

Ol.clPhishing y Pharming: Una aproximación desde el Cibercrimen

AUTOR

Esteban Maldonado Ayala, Comisario alumno de la Academia Superior de Estudios Policiales; Analista Informático especializado en Forense; Egresado de la carrera de Derecho Universidad Bolivariana; fundador de la Brigada Investigadora del Ciber Crimen Metropolitana PDI; ex profesor de la Especialidad en Delitos Informáticos, Centro de Capacitación Profesional PDI; relator en cursos de capacitación y actividades de extensión sobre Informática Forense; ex integrante del GTE Informática y Comunicaciones en las rondas preparatorias de la Reunión de Ministros de Interior de MERCOSUR y países asociados.

RESUMEN

Se examinan brevemente las características del fenómeno tecnológico y como éste se relaciona con la comisión de delitos y la respuesta jurídica y criminológica de la autoridad. Se analiza el phishing y el pharming como novedosas formas de comisión del fraude. Se describe el marco legal relacionado y sus inconvenientes presentes. Se exponen los detalles concernientes al tratamiento de la prueba, en específico la pericial. Se detallan las dificultades que se presentan ante la investigación policial del phishing y el pharming y se ofrecen dos soluciones. Finalmente se indican las iniciativas que tanto la PDI como el Ministerio Público y el sector bancario han realizado en relación con el fenómeno.

PALABRAS CLAVE

Delitos informáticos, fraude, phishing, pharming, malware, investigación policial, Derecho Penal, Derecho Procesal, prueba pericial, criminalística, Cibercrimen, informática forense.

"Usted planeaba desviar mucho más, quedó demostrado, pero fue descubierto antes de que pudiera hacerlo. Se trataba de un ingenioso fraude computarizado, completamente acorde con su reconocida habilidad en el ajedrez, pero no por eso dejaba de ser un delito. Y como usted dice, todo está computarizado, y en nuestros días no puede darse ningún paso, ni siquiera pequeño, sin una computadora. En consecuencia, defraudar por medio de una computadora supone descomponer lo que hoy por hoy constituye la estructura esencial de la civilización. Es un crimen terrible, y debe ser desanimado".

"Encajar Perfectamente"
Isaac Asimov

INTRODUCCION

Es desde toda perspectiva innegable que a partir de la revolución industrial, la tecnología ha ocupado cada espacio disponible en una multiplicidad de ámbitos. Desde su gran influencia en la Economía, especialmente en los medios de producción; hasta su omnipresencia en los actuales medios de comunicación, tanto personales como masivos, podemos encontrar evidencia de tal relación y grado de preponderancia.

La Informática, como fenómeno tecnológico, consiste en el procesamiento de información, en forma automática, a través del uso de computadores. En tal sentido y producto de la masificación del uso de estas herramientas,

sociológicamente ejerce importante influencia en el actual desarrollo cultural, proveyendo inmediatez en la creación y facilitando la diseminación electrónica de aceptadas pautas de comportamiento.

Por lo tanto, esta nueva *ciencia*, así como su más grande producto: Internet, han conformado un entramado social de características muy singulares, donde sus integrantes ya no son solo los genios de las escuelas tecnológicas, los piratas informáticos o reconocidos investigadores universitarios, tal como ocurría sólo veinte años atrás. Por el contrario, hoy cada uno de nosotros es un activo participante. Con tan sólo utilizar un teléfono celular o charlar animadamente vía mensajería instantánea ya somos titulares de pequeñas, pero importantes, cuotas de participación en este especial universo.

Castells (2001)ⁱ se refiere a la Internet señalando que *“es el corazón de un nuevo paradigma socio técnico que constituye, en realidad, la base material de nuestras vidas y de nuestras formas de relación, trabajo y de comunicación. Lo que hace Internet es procesar la virtualidad y transformarla en nuestra realidad, constituyendo la sociedad red, que es la sociedad en que vivimos”*.

Inevitablemente, como expresión subcultural al fin y al cabo, la criminalidad no queda al margen de tamaña influencia. Es así que descubre y aprovecha las *potencialidades* que este nuevo mundo ofrece. El fraude se transforma y pasa de ser una actividad realizada personalmente ante la víctima, basada exclusivamente en el engaño, a una modalidad en que su principal arma es la manipulación electrónica, acorde con los nuevos tiempos.

Queda establecido que, desde lo penal, el fenómeno ofrece interesantes espacios de

análisis donde el conflicto jurídico se hace presente y de modo complejo. En el Derecho todavía se discute si la criminalidad informática constituye sólo una modalidad delictiva a la luz de tipos ya existentes o puede dar lugar a figuras autónomas, bajo bienes jurídicos también autónomos. De igual modo, se traba la litis en torno a si los *hackers* deben ser considerados propiamente como delincuentes, dado que serían sólo buscadores de emociones personales, versus los delincuentes tradicionales que miran esencialmente hacia la obtención de beneficios económicos.

Viejas figuras típicas como las amenazas, las injurias, las calumnias, la usurpación de nombre, la pornografía infantil, el abuso sexual, violación de la privacidad, falsificación, entre otras, han encontrado efectivos cauces de comisión en la red de redes. Del mismo modo, nuevas descripciones sustantivas han cobrado vida al interior del ordenamiento legal chileno, plasmándose, por ejemplo, en las leyes 19.223 sobre delitos informáticos y 20.009 en cuanto al uso malicioso de tarjetas de crédito y débito. Ello, sin contar que las altas velocidades de transmisión disponibles y las técnicas específicas de compartición de archivos, tipo *“peer to peer”*, han infringido una grave herida a la propiedad intelectual, especialmente al derecho de autor, discusión que en Europa ha cobrado especial importancia a la luz del caso seguido en contra del sitio de enlaces *“Pirate Bay”*, en que luego de la condena impuesta surge espontáneamente todo un movimiento que exigía abrir espacio a la discusión política, en torno a los derechos de las personas en oposición a los que protegen las obras del intelecto.

Entonces, para el trabajo policial y, en general, para el tratamiento jurisdiccional de estos delitos, ya no basta con los

conocimientos legales y las tradicionales artes de investigación. Hoy se hace necesario agregar un profundo dominio de las nuevas tecnologías de la información y las comunicaciones, de tal modo que las instituciones policiales puedan ofrecer respuestas de calidad a las cada vez más complejas exigencias de una sociedad que día a día profundiza su virtualización.

Vamos a examinar dos formas de ejecución del fraude, que nacen en esencia gracias a la emergencia de las transacciones en línea, tanto relacionadas con cuentas corrientes bancarias como con tarjetas de crédito y débito.

EL PHISHING

Anglicismo que refiere una nueva forma de realización del fraude informático, en la que se hace extensivo uso de la ingeniería social en aras de:

- Obtener nombres de usuario y claves de acceso que luego puedan ser utilizadas para la obtención de dinero por medio de transferencias electrónicas de dinero.
- Conseguir los datos consignados en las tarjetas de crédito, para luego realizar compras presenciales o a través de Internet, logrando la final apropiación de las especies que obtenga.

El sujeto activo, simula una comunicación oficial electrónica por medio de la cual solicita fraudulentamente las informaciones antes señaladas u ofrece un *link* hacia un sitio web que aparenta ser de propiedad de una determinada entidad bancaria.

Como en la actividad pesquera tradicional, tal como se lanza una red, se envía aquella comunicación a una gran cantidad de

destinatarios, generalmente a través del correo electrónico, quedando a la espera de que la falta de conocimientos técnicos para reconocer el engaño les haga remitir los datos requeridos, confiados en que la comunicación realmente proviene de quien dice ser su emisor.

La historia señala que los primeros casos de *phishing* se detectaron a mediados del año 1990 por la empresa estadounidense America On Line. El estafador enviaba un correo electrónico solicitando diversas informaciones de facturación, entre las que se encontraban los números de las tarjetas de crédito empleadas para pagar por el servicio.

En Chile los primeros casos comienzan a registrarse a partir del año 2007, momento desde el cual se verifica una creciente frecuencia del fenómeno.

EL PHARMING

Una vez que el *phishing* pierde eficacia, debido a que las entidades bancarias afectadas, las empresas de tecnología y las fuerzas policiales realizan campañas preventivas a través de los medios de comunicación, los delincuentes informáticos desarrollan una técnica bastante más compleja que tiene por objeto perfeccionar el engaño, eliminando el envío masivo de una comunicación anzuelo.

Antes de continuar, el lector debe saber que en Internet los computadores no se *encuentran* por medio de nombres o *URLs* (por ejemplo www.policia.cl), sino que lo hacen gracias a una convención informática numérica denominada *dirección IP*. Por tal motivo, existe una estructura que realiza el trabajo de traducción entre esa *URL* y su dirección IP asociada. En primer lugar la consulta se resuelve internamente y luego mediante

la remisión del pedido a un servidor de nombres.

A esto se le denomina *DNS* o *Domain Name System*.

Habida cuenta de lo señalado, el *pharming* consiste en la introducción de código malicioso (conocido también como *malware*) en el *computador víctima*, con el fin de modificar un importante insumo del sistema de resolución de nombres.

En lo específico, ese *malware* altera un archivo de sistema denominado "*hosts*", introduciendo fraudulentamente una *URL* real junto a una dirección IP que dirige al usuario hacia una copia de un sitio web, modificada para engañarlo y obtener sus datos de cuenta corriente o números de tarjeta de crédito o débito, haciéndole creer que se trata del original.

De este modo, si se digita *www.banco.cl*, el software de navegación encontrará la *URL* en el listado del archivo *hosts* y llevará a la víctima al sitio suplantado.

Al igual que el *phishing*, las informaciones logradas por el delincuente serán empleadas para la realización de transferencias electrónicas o compras a través de Internet, con el perjuicio económico que ello implica.

MARCO LEGAL

Chile no posee legislación específica destinada al castigo del *phishing* y el *pharming*, como tipos independientes. Han de estimarse como una especial parte del *iter criminis* del fraude o del uso fraudulento de tarjetas de crédito o débito, según corresponda.

En consecuencia, si se han obtenido nombres de usuario y claves de acceso, que permitan la realización de

transferencias electrónicas de fondos, en estricto rigor el fenómeno debería ser tratado penalmente por la vía de subsumir la acción en la figura de la estafa residual, tipificada en el artículo 473º del Código Penal, que emplea la expresión "*el que defraudare o perjudicare a otro usando de cualquier engaño que no se halle expresado en los artículos anteriores...*".

Por su parte, si el sujeto activo consigue datos contenidos en una tarjeta de crédito o débito, deberá estarse a lo preceptuado en el artículo 5º de la Ley N° 20.009, que describe las conductas constitutivas del tipo.

No podría ser de otro modo, dado que estamos frente a un atentado en que el sistema informático se emplea como parte de una especial forma de comisión, facilitando la estructura sobre la que se orquesta el ardid que permite al sujeto activo obtener ganancias indebidas (Fillia, Monteleone, Nager y Sueiro, 2007)ⁱⁱ.

Para el caso especial del *phishing*, la jurisprudencia nacional ha estimado que también la acción es constitutiva de infracción al artículo 2º de la Ley N° 19.223, sobre delitos informáticos, donde se tipifica el llamado *espionaje informático*.

En esa misma línea de ideas, el *pharming* debiera ser tratado además en virtud del artículo 1º de la citada norma, dado que ciertamente se modifica el *funcionamiento* del sistema de tratamiento de información, acción que es claramente intencionada por parte del atacante.

La situación no es menor, dado que refleja escasos avances legislativos en temas que cada vez más adquieren gran relevancia para la preservación del orden económico imperante. Debe recordarse que el límite se establece en el tradicional respeto a los

principios de legalidad y reserva, dado que no es posible sancionar conductas que no se encuentren previamente establecidas en la Ley.

Se ha ignorado que la sociedad de la información representa un nuevo contexto (Marti y Vega-Almeida, 2005)ⁱⁱⁱ. Hoy la “*confianza en el sistema*” se alza como una necesidad jurídica transversal que exige cada vez mayor protección, ya que, como se ha reiterado latamente, descansa sobre bases tecnológicas.

EL TRATAMIENTO DE LA PRUEBA

En Chile la prueba se rige por dos principios básicos, descritos en los artículos 295º y 297º del Código Procesal Penal:

- Todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento podrán ser probados por cualquier medio producido e incorporado en conformidad a la ley.
- Los tribunales apreciarán la prueba con libertad, pero no podrán contradecir los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados.

Por lo tanto la obtención y exposición de la prueba cobra importancia capital. Para nuestros efectos asumiremos que el sistema más eficaz es precisamente el pericial, dado el especial soporte sobre el que se desarrolla la acción, motivo por el cual no bastará con señalarlo, sino que en juicio deberá acompañarse una comprensiva explicación técnica acerca de su funcionamiento.

Insa, Lázaro y García (2008)^{iv} proponen cinco puntos clave para desarrollar el

sistema de presentación de pruebas electrónicas en juicio, que servirá de base para explicar el argumento:

- Los jueces son los actores centrales en la admisibilidad de la prueba electrónica y los expertos de la policía ocupan una posición principal en la obtención de pruebas. Actuemos sobre estas dos tipologías de actores.
- La legislación tiene el efecto de influir positivamente en las percepciones de seguridad que tienen los diferentes agentes sociales. Adaptemos la legislación existente.
- Confianza en los expertos relacionados con la obtención, análisis y conservación de la prueba electrónica. Sigamos los procedimientos técnicos de los expertos.
- Formación, conocimiento y experiencia son los elementos necesarios e imprescindibles que tienen que reunir los expertos. Actuemos sobre la formación.
- La mejora en la comunicación entre los actores relacionados con la prueba electrónica, en el contexto nacional, europeo e internacional, es un bienpreciado y deseado unánimemente. Mejoremos el entendimiento entre jueces y técnicos.

Orta Martínez (2007)^v describe claramente esa relación cuando señala que “*la computación avanzada por lo general no forma parte de los conocimientos privados del Juez para poder valorarlos adecuadamente, por lo que es necesaria la promoción y evacuación de la llamada prueba pericial informática o experticia informática, siendo este auxilio*

de prueba el más idóneo cuando de hechos jurídicos informáticos se trata”.

Entonces, la investigación criminalística y específicamente el perito deberán ser capaces de reconstruir los acontecimientos que dieron lugar al delito. Especialmente, se deberán extraer todos los datos contenidos tanto en servidores como en computadores personales, que permitan determinar la relación causal que llevó a la consumación, para luego entregar sus impresiones al Juez en un lenguaje lo suficientemente neutro para ser entendido.

DIFICULTADES EN LA INVESTIGACIÓN POLICIAL DEL PHISHING Y EL PHARMING, DOS AREAS DE SOLUCION

Habida consideración de su falta de responsabilidad, no todos los bancos tienen protocolos de actuación adecuados, por lo que tardan incluso meses en aportar las informaciones relacionadas con las transacciones fraudulentas. En una extensiva interpretación de la Ley General de Bancos, sólo entregan esos datos si se presenta una orden de investigar y existe autorización del propietario de la cuenta afectada, quien debe consentir formalmente en el levantamiento de la reserva bancaria.

Por su parte, las empresas que desarrollan el rubro del giro internacional, tales como *Western Union* y *Chilexpress*, tampoco poseen estructuras destinadas a la entrega oportuna de información respecto del destino de los dineros remitidos y de las personas a quienes se dirigió el envío.

En materia de cooperación internacional, habida cuenta de la falta de instrumentos jurídicos globalmente suscritos, las consultas no siempre son respondidas, complicando gravemente la investigación,

por cuanto los destinos de los dineros, en gran parte de los casos, corresponden a terceros países, específicamente Rusia, México y Perú en el caso de las víctimas chilenas.

Todas estas dificultades pueden explicarse teniendo presente que los países generalmente acuden a su legislación interna para aceptar o rechazar un pedido de información, especialmente si es requerida en el marco de investigaciones realizadas en lo penal.

El Derecho Internacional ofrece una interesante solución, amén de los principios de libre consentimiento, buena fe y la norma *pacta sunt servanda*, universalmente reconocida, existente consuetudinariamente y formalmente considerada^{vi}, se ha establecido que en general “una parte no podrá invocar las disposiciones de su derecho interno como justificación del incumplimiento de un tratado” (artículo 27^o Convención de Viena).

Convención del Consejo de Europa sobre Ciberdelitos

Entonces, una primera solución mira hacia la Convención del Consejo de Europa sobre Ciberdelitos, suscrita en Budapest al año 2001 y entrada en vigor en el año 2004^{vii}.

Este instrumento básicamente se divide en dos grandes temas:

- Señala medidas que deben adoptarse a nivel nacional, especialmente en relación a diversas adecuaciones en materia penal y procesal que los países suscritos deben realizar en sus ordenamientos internos. Para nuestros efectos e ilustración, interesa el artículo 8^o, referido al fraude informático, donde se hace referencia

precisamente al tema de la interferencia en el funcionamiento y a la obtención de beneficios económicos producto de esa actuación fraudulenta o delictiva.

- Propone un ordenado sistema de cooperación internacional, tratando adecuadamente los temas de la extradición y la asistencia mutua, para luego referirse al procesamiento jurídico internacional de datos almacenados y finalmente plantear la creación de una red de contactos 24/7.

Como puede advertirse, adherir a la Convención supone un gran esfuerzo interno, pero también significa un avance importantísimo en el tratamiento del fenómeno delictivo informático a nivel global, permitiendo la necesaria estandarización jurídica y la imprescindible cooperación internacional. Lo contrario sería oponerse a la mundialización en todo sentido, ya que el problema nunca ha sido local.

Creación de capacidades sostenidas en países en desarrollo

Como ya se ha señalado, para el tratamiento jurisdiccional de estos delitos, ya no basta con los conocimientos legales y la tradicional *expertise* criminalística.

Se hace imprescindible la creación y puesta en práctica de planes intensivos de capacitación, ofrecidos por economías más desarrolladas y por aquellos países de la región que hayan logrado mayores competencias en la investigación tecnológico criminalística, dada la globalidad del problema.

En tal orden, debe resistirse la siempre presente intención de emplear estos medios como herramientas de orden político, dado que eventualmente todos

pueden llegar a ser víctimas, habida cuenta de su creciente dependencia de las tecnologías informáticas. El correcto sentido de estas ayudas mira a la instalación de redes de cooperación, habilitadas para la práctica de investigaciones localmente guiadas, que tengan por objetivo la generación válida de evidencias que puedan ser transformadas en pruebas, utilizables bajo las reglas de cualquier sistema de enjuiciamiento criminal.

INICIATIVAS ESPECÍFICAS

Policía de Investigaciones de Chile PDI

En respuesta al creciente fenómeno del delito informático, la PDI crea en el año 2000 la Brigada Investigadora del Cibercrimen Metropolitana, estableciendo que su misión fundamental consiste en investigar los ilícitos en que se utilicen computadores como componentes de especiales formas de comisión.

En paralelo al trabajo criminalístico, dicha unidad realiza actividades de extensión, durante las cuales se informa y advierte al público a través de charlas, seminarios y entrevistas en medios de comunicación.

Junto a ello, se emplean las redes sociales para establecer contacto con quienes deseen orientación en caso de sospechar que pueden ser potenciales víctimas.

De este modo, la PDI ha logrado importantes avances en la relación con el público del mundo tecnológico, aumentando la confianza en la asistencia profesional de sus oficiales, tanto a nivel criminalístico como en actividades de prevención.

A nivel interno, se produjo y publicó una cartilla diseñada especialmente para estandarizar una metodología para el

levantamiento de evidencias informáticas, con el fin que se utilice por todos los funcionarios que concurren a los distintos sitios de suceso informáticos.^{viii}

Ministerio Público

La respuesta del ente persecutor se ha traducido instruyendo a los Fiscales especializados en delitos económicos, en el adecuado tratamiento de los nuevos ilícitos, procediendo además a la acumulación de carpetas, con el objeto de responder adecuadamente a delitos cometidos por autores específicos, que afectan a una gran cantidad de víctimas.

Además, cuando se tiene conocimiento de una determinada pérdida patrimonial, producto de las acciones materia del presente artículo, el Fiscal tiene la facultad de solicitar la incautación de los fondos distraídos ilícitamente.

Sector Bancario

Dado que en lo esencial, y a la luz de la actual legislación, el sector bancario no tendría responsabilidad, proactivamente se han abocado a la realización de actividades preventivas, tales como el envío de comunicaciones electrónicas o físicas a sus clientes y la realización de campañas televisivas y radiales, en las que se advierte de los riesgos del fenómeno y se indican medidas para mitigar las posibilidades de llegar a ser víctima.

CONSIDERACIONES FINALES

Como ha podido apreciar el lector, el mundo de la delincuencia informática no es ajeno al desarrollo que alcanzan las nuevas tecnologías de la información.

A partir de dicha premisa, es necesario señalar que también la respuesta de la autoridad debe ajustarse al *estado del arte*

de la ciencia informática. De otro modo se corre el grave riesgo de caer en la obsolescencia, y los usuarios de los servicios criminalístico policiales que provee el Estado serán los principales perjudicados.

Esa posibilidad implica afectar seriamente la necesaria confianza que el público debe tener en la estructura tecnológica sobre la que descansa nuestra civilización.

Los ciudadanos tienen el derecho a ser protegidos, y el Estado tiene la obligación de ofrecer esa protección.

REFERENCIAS

ⁱ Castells, Manuel, "Internet: ¿Una arquitectura de libertad? Libre comunicación y control del poder". http://www.uoc.edu/web/esp/launiversidad/inaugural01/internet_arq.html, 2001.

ⁱⁱ Fillia, Monteleone, Nager y Sueiro, "Análisis Integrado de la criminalidad informática", Fabián J. Di Plácido Ediciones, Buenos Aires, 2007.

ⁱⁱⁱ MARTI, Johannis y VEGA-ALMEIDA Rosa Lidia. Sociedad de la información: Los mecanismos reguladores en el contexto de una sociedad emergente. Ci. Inf., Brasília, v. 34, n. 1, p.37-44, jan./abr. 2005.

^{iv} INSA MERIDA, Fredesvinda, LAZARO HERRERO, Carmen y GARCIA GONZALEZ, Nuria. Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad.: Un proyecto europeo. *Enlace*, mayo 2008, vol.5, no.2, p.139-152. ISSN 1690-7515.

^v RICO CARRILLO, Mariana y otros. "Derecho de las nuevas tecnologías", P. 573 "Las pruebas en el Derecho Informático", Ediciones La Roca, Buenos Aires, 2007.

vi Convención de Viena sobre el Derecho de los Tratados, Naciones Unidas, 1969.

vii Convención del Consejo de Europa sobre Ciberdelincuencia, Budapest, 2001.

viii Cartilla de Instrucciones de Trabajo para Levantamiento de Evidencias Informáticas, BRICIBMET, 2007.