia y luego recogido en algunos de los pasajes de la exposición elevada) se trata de determinar la responsabilidad penal de este intermediario, conocido como 'mulero'. Los encargados de la sustracción y posterior ingreso permanecen sin identificar. Suelen residir en el extranjero. La conducta se englobaría en la figura de la estafa informática, salvo que actúen bajo error. La propia dinámica comisiva está pensada para hacer verosímil el engaño, dando al intermediario la condición de víctima de los scammers, que son quienes desde el extranjero transfieren el dinero apropiado a las cuentas de colaboradores, conscientes o inconscientes, situados en España. La responsabilidad de los 'muleros' dependerá de si tienen o no conciencia del origen ilícito del dinero.

En resoluciones de esta Sala (ver auto de 30-3-10 y de 6-4-11 cuestión de competencia 20023/11 entre otras) se ha especificado que nos encontramos en presencia de cuatro ubicaciones:

a) Lugar de emisión de los correos: A efectos de la investigación, éste sería el lugar en el que se inicia la trama defraudatoria, aunque a efectos de la investigación de los hechos resulta irrelevante por las propias indicaciones que hace la policía en torno al origen de este tipo de cuentas de correo y su anonimato.

b) Lugar de actuación y de residencia de la intermediaria: Granollers, donde recibe las transferencias en su cuenta corriente, de donde se extrae materialmente el dinero del circuito bancario, y desde donde se efectúan los envíos de metálico a los destinos en el extranjero con arreglo a las instrucciones recibidas. A los efectos de la investigación del delito de estafa, este lugar cobra trascendencia. La actuación de Tamara implica una cooperación necesaria en el delito de estafa: Granollers sería el lugar donde se han realizado parte de las acciones típicas, y donde, se hace salir el dinero del circuito bancario al convertirlo en metálico.

El envío por empresas dedicadas a tal fin produce al efecto de impedir la reversión del mismo al circuito y el reintegro a los perjudicados. Sería el Juzgado de Instrucción de Granollers competente para la instrucción de la causa por ser el lugar donde se han realizado conductas típicas del delito investigado. Además, es el lugar donde la investigación policial puede tener algún efecto, al poderse operar bien sobre el equipo informático de la imputada, bien sobre las empresas de envíos de dinero

metálico al extranjero; en definitiva donde la instrucción puede alcanzar, dentro de lo posible, más eficacia.

c) Lugar de residencia de las víctimas del delito y domicilio de la entidad bancaria donde tienen abiertas sus cuentas corrientes. Estos son lugares, a efectos de la instrucción de la causa, absolutamente irrelevantes. La mecánica operativa desplegada a través de Internet prescinde de la localización física de la concreta sucursal bancaria en la que la víctima tenga situada su cuenta corriente. Se opera desde la red y a través de claves y procedimientos informáticos. La operativa que no precisa la presencia física del autor en las localidades donde se encuentran ubicadas dichas cuentas corrientes.

d) Lugar de emisión de la orden de transferencia. Puede ser relevante para la investigación. Normalmente no coincidirá con ninguno de los lugares anteriormente considerados, ni los domicilios de las cuentas corrientes de donde se extrae el dinero, ni el domicilio de la cuenta corriente del intermediario.

Desconociéndose aquí el lugar en que se hubiese podido producir la aprehensión de las claves y se hubiese efectuado la orden de transferencia, la competencia ha de asignarse a Granollers.”

En el mismo sentido el ATS 20/12/02 (rec. 20712/2012) que resuelve cuestión de competencia negativa entre los juzgados de instrucción de Pozuelo de Alarcón, lugar donde la víctima de phishing interpuso denuncia, y de Burgos, donde el “mulero” había recibido y extraído del circuito bancario la suma defraudada enviándola a persona sita en Kiev (Ucrania), habiendo a su vez denunciado que su banco le había alertado de estar siendo partícipe en una “operación de blanqueo”. La competencia es atribuida al juzgado de Burgos al calificar los hechos como una posible estafa informática y reiterar la doctrina de la Sala expuesta anteriormente, mencionando precedentes (ver autos de 6-4-11, 23-10-11, 2-11-11, 10-11-11, 22-02-12, 16-10-12 cuestión de competencia 20423/12): “venimos diciendo que el lugar de emisión de los correos por parte de la empresa contratante y el lugar de residencia del titular de la cuenta bancaria víctima del delito, son datos que resultan irrelevantes a los efectos de la instrucción de la causa. Siendo datos trascendentes el lugar de actuación y de residencia del intermediario, al ser donde se reciben las transferencias y se extrae materialmente el dinero del circuito bancario para su envío a destinos en el extranjero.”

A pesar de lo que se viene exponiendo, y debido precisamente a las matizaciones que se han dejado apuntadas, la Sala II del Tribunal Supremo no mantiene una postura tan tajante cuando de resolver los recursos de casación frente a las sentencias dictadas contra los “muleros” se trata. Si bien la calificación preferentemente se acomoda al delito de estafa informática, el elemento distintivo se hace recaer en el aspecto subjetivo de la participación de éste en el complejo entramado delictivo, según que actúe conscientemente o no. La STS nº 834/2012, de 25 de octubre es exponente de esta posición:

“En definitiva, la calificación jurídica de los hechos como integrantes de un delito de estafa informática, receptación o blanqueo de capitales, obligará a analizar en qué medida el dolo de ese tercero que hace posible el rendimiento del capital evadido, capta los elementos del tipo objetivo del delito de estafa. Abrir una cuenta corriente con el exclusivo objeto de ingresar el dinero del que se desapodera a la víctima, encierra un hecho decisivo para la consumación del delito de estafa, pues en la mayoría de los casos, al autor principal no le será suficiente con disponer de la información precisa sobre las claves personales para ejecutar el acto de desapoderamiento. Necesitará una cuenta corriente

que no levante sospechas y que, mediante la extracción de las cantidades transferidas pueda llegar a obtener el beneficio económico perseguido. Precisamente por ello, la contribución de quien se presta interesadamente a convertirse en depositario momentáneo de los fondos sustraídos, integrará de ordinario el delito de estafa. Pero para ello resultará indispensable -claro es que quede suficientemente acreditada su participación dolosa en el delito cuya secuencia inicial ejecuta un tercero, pero a la que coopera de forma decisiva.

Todo aconseja, por tanto, atender a las circunstancias del caso concreto, huyendo de fórmulas estereotipadas cuya rigidez puede dificultar la adecuada calificación de los hechos.”

En los mismos términos se pronuncia la más reciente STS 845/2014, de 2 de diciembre: abrir una cuenta corriente con el exclusivo objeto de ingresar el dinero del que se desapodera a la víctima, encierra un hecho decisivo para la consumación del delito de estafa. No basta con disponer de las claves que permitan realizar la operación, es necesaria una cuenta corriente que no levante sospechas y que, mediante la extracción de las cantidades transferidas pueda llegar a obtener el beneficio económico perseguido. Precisamente por ello, la contribución de quien se presta interesadamente a convertirse en depositario momentáneo de los fondos sustraídos, integrará de ordinario el delito de estafa. Aunque es indispensables que quede acreditada su participación dolosa. En este caso no puede considerarse arbitraria o infundada la inferencia de la Sala sentenciadora respecto al conocimiento sobre la ilicitud del dinero obtenido por este mecanismo de quien lo recibe en sus cuentas, dispone de él y se aprovecha en parte de él. Se ha valorado la reiteración de los comportamientos y los flujos económicos entre los acusados. El dolo abarcó todos los elementos del tipo ya que estuvieron al corriente de toda la operativa, lo que unido a su relevante y eficiente aportación, conforman la coautoría que se les atribuye.

Desde esta posición, la atribución al mulero de un delito de estafa informática se asienta sobre los siguientes presupuestos:

- Su participación lo es a título de cooperador necesario, en cuanto que interviene cuando el delito aún no se ha consumado, proporcionando la cuenta bancaria destino a la que directamente irá a parar el dinero fraudulentamente extraído de la cuenta de la víctima; se trata de una aportación sin la cual el delito no se habría cometido según el plan del autor.

- Su imputación, naturalmente a título de dolo pues de una estafa se trata, deriva de un juicio de inferencia que se realiza a través de los datos objetivos con los que cuenta el tribunal, acudiéndose en ocasiones a la llamada “ignorancia deliberada” que es la que se atribuye a quien, teniendo a su alcance la posibilidad de despejar las dudas que naturalmente le pueden surgir como consecuencia de la propia mecánica en la que se involucra (una oferta de trabajo que le ofrece pingues beneficios sin apenas esfuerzo de su parte, el ingreso de dinero en su cuenta bancaria procedente de terceros, el envío del metálico al extranjero) no lo hace dado el provecho a obtener, por lo que al menos cabe atribuir a título de dolo eventual la estafa.

Junto a la calificación de estafa, surgen posiciones que hacen responder al mulero bancario, bien de un delito de receptación (art. 298), bien de un delito de blanqueo de capitales imprudente (art. 301.1 y 3), por cuanto estas figuras no exigen un conocimiento pleno del ilícito patrimonial previo, basta con conocer que los efectos, en este caso el dinero, procede de algún delito patrimonial del que se

aprovecha para obtener un lucro propio.

La primera opción choca con el principal inconveniente de que el receptador interviene cuando el delito patrimonial previo ya se ha consumado, y en él no ha tenido intervención alguna. En efecto, el mulero, como se dejó dicho, es pieza fundamental para la consumación, pues protagoniza con su conducta la extracción de la suma defraudada del circuito bancario, consuma la desposesión a la víctima.

La segunda opción es por la que optan los tribunales en las ocasiones en que el juicio de inferencia no arroja la atribución a título de dolo de la conducta, sino a título de imprudencia grave. Se produce, pues, la ruptura del título de imputación, estimándose que era exigible al partícipe una averiguación más cuidadosa que le hubiera permitido conocer la procedencia ilícita del capital que contribuyó a blanquear, superándose la pega expuesta para la receptación en tanto en cuanto es posible el autoblanqueo.

Finalmente en otros casos en Tribunal Supremo ha criticado la utilización del recurso al expediente de la “ignorancia deliberada” al considerar que su aplicación exige que el sujeto tenga un específico deber de despejar las dudas acerca de la regularidad de la operación, mientras que no puede suponer una inversión de la carga de la prueba ni una presunción del dolo. Así, a título de ejemplo, la STS 3-12-12, nº 987/2012, que absuelve al acusado licenciado en filosofía y que había sido condenado por estafa informática; por su parte, la STS 20-3-2013, nº 227/2013, que confirma la absolución de la acusada del delito de estafa informática señala que si bien la forma de actuar de la empresa que le dirigió la oferta de trabajo “era francamente extraña al modo de operar de las entidades financieras convencionales. Pero lo cierto es que, como, con patente rigor, razona la sala, nada indica que la acusada, por su cultura y experiencia, tuviera que haber sido consciente y ni siquiera albergado una sospecha al respecto".
IV. Posición de la víctima. La obligación de autoprotección

Como se viene exponiendo, en ciertos casos de phishing la propia víctima “coopera” involuntariamente al delito de estafa al proporcionar inocentemente los datos y claves que van a posibilitar las extracciones fraudulentas. Y es que en este caso si concurre un engaño como en el caso de la estafa clásica, por lo que es habitual el recurso de la defensa al argumento de la obligación de autoprotección.

A este respecto la anteriormente mencionada STS nº 845 de 2-12-2014 rechaza que pueda culpabilizarse a la víctima ni oponerse un deber de autoprotección frente a un ataque fraudulento como el que representa la dinámica delictiva de este delito, pues fuera de los casos de engaño burdo, no existe ni está en el tipo de la estafa un elemento tal, ni ha de merecer este delito de estafa un inferior grado de protección que el resto de los delitos patrimoniales, estando presente en este caso la buena fe negocial que impregna y fundamenta el ordenamiento jurídico.

De hecho, en la mayoría de los casos la entidad bancaria ha restaurado la integridad de los fondos depositados por el titular de la cuenta, teniendo en cuenta que el art. 31 de la Ley 16/2009 de 13 noviembre, de Servicios de Pago, dispone que en los casos de operaciones de pago no autorizadas por el titular de la cuenta la obligación del Banco es "devolver de inmediato el importe de la operación no autorizada y, en su caso, restablecer en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada", ello salvo que acredite una actuación fraudulenta del propio cliente, con negligencia grave o haya existido un retraso en comunicar el hecho a la entidad.

http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo;mulero-bancariordquo;:-categorizacion-y-doctrina-de-la-sala-segunda-del-tribunal-supremo/