CHIHUAHUA
GOBIERNO DEL ESTADO

CHIHUAHUA

FISCALÍA
GENERAL DEL ESTADO

ESTADO LIBRE Y SOBERANO DE CHIHUAHUA

Secretaría de Educación y Deporte

FISCALÍA GENERAL DEL ESTADO

INSTITUTO ESTATAL DE SEGURIDAD PÚBLICA

T E S I N A

REFORMA AL ARTÍCULO 327 BIS DEL CÓDIGO PENAL DEL ESTADO DE CHIHUAHUA PARA PROTECCIÓN DE LOS DATOS PERSONALES

Para obtener el Grado de:

MAESTRA EN DERECHOS HUMANOS Y PERSPECTIVA DE GÉNERO

Catedrático: MTRA. ETHEL GARZA ARMENDARIZ

Postulante: Lic. ADRIANA JAQUEZ VALLES

Chihuahua, Chih., a 13 de Junio de 2022.

ESTADO LIBRE Y SOBERANO

DE CHIHUAHUA

Secretaría de Educación y Deporte

FISCALÍA GENERAL DEL ESTADO

INSTITUTO ESTATAL DE SEGURIDAD PÚBLICA

T E S I N A

REFORMA AL ARTÍCULO 327 BIS DEL CÓDIGO PENAL DEL ESTADO DE CHIHUAHUA PARA PROTECCIÓN DE LOS DATOS PERSONALES

Para obtener el Grado de:

MAESTRA EN DERECHOS HUMANOS Y PERSPECTIVA DE GÉNERO

Catedrático: MTRA. ETHEL GARZA ARMENDARIZ

Postulante: **Lic. ADRIANA JAQUEZ VALLES**

Chihuahua, Chih., a 13 de Junio de 2022

AGRADECIMIENTOS Y DEDICATORIAS

Dedicatoria: El presente lo dedico principalmente a Dios, por darme la vida y que gracias a él, he llegado hasta donde me encuentro. A mis hijos José Luis y Josué que son mi motor, el tesoro más preciado que tengo en mi vida, son mi fuente de motivación, les doy gracias por darnos fuerza para seguir adelante y continuar en este proceso de obtener uno de mis sueños más deseados, a mi mamá Martha Valles, por ser el pilar más importante, gracias por demostrarme siempre su amor y apoyo incondicional, por confiar en mí, por los consejos, valores y principios que me han inculcado, y hermanos Martha, Andrés, Armando, Isaac y Jonathan, por estar siempre presentes, acompañarme y por el apoyo moral, todo este tiempo.

Agradecemos a Fiscalía General del Estado por darme la oportunidad de estudiar un posgrado, a nuestros docentes de la Instituto Estatal de Seguridad Pública del Estado de Chihuahua, por haber compartido sus conocimientos a lo largo de la preparación en esta etapa profesional

INTRODUCCIÓN

La presente investigación pretende evidenciar los elementos ausentes del marco jurídico chihuahuense, concerniente a la protección de los datos personales y evitar el uso inadecuado por terceras personas y en perjuicio de los individuos titulares de derechos; al mismo tiempo propone instrumentos que pueden contribuir en la reducción de este delito como lo es una reforma al artículo 327 bis del Código Penal del Estado de Chihuahua en donde se tipifique este delito.

El principal motivo para realizar este estudio, se origina en el incremento de casos donde sujetos carentes de moralidad se hacen pasar por instituciones públicas o privadas y logran que sus miembros, socios, clientes o beneficiarios otorguen información personal que al final es utilizada en su perjuicio y que pierdan dinero en la mayoría de los casos. Aunque esta conducta de mala fe tiene relación con otros delitos como el fraude, es preciso diferenciarlo ya que la legislación actual no lo contempla y por consiguiente abre una ventana para la impunidad.

Ésta investigación cuya metodología es de naturaleza cualitativa, utiliza el método descriptivo, con instrumentos como entrevistas y encuestas para estudiar a la población mayor de edad residente del Estado de Chihuahua, que ha sido víctima de esta omisión legislativa. Igualmente se estudiará mediante los mismos instrumentos a los Agentes del Ministerio Público que son los encargados de emprender acciones legales contra aquellos que resulten responsables de infracciones a la ley, siendo el caso anterior muy particular ya que no existen leyes que sancionen este ilícito. Además, engloba cinco categorías: elementos jurídicos ausentes, Derechos Humanos perjudicados, incidencia del delito, medidas legales propuestas para la reducción del delito y medidas técnicas encaminadas en la reducción del delito. Se contempla que la citada investigación emplee un tiempo de ocho meses.

ÍNDICE

CAPÍTULO PRIMERO

1.1 Descripción general de la problemática

El presente trabajo analiza la evolución del phishing como práctica criminal, abarcando desde su concepto y técnicas más básicas hasta sus variantes más sofisticadas. Además se incluyen conceptos básicos que permiten delimitar los límites de la punibilidad de éste delito y se analiza el marco jurídico español, que penaliza esta práctica, a la par de que menciona cómo es que sus instituciones manejan dichos ilícitos.

El objetivo principal es demostrar la vulnerabilidad de los mecanismos actuales de seguridad a ataques que son dirigidos a la ingenuidad e inexperiencia de los usuarios e incluso instituciones, y dar las pautas legales para sancionar esta práctica que va en aumento año con año.

1.2 Precedentes del phishing

La palabra phishing proviene de la palabra en inglés fishing (pesca), y surge por la analogía entre como un pescador (7isher) usa una carnada para capturar peces, de la misma forma que un estafador en internet (phisher) envía correos electrónicos prometiendo beneficios (la carnada) a cambio de que la persona que lo recibe brinde información vital como la contraseña del banco o del correo. La primera vez que se utilizó este término para referirse a esta práctica fue en Enero de 1996 en la publicación 2600: The Hacker Quaterly, donde retrataban

las técnicas de ingeniería social usadas por hackers para obtener contraseñas y números de tarjeta de crédito de usuarios de America On-Line (ya para este momento era usual en terminología hacker remplazar la f al comienzo de algunas palabras por ph).

Para principios de este siglo los criminales informáticos ya habían agotado lo que podían obtener de AOL y vieron en el floreciente comercio electrónico implementado por entidades bancarias una nueva fuente de víctimas con una tasa de retorno mayor. El primer ataque de phishing registrado hacia una entidad financiera fue en Junio de 2001 en contra de e- Gold, un sistema de pago en línea. A partir de ese instante el número de ataques empezó a crecer rápidamente y para 2003 ya se registraban las pérdidas en los miles de millones de dólares.

1.3 Delimitación y definición del problema a abordar

El phishing abarca un diverso número de técnicas que varían en su complejidad y en las vulnerabilidades que explotan. En esta sección se abarcan las distintas técnicas registradas hasta el momento, con ejemplos y variantes posibles. En sí pueden existir otras técnicas aún no registradas, o que se basan en vulnerabilidades puntuales a un sistema u organización especifica.

Asimismo ante las soluciones que emergen en el mercado para contrarrestar las técnicas de phishing más conocidas, los phishers idean nuevas maneras de engañar a los usuarios, por lo que es una dinámica de realimentación constante. En las secciones posteriores se analiza los distintos mecanismos de

defensa ante el phishing.

Para definir phishing es necesario analizar lo que no es. Como se mencionó al principio de este trabajo el phishing es sólo una de las formas de fraude en internet y una forma de robo de identidad, y no debe ser confundida con prácticas como los fraudes en transacciones electrónicas.

1.4 Derecho a la protección de los datos personales

La protección de los datos personales es un derecho vinculado a la protección de la privacidad y los medios para controlar el uso y destino de información personal, con el propósito de impedir su tráfico ilícito y la potencial vulneración de la dignidad. Es trascendental que el titular de los derechos conozca en todo momento quiénes son los que disponen de sus datos y para qué están siendo utilizados. Además de que conozca su derecho a solicitar la rectificación de sus datos si estos están incompletos o inexactos; o que solicite la cancelación de los mismos por no ajustarse a las disposiciones aplicables. Sin embargo, el más importante es que éste goza del derecho a oponerse al uso de sus datos cuando son obtenidos sin su consentimiento o mediante engaños.

Los datos personales son cualquier información relativa a una persona física, que la identifica o hace identificable. Es la información que describe, que da identidad, que caracteriza y diferencia de otros individuos. Dichos datos se pueden agrupar en datos sensibles y datos patrimoniales o financieros.

Los datos sensibles son de acuerdo a Jijena Leyva (1999) los datos personales que informan sobre los aspectos más íntimos de los individuos, y cuyo uso indebido puede provocar actos discriminatorios o poner en peligro a esa persona o a sus familias. Un claro ejemplo de ello es el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual. En ese sentido, estos datos requieren de especial protección y cuidado por parte de las instituciones públicas y privadas que respaldan los datos.

Por otro lado, según Albarrán Martínez (1998), los datos patrimoniales o financieros son aquellos que brindan información sobre la capacidad económica de las personas físicas que hacen referencia a los recursos económicos o patrimoniales que posee. Además, incluye datos sobre su capacidad para afrontar deudas, de su dinero, bienes muebles e inmuebles; información fiscal; historial crediticio; ingresos y egresos; cuentas bancarias; seguros; afores; fianzas, número de tarjeta de crédito, número de seguridad, entre otros más.

Lo anteriormente descrito, al implicar su uso un riesgo importante para el titular, estos datos también requieren de especial protección por parte de las instituciones, es decir por parte de bancos o sociedades comerciales, así como del Estado.

1.5 La evolución del delito: las tecnologías de la información y comunicación

La constante evolución de las tecnologías de la comunicación trae consigo nuevas posibilidades para un indebido aprovechamiento por parte de individuos sin escrúpulos. Eso viene sucediendo desde la creación de otros medios de comunicación como el telégrafo, continuándose con la sistematización del uso del teléfono fijo y después el teléfono móvil. A posteriori, con la invención y desarrollo de la computadora y así como la expansión del internet; la capacidad de procesamiento de datos e información y el acceso a miles de personas en un medio interactivo de características globales amplía las posibilidades de comisión de hechos ilícitos e ilegales a partir del fácil manejo del surgimiento de entornos digitales "amigables" y aplicaciones prácticas y sencillas en cuanto a su manejo, tanto así como las posibilidades de anonimato en las comunicaciones.

Los delitos informáticos son definidos por la Organización para la Cooperación Económica y el Desarrollo (1983) como *"cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos"* (p. 9).

Aunque existe un número considerable de delitos cibernéticos, el phishing, smishing y vishing son notables porque que se valen de diversas técnicas de estafa con el objetivo de robar dinero o acceder a información valiosa almacenada en los dispositivos de las personas. Para Basto García (2020), estos métodos se basan en la ingeniería social para intentar manipular a las víctimas hasta que proporcionen sus datos personales en una página fraudulenta.

CAPÍTULO SEGUNDO

2.1 Problemática actual

El mundo globalizado facilita la comunicación entre las diversas sociedades, haciendo que la interacción social se virtualice y que a la par se desarrollen las tecnologías de la información. Este progreso social y tecnológico arrastra consigo a la evolución de las actividades delincuenciales e incluso la aparición de nuevas formas delictivas, ya que el uso de redes de comunicación no excluye a los delincuentes. Dichos individuos, en búsqueda de su beneficio, encuentran la forma de cometer delitos en cualquier lugar del planeta, a una velocidad considerable, y hacia una enorme cantidad de víctimas potenciales, así como desde el anonimato o con identidades falsas.

El anterior punto revela que no se puede garantizar la autenticidad del nombre de un usuario, facilitando que individuos carentes de sentido de la legalidad suplanten identidades de personas o empresas para estafar y obtener información confidencial de forma fraudulenta. De esta forma los usuarios proporcionan contraseñas o información detallada sobre tarjetas de crédito u otra información bancaria, permitiendo que criminales lucren con ello.

A diario miles de clientes del sector financiero son presa de la delincuencia digital, siendo este conjunto quien más sufre afectaciones. Por desgracia, existe un vació legal que no permite una justa aplicación de la ley, permitiendo la evasión de la justicia por parte de estos malhechores. Este escenario orilla a los gobiernos, las instituciones y organismos internacionales, a plantear la necesidad de hacer un frente común y forjar barreras tecnológicas, así como jurídicas y sociales contra estos delitos cibernéticos.

Por lo anterior se plantea: ¿Qué elementos se deben integrar al marco jurídico chihuahuense, para legislar el derecho a la protección de datos personales y evitar el mal uso de los mismos en perjuicio de los individuos?

2.2 Legislación Estatal

La importancia de esta investigación radica en que la actual legislación chihuahuense carece de instrumentos jurídicos que permitan sancionar a los individuos carentes de moralidad, y que mediante engaños se hacen de datos de terceras personas, lucrando con ellas para su beneficio personal, como en el phishing. La existencia de una base legal sólida que sancione ilícitos permite a los impartidores de justicia aplicar la ley en un sentido estricto, emitiendo acusaciones y sentencias firmes. Lo anterior hace valer el derecho a la administración de justicia, consagrado en el artículo 17 de la Constitución Política de los Estados Unidos Mexicanos.

En la actualidad, la incidencia de delitos informáticos va en aumento como consecuencia del desarrollo de nuevas tecnologías de la comunicación, así como de la integración de individuos de los distintos grados socioeconómicos, sin exceptuar a malhechores o potenciales criminales. Esto abre una ventana para que más delitos se realicen de manera virtual o digital, por desgracia, la mayoría de los marcos jurídicos estatales son omisos al tipificar estas acciones de mala fe; prestando particular interés en el phishing, sólo una entidad federativa de la República Mexicana lo ha logrado, Coahuila, a través de la reforma al artículo 268 del Código Penal de Coahuila de Zaragoza, publicada el 12 de febrero del 2021.

2.3 Legislación federal

Pese a que año con año incrementan los casos de victimas de phishing en nuestro país, no existe legislación federal alguna con carácter penal que lo sancione, ya que lo más próximo que tenemos son los delitos informáticos, que en el artículo 211 del Capítulo II - Acceso Ilícito a Sistemas y Equipos de Informática, del Título Noveno - Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática del Libro Segundo del Código Penal Federal describen:

> **Artículo 211 bis 1**
>
> "Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa."
>
> **Artículo 211 bis 4**
>
> "Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa."

Por ello, los individuos que se atreven a cometer estos ilícitos evaden el proceso penal, al no haber elementos suficientes para juzgar su acción en base al marco jurídico vigente, donde no existe la figura de phishing como delito.

2.4 El phishing como figura delictiva

Ahora bien, con miras a responder la interrogante acerca de la naturaleza jurídica del phishing, se debe tener presente que nos situamos en el ámbito de aquello que se ha denominado iter criminis, término con el cual se alude a la progresión de etapas sucesivas que conforman el proceso de ejecución de un delito.

Así, se debe mencionar que primero el sujeto idea el hecho punible, de modo que se representa intelectualmente la posibilidad de realización del mismo. Luego, si su voluntad acoge aquello que ha discurrido, el sujeto resuelve cometerlo, disponiéndose a planificar su conducta. Posteriormente, se dirige a preparar la ejecución del hecho punible, para lo cual ordena los medios e instrumentos para asegurar su éxito. Solo una vez que se encuentra en este punto se orientará a verificar la acción típica, o si se tratara de delitos de resultado, a causar el evento típico. Culmina este desarrollo con la consumación del hecho típico, es decir, con la realización completa de este. Al respecto, la doctrina ha entendido que el delito se encuentra consumado en aquellos casos en que el hecho concreto corresponde exactamente a la descripción abstracta que está contenida en el tipo que la ley señala. Asimismo, "hay quienes hablan también de delito agotado, refiriéndose a aquel momento del desarrollo del delito en que se han producido todas las consecuencias del hecho delictuoso y en que el sujeto activo, por consiguiente, no sólo ha dado cima al hecho típico, sino ha logrado,

además, obtener todos los efectos ilícitos que mediante él se proponía conseguir". Bajo esta lógica, es posible distinguir en la realización del hecho punible dos fases: una interna o psicológica y otra externa o material.

1. La fase interna corresponde a aquella que se desarrolla en la psiquis del sujeto, y "consiste en fenómenos psicológicos del sujeto no trascendentes al exterior ni perceptibles por extraños". Generalmente, aquí tiene lugar una ideación del plan delictivo, seguido de una deliberación acerca de éste, ponderando las consiguientes ventajas e inconvenientes que pudieran conllevar la realización del hecho punible, sucedida por la resolución de realizarlo.

2. En la fase externa, en tanto, el sujeto una vez que ha resuelto la comisión del hecho punible, se dirige a realizar lo necesario para cumplir con su fin, proyectando de esta forma su propósito de delinquir en la exterioridad. Existe, por tanto, un traslado del dominio psicológico en el que se centraba la fase interna, hacia una "materialización de la voluntad criminal". Así, "algunos de los actos de que se vale para cumplirlo están distantes de la consumación misma, pero gradualmente se va acercando a ésta con actos más próximos y directos hasta que llega, finalmente a su meta".

2.5 Justificación investigativa

La presente investigación brinda los elementos necesarios para considerar la urgencia de tipificar al phishing como delito ya que afecta a decenas de chihuahuenses día con día.

El principal beneficiario es la población en general ya que con regularidad emplean los medios electrónicos o digitales y que por ignorancia o descuido en ocasiones no se toman las debidas precauciones con el uso de su información, convirtiéndose en blancos de estos sujetos. Además, se genera mayor confianza en las autoridades y las leyes, al darse cuenta de que el acto del que fueron víctima es perseguido y que existen posibilidades de que se resarza el daño.

Dado que el Código Penal del Estado de Chihuahua es ambiguo con respecto a la aplicación de la justicia en delitos cibernéticos y haciendo énfasis en lo que se conoce como phishing, conlleva a una alta impunidad ya que sin leyes claras no es posible perseguir delitos. Una reforma al artículo 327 bis del Código Penal del Estado de Chihuahua, en donde se adicione la tipificación de este delito no sólo es viable, sino urgente y necesario, contribuyendo en la disminución de la incidencia de esta transgresión. Es preciso mencionar que en el actual contexto de la pandemia por SARS-Cov-2 y la crisis económica generada, se ha disparado de manera considerable la incidencia de esta problemática, perjudicando sobre todo a usuarios de instituciones bancarias u organismos financieros.

CAPÍTULO TERCERO

Conceptualización

3.1 Delito

Desde el origen de la humanidad está presente la inexplicable necesidad de convivir con otros individuos de nuestra especie, formándose sociedades primitivas que han evolucionado y lo siguen haciendo hasta convertirse en la actual. Sin embargo, desde tiempos remotos hay registro de la existencia de códigos que buscaban mantener la paz social, como el Hammurabi, del 1700 a.C., donde se establecen penas para algunos de los actos inaceptables para la sociedad de aquel entonces, concebidos como delitos en la actualidad.

Por lo anterior, es preciso definir a la palabra delito, que de acuerdo a la definición sustancial de Reyes Echandía (1998) significa *"el comportamiento humano que a precio del legislador compromete las condiciones de existencia, conservación y desarrollo de la comunidad y exige como respuesta una sanción penal"* (p. 93).

Esta definición explica cuáles son los motivos que impulsan al legislador a sancionar algunas conductas y otras no. Sin embargo, es relevante destacar que la concepción actual de delito varía de acuerdo a las épocas que se viven y estas leyes que penalizan dichas acciones no son perpetuas. Es decir, evolucionan año con año, despenalizando ciertas conductas y tipificando algunas otras.

De acuerdo a lo antes descrito podemos resumir que delito es un comportamiento que, ya sea por propia voluntad o por imprudencia, resulta contrario a lo establecido por la ley. El delito, por lo tanto, implica una violación de las normas vigentes, lo que hace que merezca un castigo o pena.

3.2 Delito informático

El nacimiento y expansión de las Tecnologías de la Información y la Comunicación (en lo sucesivo, "TIC"), en especial de Internet, han supuesto la adaptación y aprovechamiento de esta nueva vía para adaptar la consecución de ciertos comportamientos tipificados en el Código Penal del Estado de Chihuahua. Para determinar qué se entiende por "delito informático", la razón deduce que lo más adecuado es acudir al citado cuerpo legal. Sin embargo, no existen referencias expresas a este tipo de ilícitos. La realidad socio-jurídica nos empuja a deducir que existen muchas más modalidades de delitos que son susceptibles de cometerse por vía informática, como, por ejemplo, la estafa, la falsedad documental y la pornografía infantil. En este sentido, el legislador ha optado por el tratamiento penal del medio empleado para cometer el delito dentro del articulado en el que se castigan ciertas conductas, en lugar de tipificar una acción u omisión cometida por medios informáticos como delito individual. En definitiva, se reconoce a las TIC como medio idóneo para la acometida de delitos ya tipificados, acercando la regulación penal a la realidad social. De acuerdo a María de Luz *Lima* (1984) el "delito electrónico" en un sentido amplio es:

> ...cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin (p. 99).

En consecuencia, debemos concluir que los "delitos informáticos" no están bien esclarecidos, porque para que ello sea posible deben estar tipificados como tales en el Código Penal del Estado de Chihuahua. No obstante, se permite la alusión en estos términos respecto a conductas u omisiones efectuadas a través de las TIC.

La continuación del examen del concepto que da nombre a este apartado obliga a exponer las conclusiones que la razón alcanza cuando lo efectúa. Tomando como punto de partida el itinerario de un procedimiento penal a efectos de determinar las características del término, los delitos cometidos a través de Internet presentan ciertas dificultades en la incoación del procedimiento, en la fase de instrucción y en su enjuiciamiento.

Sin ánimo de incurrir en reiteraciones innecesarias, basta decir, como muestra de tales contingencias que estas infracciones precisan de la readaptación del concepto "lugar de comisión del delito", ya que no es posible ubicar desde el punto de vista clásico la realización de la acción.

Asimismo, la víctima debe contar con conocimientos mínimos y medios materiales suficientes para la recolección de pruebas que acrediten ciertos indicios

de la presunta comisión de la acción gravosa, hecho por el que finalmente estos asuntos terminan en manos del Agente Ministerio Público y Agentes de Investigación. Finalmente, es necesaria la formación de los Jueces y Magistrados en esta materia, ya que muchos de ellos carecen de conocimientos suficientes como para comprender lo que un perito informático pueda exponer en un informe y posterior comparecencia en juicio, y finalmente dictar una resolución conforme a Derecho que cumpla con las exigencias derivadas del derecho a la tutela judicial efectiva.

3.3 Conducta

Se puede definir como el primer elemento básico del delito, y se define como el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito. Lo que significa que sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito porque tiene una finalidad al realizarse la acción u omisión.

3.4 Tipicidad

Para Quintino Zepeda (2017), la tipicidad se define como *"el encuadramiento de la conducta en el tipo penal, es decir cuando una conducta está descrita en alguna ley penal y ocurre que alguien lleva a cabo dicha conducta descrita"* (p.18).

Por su parte, Muñoz Conde (2017) la describe cómo: *"la cualidad que se atribuye a un comportamiento cuando es subsumible en el supuesto del hecho de una norma penal"* (p. 40).

3.5 Delincuente cibernético

En los últimos tiempos, resultan bastante frecuentes las referencias a piratas informáticos con ocasión de los ciberataques perpetrados, que se han vuelto un plato recurrente en la prensa diaria. Es preciso comentar que, ciberdelincuente no es sinónimo de hacker, ya que el primero engloba a múltiples sujetos que cometen estos ilícitos, como son los crackers, phreackers, viruckers, piratas informáticos, script kiddie, noob, newbie, lammer, dropper, carder, cyberstalker, phisher, entre otros.

En este sentido, llama poderosamente la atención la referencia a éstos con el término hacker, error en el que también incurre la Real Academia de la Lengua Española.

Las figuras analizadas tienen su origen en el ámbito de la ingeniería informática, de tal manera que tanto hackers como crackers son expertos en acceder, monitorizar y llevar a cabo el mantenimiento de los sistemas informáticos. No obstante, a mediados de la década de 1980 comenzaron a surgir individuos cuyo entretenimiento consistía en la violación de los mecanismos de seguridad de estos sistemas con objetivos dispares. Frente a ellos, los expertos en ciberseguridad que se encontraban dentro de la esfera legal de sus funciones

acuñaron el término cracker para referirse a los primeros, mientras que ellos patrimonializaron el concepto de hacker.

De esta forma, frente a los hackers (cuya función principal es solventar los problemas de seguridad de los sistemas), podemos definir a los crackers, también conocidos como "sombreros negros" o "piratas informáticos", como las personas que profanan la seguridad de un sistema informático sin consentimiento del usuario para obtener información que utilizarán con fines espurios y que redundarán en su propio beneficio.

En analogía con lo sucedido con los tipos de phishing, los crackers se catalogan dependiendo de la parte del sistema en la que estén especializados sus ataques y del lugar desde el que los perpetran. Por ejemplo, existen individuos expertos en intervenir comunicaciones telefónicas (phreakers), en alterar la configuración de sitios web (cyberpunks) o parte de un software (crackers de sistemas), o que prestan sus servicios dentro de una empresa a la que atacan desde dentro de sus sistemas (insiders).

La motivación que empuja a este colectivo a violar los sistemas de seguridad de particulares y empresas es de carácter dispar y varía según los conocimientos que haya adquirido. En este sentido, un cracker novel estará capacitado para programar un ataque de phishing sencillo contra una persona o un colectivo determinado de ellas con el objetivo de que le faciliten sus datos bancarios y enriquecerse a costa del patrimonio de las víctimas mediante

transferencias de cantidades pequeñas de dinero, pero no podrá violar los sistemas de seguridad del Gobierno de una nación sin ser detectado.

En muchas ocasiones, la motivación subyacente en la actuación de estos individuos no es tanto el enriquecimiento injusto, sino la reivindicación de una causa que creen justa, la simple diversión (aderezada por grandes cantidades de ego) o el desafío, mayoritariamente ejercitado a instancias de los Gobiernos contra otras organizaciones gubernamentales por motivos políticos o estratégicos. Resulta anecdótico que, pese a su ocupación, finalmente muchos de estos crackers (que comienzan muy jóvenes en el "oficio") se reforman y son fichados por grandes empresas dedicadas a la seguridad en Internet.

El perfil del delincuente informático cuenta con ciertas características que le facilitan conducir o perpetrar el delito, características técnicas de forma amplia, que a conciencia y voluntad busca hacer un daño sobre un bien o una persona en específico para obtener, destruir, alterar o divulgar la información deseada.

Haciendo hincapié en la figura de phisher, se refieren al individuo que se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, o incluso utilizando también llamadas telefónicas cuya finalidad es solicitar a sus clientes o usuarios, información sobre tarjetas de crédito, cuentas bancarias, contraseñas y demás datos relevantes que les permitan efectivizar el delito.

CAPÍTULO CUARTO

Phishing

4.1 Concepto de phishing

La actualización tecnológica y su uso cada vez mayor en diversos rubros, ha alcanzado a la banca, digitalizando procesos y realizando diversos trámites en línea a través de los smartphone, sin embargo, con ello aumentan los ataques a las instituciones financieras y a los usuarios. Mediante el phishing o suplantación de identidad, se hace relación al abuso informático caracterizado por intentar adquirir información confidencial de forma fraudulenta. Bolaños, Simone y Becerra (2005) señalan que:

> [...] consiste en una modalidad de estafa que tiene como objetivo intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjetas de crédito, identidades, etc. En resumen, extrae todas las referencias posibles para después usarlas con fines fraudulentos. (págs. 20,21).

El sistema financiero y bancario además de incorporar verdaderos sistemas de protección para evitar riesgos que amenacen la seguridad de la actividad financiera, también les compete generar procesos de educación e información expedita para los usuarios o clientes. Estos permitan evitar el phishing que comprometan las transacciones bancarias físicas o en línea, prevenir los ataques

a través de software malicioso y ante todo, garantizar la seguridad de las claves y dispositivos electrónicos, mediante los cuales se realiza transacciones financieras.

Es importante precisar que phishing no es sinónimo de usurpación de identidad, puesto que este ilícito tiene características bien marcadas, que de acuerdo a lo señalado por Mónica Márquez (2019), lo anterior se entiende como *"el apoderamiento con o sin violencia, intimidación o violación de los rasgos propios de un individuo o de una colectividad, que la caracteriza y hace diferente de los demás"* (p.341).

4.2 Origen de la palabra

Como es mencionado en los textos bibliográficos "La palabra Phishing proviene de la palabra en inglés "fishing" (pesca)". Si nos detenemos a pensar un poco, podremos afirmar que la palabra pesca es utiliza ya que el phishing es una pesca de información que realizan los hackers en Internet para poder robar información a los cibernautas de sus cuentas bancarias. Haciendo la comparación entre la pesca en general y el phishing, encontramos que en la pesca se usa una carnada para poner en el anzuelo y con esta atrapar los pescados. En el phishing también se usa una carnada y se pone en un anzuelo. Para este caso el anzuelo sería la bandeja de entrada de los correos electrónicos de los cibernautas y la carnada sería un e-mail enviado aparentemente por una entidad financiera. Así entonces, las personas al revisar sus cuentas de correo y encontrar un e-mail de

alguna entidad financiera donde ellos tienen cuenta, "morderían" el anzuelo y revelarían su información personal.

4.3 Historia del Phishing

"La primera mención del término phishing data de enero de 1996 en un grupo de noticias de hackers alt.2600, aunque el término apareció tempranamente en la edición impresa del boletín de noticias hacker "2600 Magazine".

El término phishing fue adoptado por crackers que intentaban "pescar" cuentas de miembros de AOL". Las personas que se dedican al phishing son conocidas con el nombre de phishers (pescadores). Estos individuos tienen como función principal el envío de correos electrónicos a diferentes personas. Para poder lograr que las personas crean que el correo que reciben es de un remitente confiable, los phishers deben de hacerse pasar por entidades financieras que sean reconocidas en el medio. Los ataques de phishing están creciendo con gran rapidez y por esta razón es que se ha hecho necesario tomar medidas de seguridad contra estos ataques. Existen leyes en la actualidad que penalizan esta modalidad de robo. Por otra parte se han encontrado nuevas variantes para realizar el phishing, como lo es el robo de información por medio del teléfono.

4.4 Evolución del Phishing

Como se mencionó anteriormente, el inicio del Phishing se dio al ser mencionado por primera vez en un grupo de noticias de hackers. Entonces desde

esa época fue que se dio el nacimiento de la nueva modalidad de robo, también conocida como phishing.

El primer intento de phishing, como también se mencionó, se dio cuando un grupo de ckrackers querían robar algunas cuentas de miembros de AOL. Después de eso, es muy difícil decir un número exacto de casos reportados por personas que hayan sido víctimas de phishing.

Existen dos clases de phishing, el tradicional y el complejo. El primero es aquel que se envía de manera masiva a los diferentes buzones de correo electrónico de personas escogidas al azar. Lo anterior hace que el detectar estos correos se pueda realizar de manera más rápida. Por otro lado, esta clase de phishing tiene elementos muy visibles que hacen que las personas sepan identificar cuando los correos son fraudulentos o no.

Actualmente en el mundo entero existen entidades y empresas que son conocidas y que tienen la facilidad de identificar cuando un sitio Web es o no auténticos. Con base en la información anterior, se afirma que estos incidentes no trascienden; además se tiene que los ataques mostrados en estadísticas nunca serán los reales.

Entre las medidas preventivas, a las personas que navegan en Internet se les da una serie de indicaciones como no dar su información personal en correos electrónicos que les llegue a sus bandejas de entrada; dentro de ésta información personal están las contraseñas, usuarios, números de tarjetas de crédito, entre otras. Por otro lado, los usuarios deberán estar alerta cuando entren a sitios Web

de entidades financieras y cerciorarse de la existencia de dos detalles muy importantes, el primero es fijarse si la dirección o URL esta antecedida por una ´s´ que indica que es página segura, así: https://. Y lo segundo a tener en cuenta es verificar la existencia de un candado en la parte inferior derecha de sus pantallas, el cual advierte que la página es segura.

Toda la información descrita anteriormente demuestra que el la clase de phishing tradicional es una forma un poco primitiva pero que igual es peligrosa y es de suma importancia para la seguridad de los cibernautas. En la actualidad no hay cifras reales de pérdida monetaria a causa del phishing ni del número de personas afectadas por esta modalidad. Lo anterior también muestra que esta actividad es muy rentable para los phishers adquirir dinero de manera "fácil".

Por otro lado hay que mirar éste problema de phishing desde el punto de vista no del usuario, sino de las diferentes entidades bancarias a las cuales les plagian sus páginas en Internet para robar dinero. A pesar de ser éste otro contexto, las consecuencias son iguales o peor de devastadoras. Para una empresa y más para una entidad financiera, lo primordial es conservar el good will y si tomamos aquellos casos en los que los phishers lograron su acometida será ahí donde la buena imagen de las empresas decaería.

Haciendo alusión a la parte técnica que esta relacionada con éste tema del phishing, es fundamental mencionar que para que los ataques de phishers disminuyan notoriamente es necesario combatir directamente con el talón de Aquiles de éste tema, el cual es la integridad del sistema del usuario. Dentro del

tema de seguridad, las empresas desarrolladoras de antivirus juegan un papel muy importante, ya que estas cuentan con personal capacitado técnicamente y un software de seguridad que está muy bien probado y la implantación del mismo ha sido exitosa. A pesar de lo anterior estas empresas no se libran de los ataques de phishing.

Por otro lado hay que tener en cuenta que el sistema operativo del navegador tiene mucho que ver a la hora de hablar de phishing. Esto se debe a que los hackers constantemente están documentándose e informándose para crear ataques más potentes y así encuentran debilidades o vulnerabilidades del software que se puedan explotar.

4.4 Ataques recientes

En general, los últimos ataques de phishing han sido reportados desde páginas de Internet habilitadas para realizar pagos y por clientes de entidades financieras. También se ha encontrado que últimamente páginas de carácter social han sido víctimas de ataques de phishing debido al gran contenido de información personal de diferentes personas que frecuentan el sitio13. "Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques". Un ejemplo muy peculiar se dio a finales del año 2006, en el cual un gusano informático tomo posesión de varias de las páginas de MySpace, un sitio muy conocido y de gran concurrencia. Los phishers lograron hacer que los enlaces de éste sitio Web se

dirigieran a otra página diferente pero con una apariencia igual o muy similar a la original.

4.5 Tipos de phishing

4.5.1 Según el servicio que ataquen:

Bancos y cajas

Aquí el objetivo es robar el pin secreto, el número de tarjeta de crédito y datos análogos con el fin de lucrarse económicamente. Al poseer el atacante estos datos puede utilizarlos para realizar transferencias a otra cuenta, realizar compras y pagos por internet, retirar dinero de la cuenta. Consecuencia de esto es una gran pérdida económica para la víctima. Las excusas utilizadas son varias: a la posible víctima se le envía un correo con un enlace donde se le solicitan los datos porque su cuenta bancaria fue bloqueada por motivos de seguridad, o por un cambio de normativa en el banco, por ejemplo. Los bancos más conocidos que han sido falsificados son ING Direct, Bankia, Banco Popular.

Pasarelas de pago online

La intención es igual que cuando se habla de bancos, obtener los datos bancarios. Las excusas que utilizan los estafadores son varias, por ejemplo que se produjo un cierre de sesión del usuario incorrecto o que se detectó una posible

intrusión en sus sistemas de seguridad. Las empresas a las cuales afectan son Paypal y Mastercard.

Redes sociales

Aquí lo que se pretende es claro: suplantar la identidad u obtener información sensible y privada del usuario de redes sociales. Las redes afectadas más comunes son Facebook, Twitter, Tuenti, Instagram. El método empleado aquí es comunicarle a la víctima que se le etiqueto en una foto, o que alguien le envía una solicitud de amistad, o por motivos de seguridad es necesario que envié sus claves. Este tipo de Phishing es cada vez más utilizado porque hoy en día las personas se comunican por este tipo de redes, el uso de las mismas va aumentando y cada vez es más común que sufran estos ataques. En la actualidad lo raro no es ser usuario de la red social, al contrario, es no serlo. Por tanto, el aumento del uso de las mismas hace que sea un blanco fácil para los Phishers.

Páginas de compra/venta y subastas

La pretensión del estafador en este tipo de phishing es obtener las cuentas de usuario de las víctimas y estafar económicamente al mismo. Las excusas típicas utilizadas para captar la atención del usuario son que se observan movimientos sospechosos, problemas con la cuenta de usuario. Las empresas que sufren estos ataques son Amazon o EBay. Hay que tener en cuenta que

actualmente las personas utilizan cada vez más este tipo de servicios para la compra venta. Antes no era un punto de atención de los phishers porque el uso de estas redes no estaba extendido. Hoy en día, el uso de las mismas es bastante extenso.

Juegos online

En este medio los motivos son varios: robar la identidad, robar los datos bancarios, los datos privados y suplantación de identidad. Los juegos online comunes suplantados por ejemplo es el World Warcraft. Las excusas son parecidas a las anteriores. Todas destinadas a engañar al usuario.

Soporte técnico y de ayuda de empresas y servicio

Un ejemplo muy común es el phishing a Apple. Aquí el objetivo es robar la cuenta al usuario, por ejemplo el ID del AppStore para poder hacer compras con la identidad y cuenta bancaria de otra persona. Se suelen suplantar empresas como Outlook, Gmail, etc.

Almacenamiento en la nube

Las empresas que ofrecen este servicio de almacenamiento son Google Drive, Dropbox. Lo que se pretende conseguir son los datos privados, documentos, fotografías que el usuario almaceno en estas páginas web. Una vez obtenidos estos datos, el estafador puede cometer varios delitos relacionados.

Servicios o empresas públicas

Es un tipo de Phishing que simula ser por ejemplo, la policía nacional, o la Agencia Tributaria y por esto su riesgo. El phisher intenta infectar el ordenador de la persona y así obtener los distintos datos para su beneficio. Una de las excusas utilizadas más comunes, es cuando intentan avisar al usuario de una posible multa y es necesario obtener sus datos.

Servicios de mensajería

Esta estafa es menos común. Aquí se utilizan empresas proveedoras de correo y mensajería para efectuar el phishing y así conseguir información privada del usuario. Por ejemplo la víctima recibe un email de la empresa DHL informándole que ha recibido un paquete y le solicita sus datos.

Falsas ofertas de empleo

Aquí hay diferentes tipos de oferta falsa que implican phishing para engañar al usuario y conseguir sus datos y a continuación usarlos con fines fraudulentos. Estas son:

- Trabajar desde casa haciendo tareas manuales: se piden sus datos y una cantidad de dinero para guardarle el puesto de trabajo.
- Oferta de trabajo, llama e infórmate: aquí se le pide a la víctima que llame a un determinado número de teléfono y aporte sus datos.

- ¡Empieza a trabajar! Solo tienes que aportar tus datos personales: muy fácil, la víctima ofrece fotografías de su documentación personal y ahí es cuando comenzarían a trabajar. Pero lo único que buscan es obtener información confidencial.
- Infórmate sobre un puesto de trabajo aquí: lo que hacen es poner un anuncio con un enlace ficticio. Cuando la víctima entra en ese enlace, se le instala malware o rellenan formularios con información susceptible.
- Transferencias bancarias: es el trabajo de mula o intermediario que utiliza el phishing bancario.

4.5.2 Según el Modus Operandi

Phishing engañoso- deceptive phishing

Esta sería la forma en la que se originó el phishing (AOL). Su procedimiento es sencillo: consiste en el envío masivo de correos electrónicos en donde se suplanta una identidad legítima. En este email se piden unos datos por medio de un enlace ficticio y manipulado. Los motivos utilizados para engañar al usuario son varios como la existencia de algún problema en la cuenta bancaria del usuario. La finalidad de esto es que la víctima ingrese sus datos en la página web a la cual dirige el enlace y así obtener esta información que luego puede ser utilizada por el phisher de forma fraudulenta, como realizar compras o suplantar la identidad.

Existen diferentes variantes sobre el phishing engañoso. Una de ellas es la instalación de software malicioso en el ordenador del usuario por medio de mensajes.

Hay unos rasgos comunes entre los tipos de phishing. El primero es la suplantación de sitios con buena reputación para así, conseguir la fiabilidad que necesitan. Otro rasgo es que utilizan la página web como cebo y utilizan todo tipo de artimañas para evitar ser descubiertos. Aquí se ve claramente como el phishing utiliza la ingeniería social, porque de algún modo u otro, necesita la "colaboración" de la víctima. Si esta no "cae" en la trampa, el ataque de phishing no tiene éxito alguno.

Dentro de este tipo de estafa también destacamos el "vishing" y el "smishing" Por su parte el Vishing es una forma de phishing que utiliza como herramienta principal el teléfono. Resulta muy rentable ya que las personas actualmente tienen plena confianza en el uso del mismo y porque las empresas legítimas también utilizan este medio. Esta técnica utiliza un software llamado "war dialeys" que desde un ordenador realiza las llamadas telefónicas. Cuando la víctima descuelga el teléfono se le intenta convencer de que visite una página web para que confirme sus datos o incluso le piden sus datos personales en la misma llamada.

El smishing por su parte, también es una técnica de phishing pero en este caso utiliza los SMS para que la víctima caiga en la trampa. El primer caso de este

estilo que se conoce fue en Pekín. A partir de este entonces el método ha ido evolucionado, donde en cada SMS se le avisa a la víctima que se le ha dado de alta en un servicio de pago y se le comunica que para darse de baja debe visitar determinada página web. Si la víctima accede a esta web se le instalara un software para capturar sus datos. El problema que se observa de este método es su elevado coste, aunque se conoce algún caso donde los estafadores hacen que el SMS corra a cargo de otra persona. Esto es un indicio de cómo se está haciendo cada vez más común su uso.

Sofware malicioso- malware based phishing

Este tipo de estafa implica la instalación de software malicioso en el ordenador de la víctima. Su propagación depende tanto de la ingeniería social y de la explotación de la vulnerabilidad del sistema. En el primer caso se necesita la acción de la víctima para que el ataque pueda dar lugar, por ejemplo que abra el archivo adjunto de algún correo electrónico y así el malware se le pueda instalar en el ordenador. En el segundo de los casos, el usuario tiene muy poca implicación. Es decir, aunque en muchas ocasiones es por parte del usuario la instalación de un malware, en muchos otros casos se pueden instalar debido a algún fallo en el sistema de seguridad del equipo.

Independientemente de cual sea el método utilizado hay diferentes técnicas y utilización de diferentes programas para conseguir el robo de datos. Estos son:

- Key-loggers y Screen-loggers: los key-loggers son programas que se utilizan para grabar y registrar las pulsaciones que se hacen en el teclado. Esto suele ponerse en marcha cuando el usuario ingrese en una página web que este registrada en este programa, tales como entidades bancarias. A partir de ese momento, el programa graba todo lo que se teclea en el ordenador y lo envía al phisher. Esto ha evolucionado tanto que incluso a veces graban los movimientos que se realizan con el ratón. Los screen-loggers por su parte, tienen la misma función pero capturan imágenes que luego envían al atacante.
- Secuestradores de sesión (session hijackers): estas aplicaciones actúan cuando el usuario ha accedido alguna vez a alguna web registrada por el software. O sea que no roba datos, sino que su actuación comienza cuando la víctima ya ha accedido a su cuenta. Esto se puede realizar instalando el software malicioso en el ordenador del usuario o mediante la técnica "men in the middle".
- Troyanos web: los troyanos son programas maliciosos que aparecen en forma de ventanas emergentes inesperadamente sobre la pantalla de validación de páginas web legítimas, con el fin de obtener datos privados. Lo importante aquí es que hacen creer al usuario que están

en una web legítima pero realmente no es así y estos por tanto introducen sus datos. Esta información se le envía al phisher.

- Ataques de re configuración de sistema (system reconfiguration attacks): este tipo de estafa se realiza a través de la modificación de los parámetros de configuración del ordenador de la víctima. Una de las técnicas es modificar el nombre de dominio. Otra forma es la instalación de proxys a través del cual se canaliza tanto la información que entra como la que sale. Esta técnica también es conocida como "men in the middle".
- Robo de datos (Data theft): por otra parte es importante también hablar de la existencia de códigos maliciosos que se instalan en el ordenador y su finalidad es enviar esta información que recaban al atacante.

DNS o "pharming"

Aquí se incluyen las técnicas que se basan en la interferencia del proceso de búsqueda del nombre de dominio. Esta es una de las técnicas de mayor peligro porque tienen poca colaboración del usuario y parece todo más real.

Introducción de contenidos- content injection phishing

Esta técnica consiste en introducir contenido malicioso en un sitio web legítimo. Esto puede hacerse mediante diferentes modalidades como redirigir al

usuario a otra página web o la instalación de algún tipo de malware en el ordenador. Dentro de esta técnica hay tres modalidades:

- Asaltar al servidor legítimo que aprovechan cualquier vulnerabilidad.
- Introducción de contenido maliciosos al sitio web legítimo mediante lo que se conoce como "cross site scripting". Aquí se aprovecha alguna vulnerabilidad para introducir datos sin ningún tipo de validación.
- Aprovechamiento de una vulnerabilidad SQL. Así consiguen la provocación de la ejecución de comandos de bases de datos de un servidor remoto que conlleve la filtración de datos privados y confidenciales. Se produce por una ausencia de los filtros adecuados, igual que en el caso anterior.

Técnica del intermediario - man in the middle phishing

Se encuentra muchas veces introducido como un tipo de phishing pero en verdad es una técnica más. Aquí el phisher se posiciona entre el ordenador del usuario y el sitio web legítimo. Así puede leer, modificar y obtener la información que entra y sale del ordenador. Puede obtener todos los datos que desee con el fin de robar cuentas bancarias o el secuestro de la sesión.

Motor de búsqueda- search engine phishing

Es como en el caso anterior, un tipo de técnica utilizada por los phishers que consiste en la creación de páginas web donde se ofrecen servicios o productos falsos. Las introducen en los índices de los motores de búsqueda y

una vez que el usuario realiza algún tipo de compra, está proporcionando información privada. Normalmente este tipo de ofertas, tienen precios muy buenos y muy bajos para que los usuarios de internet caigan en la trampa más fácilmente.

Lavado de dinero producto del phishing

Otra forma de realizar el phishing indirectamente es a través de las "mulas", que son aquellas personas que participan en los ataques de phishing, muchas veces sin tener conocimiento. Un ejemplo de esto y que se ha dado a conocer en estos días, es el del sinnúmero de ofertas que a diario se observan solicitando personas para trabajar desde la comodidad de su casa. Para poder ser contratado en este tipo de trabajos es necesario llenar un formulario en el cual piden varios datos personales, entre ellos números de cuentas bancarias; con esta información es que los phishers se basan para realizar sus ataques. Éstos lo que hacen, es consignar la plata obtenida en alguno de sus ataques en las cuentas de estos "trabajadores" y así en caso de ser descubiertos no podrán ser encontrados por el número de cuenta. Los empleados de dicha empresa recibirán un porcentaje del dinero obtenido en el fraude como parte de pago por su trabajo.

CAPÍTULO QUINTO

5.1 Victima

De acuerdo a la definición brindada por la Organización de las Naciones Unidas, en el VI Congreso (Caracas 1980) y el VII Congreso (Hilan 1985), donde se planteó que el término "víctima", puede indicar que la persona ha sufrido una pérdida, daño o lesión, sea en su persona propiamente dicha, su propiedad o sus derechos humanos, como resultado de una conducta que:

a) Constituya una violación a la legalización penal nacional.

b) Constituya un delito bajo el derecho internacional, que constituya una violación a los principios sobre derechos humanos reconocidos internacionalmente.

c) Que alguna forma implique un abuso de poder por parte de personas que ocupan posiciones de autoridad política o económica.

5.2 Obligación de autoprotección

Sin ánimo de incurrir en reiteraciones innecesarias, y a pesar de que se ha hecho referencia en los epígrafes precedentes a la posición que ocupa la víctima del delito dentro de la mecánica defraudatoria, es preciso rememorar sucintamente cuál es la repercusión de su actuación y determinar qué grado de observancia le es exigible a efectos de protegerse frente a este tipo de amenazas informáticas.

Como se ha manifestado anteriormente, el engaño producido a través de la conducta típica se encuentra incardinado en la manipulación informática a través de la que se pretenden conseguir los datos bancarios de la víctima; no obstante, a través de dicha adulteración el phisher le envía un mecanismo de acceso a ellos que se encuentra camuflado por un aura de confiabilidad, y a través de cuya activación aquélla dará la clave de acceso a sus datos. Cabe recordar que el sujeto de los inmersos en la trama que recibe el título de "víctima" es el que sufre el detrimento patrimonial consecuencia de la maquinación fraudulenta.

Lo analizado previamente respecto al elemento subjetivo de los delitos de estafa informática, blanqueo de capitales y receptación cometidos por el mulero bancario ofrece al analista un punto de partida sólido para estudiar el alcance de la conducta de la víctima desde el punto de vista del deber de cuidado propio frente a los ciberataques. En efecto, si atendemos a lo que sucede en el ring que suponen los procedimientos por estafa informática, un argumento recurrente por parte de las defensas de los investigados es el consagrado "deber de autoprotección", a través del que se pretende atribuir cierto grado de responsabilidad en los hechos a la víctima con fundamento en la imprudencia que ha mostrado al recibir el email o SMS sospechoso y fiarse de su contenido.

Lo cierto es que este razonamiento se encuentra justificado en los procedimientos donde resulta probado que el engaño contenido en la manipulación se puede calificar de "burdo" o "estúpido" -y, por tanto, inidóneo para

lograr el fin perseguido- atendiendo a múltiples factores o elementos que lo componen y que cualquier persona con un mínimo raciocinio puede apreciar. De esta manera, la credulidad de la víctima en estos supuestos puede ocasionar la atipicidad de la conducta. Pensemos en un email presuntamente remitido por una entidad pública española repleto de faltas de ortografía, en un castellano deficiente, encabezado por un signo distintivo de una institución de otro país y dirigido a una persona diferente de la receptora.

Por tanto, de tan gráficas palabras se puede extraer que los supuestos de engaño zafio constituyen la única excepción a la inexigibilidad de autotutela a la víctima.

Dejando de lado esta singularidad, y teniendo en cuenta que el autor del delito de estafa informática actúa mediando dolo en su fuero interno y con el objetivo de que el engaño realizado produzca error en la víctima, la jurisprudencia ha declarado en numerosas ocasiones que el principio de confianza y de buena fe procesal no admite la realización de excepciones que desequilibren la posición de las partes, por lo que en ningún caso podrá cargarse a la víctima con una culpa que no ostenta. Por ello, la comprobación en el caso concreto de la idoneidad del fraude ex ante resultará fundamental para determinar si, de haber recurrido la víctima a una mínima comprobación de la fiabilidad del mensaje (sin recurrir a profesionales de la informática o a mecanismos únicamente al alcance de los mismos), podría haberse evitado la consumación del engaño.

5.3 Impacto

Impacto social

Los delitos cibernéticos y el phishing en particular afectan a la confianza de los usuarios al realizar operaciones en internet, sobre todo en transferencias o transacciones. Al ser un fenómeno en aumento, al igual que la tecnología, pero ambos aumentan a la misma velocidad y por tanto la confianza de los usuarios de internet para realizar diferentes operaciones va disminuyendo. El miedo de ser una víctima de phishing se nota sobre todo en las plataformas de compra y venta online, donde vez más personas tienen menos fiabilidad a los sistemas de seguridad en la red.

Además por otra parte, la desconfianza que crea en los usuarios que una empresa sea suplantada frena el uso de las mismas plataformas. La pérdida de seguridad de los usuarios en una empresa le causa perjuicios ya que su imagen pública se ve dañada y por tanto, cada vez menos usuarios confiaran en ellas.

Un dato importante obtenido mediante estudios de instituciones dedicadas a la prevención del phishing, es que el 82% de estos ataques son realizados para obtener datos bancarios. Mientras que el 21,5% corresponde a ataques para conocer datos sobre empresas de compra y venta online.

Impacto económico

Es importante saber que ya que estamos hablando de un delito relativamente nuevo, hay pocas estadísticas sobre su impacto, si bien se puede

decir que por cada fraude exitoso, la pérdida económica a nivel mundial tiene una media de 593€. En España estos fraudes no tienen tanto beneficio, siendo la media inferior a los 400€. Esto es así por un motivo: según el código penal español, para que una estafa pueda ser concebida como un delito, lo defraudado debe superar los 400€, en caso contrario, se estaría hablando de una falta. Por tanto, a los estafadores les es más rentable cometer más ataques phishing de menor ganancia económica pero que sea constitutivo de falta y no de delito.

En EE.UU, un estudio determina que las pérdidas económicas por este delito son mayores que cualquier otro tipo de fraude, rozando los 1,5 millones de dólares, mientras que por otros delitos son pérdidas que rondan los 2400 dólares. Por tanto llegamos a la conclusión de que a pesar de que los ataques por virus son más dañinos porque llegan a una colectividad mayor, el impacto económico por phishing es considerablemente mayor.

En nuestro país, el impacto también es bastante considerable. Desgraciadamente no existen datos de agencias gubernamentales que sustenten esta hipótesis, más que la experiencia de los agentes del Ministerio Público que trabajan con éstos casos; pese a que cada caso particular no tiene una gran ganancia, si se multiplica la ganancia de cada uno con todos aquellos realizados al año, se puede entender la dimensión del problema.

5.4 Dificultad probatoria

Como se ha manifestado a lo largo del estudio objeto del trabajo, a pesar de que la naturaleza de los delitos mal llamados "informáticos" no presente novedades respecto a su concepción original, la vía empleada para su comisión posee características propias que dotan también de singularidad a su investigación con respecto a los tipos restantes. Así, es innegable que desde que los seres humanos realizamos un uso universalizado de Internet hemos desarrollado la capacidad de requerir inmediatez a las tareas más sencillas como consecuencia de las prestaciones que este medio nos ofrece, tales como comunicarnos, desarrollar prestaciones laborales o recibir la compra en casa en menos de 24 h. Esta celeridad no es desconocida por los crackers, que, como sujetos especialmente cualificados y conocedores de las posibilidades de la Red, sacan rendimiento de ellas utilizándolas para dificultar el descubrimiento de su identidad y la consecuente imputación del hecho delictivo que han perpetrado a través de dicho mecanismo.

Con el fin de facilitar la comprensión de los inconvenientes experimentados en la investigación de estos delitos, su estudio se dividirá en tres puntos: i) Divergencia espacio-temporal en la comisión del delito; ii) Objeto material de la indagación; y iii) Tareas de investigación en el proceso penal.

Divergencia espacio-temporal en la comisión del delito: el paralelismo espacio-temporal que concurre en los delitos consumados a través de la

presencialidad resulta, en muchas ocasiones, inútil para efectuar el juicio de imputabilidad en el proceso penal por delitos informáticos. En efecto, Internet ha posibilitado que, por ejemplo, una persona pueda acceder a los archivos almacenados en su ordenador a través de un dispositivo diferente y desde un rincón lejano del Mundo. Esto es posible como consecuencia de la invención de programas, aplicaciones y opciones integradas en las funcionalidades de los equipos informáticos (muchos de ellos disponibles para su descarga gratuita) que resultan tremendamente útiles en entornos de trabajo competitivos. Sin embargo, estas herramientas encuentran su antítesis en el malware, que, configurado en algunas de sus modalidades, también ofrece acceso a un sistema y a sus archivos con fines radicalmente distintos a los anteriores. La tecnología también presenta la posibilidad de programar tareas en nuestro equipo que serán ejecutadas por el sistema en la fecha y hora que planifiquemos, lo que, en el proceder de un ciberdelincuente, puede constituir un medio impeditivo del descubrimiento de su identidad y de la técnica que ha utilizado para apropiarse de los datos o patrimonio de la víctima, ya que cuando los hechos acometidos por él comiencen a ser investigados en el seno de un procedimiento penal es muy probable que haya desplegado una multiplicidad de acciones para evitar que eso suceda.

Por tanto, la Red excluye de plano la concepción física de los parámetros "tiempo" y "espacio" en los delitos que nos ocupan, creando en su lugar una dimensión codificada a través de conexiones invisibles (coloquialmente conocida como

"ciberespacio") mediante la que los sistemas que la componen interaccionan por orden de los usuarios, y en la que los phishers podrán atacar a otros usuarios desde espacios físicos diferentes (mención especial a la transnacionalidad) e incluso en tiempos dispares. Asimismo, éstos disponen de técnicas de las que se sirven para ocultar las pruebas de su proceder y procurar el mantenimiento de su anonimato, en su mayoría orquestadas mediante la manipulación del software empleado para efectuar el ataque.

Objeto material de la indagación: lo expuesto respecto a la dicotomía espacio-temporal del ciberespacio es asumible también para el objeto de su tráfico, aunque con los matices inherentes a su naturaleza. Obsérvese que los datos objeto de tratamiento en las operaciones informáticas no son tangibles, sino que el soporte físico ha sido sustituido por el magnético con las contingencias que ello conlleva en las tareas de investigación: sirva como ejemplo la dificultad de comprobar la validez y veracidad de los documentos electrónicos. Como se ha expuesto en el anterior punto, de esta inmaterialidad deriva la volatilidad de estos datos y la que el phisher desee otorgarles a través de la acción dirigida a auto encubrirse.

En definitiva, resulta primordial para el perjudicado asegurar que el testimonio del delito por el que se ha visto afectado perdure en el tiempo a través de la recopilación de pruebas para hacer valer su derecho en un procedimiento penal posterior. En este sentido, será fundamental que se sirva de un documento gráfico

en el que conste el contenido del email completo a través del que el phisher ha orquestado su manipulación psicológica y el resultado de la carga del enlace adjunto (en caso de redirigir a una web falsa), así como los documentos (bancarios, de identidad) que demuestren que los datos utilizados por el ciberdelincuente para realizar el desapoderamiento patrimonial le pertenecen. También es recomendable recurrir al encargo de una pericial informática lo antes posible tras el ciberataque (para evitar la potencial eliminación de pruebas), que será efectuada por un equipo de titulados expertos que autenticarán su efectiva consecución, determinarán los medios que el phisher ha empleado, y que podrá ser aportada como prueba preconstituida en el proceso penal.

Tareas de investigación en el proceso penal: tras la denuncia del perjudicado, que apertura el correspondiente atestado, se inicia la fase de investigación policial en la que varios agentes designados al efecto llevarán a cabo la recopilación de evidencias probatorias al objeto de remitirlas al Juzgado de Instrucción a quien por reparto corresponda conocer del asunto. Uno de los cometidos de mayor relevancia de la investigación policial es apreciar, tras el examen previo de los datos aportados o extraídos de la misma, la necesidad de oficiar un mandamiento al proveedor de servicios de Internet del que el presunto cracker se ha servido para efectuar el ataque al objeto de que facilite la dirección "IP" (siglas de Internet Protocol Address) desde la que éste ha tenido lugar. La solicitud de realización del mandamiento debe remitirse al Juez o Magistrado

encargado de la instrucción del procedimiento, que decidirá sobre la idoneidad de la práctica de la prueba. En este punto es necesario recordar la volatilidad de los datos informáticos, si bien los proveedores de servicios tienen la posibilidad de conservar unos ficheros históricos o log en los que se almacenan de manera automática y secuencial los de todas las conexiones realizadas a través del servicio que ofrecen; la existencia de estos registros posibilita la identificación de las "IPs" intervinientes en el tráfico y su geolocalización, referencia que será de suma utilidad en el proceso. No obstante, existen voces discordantes respecto al valimiento de este medio de prueba para identificar al phisher, siendo más partidarias de sustituirlo por un mandamiento judicial a través del que se requiera al proveedor de servicios para que conserve esos ficheros en tanto el procedimiento penal se encuentre abierto. Para seguir el curso de una instrucción menos engorrosa, lo cierto es que ambos mandamientos son compatibles e, incluso, experimentan una relación de necesidad mutua, en tanto existe un riesgo de borrado de la información que haría inviable la determinación de la IP interviniente.

Una vez determinada la IP desde la que ha operado el sujeto activo del delito, el instructor podrá decidir mediante Auto motivado, en razón del principio de idoneidad, librar un mandamiento a la compañía telefónica -habitualmente a petición de la Policía Judicial- para que haga constar los datos del abonado, es decir, el domicilio donde se encuentra instalada, los datos del titular de la conexión

a Internet y de la línea telefónica utilizada, así como los datos técnicos asociados a dicha conexión.

Sin embargo, es posible que nos encontremos ante uno de los supuestos en los que el ciberdelincuente ha procedido desde una red pública, en cuyo caso el mandamiento será devuelto por la compañía significando que la dirección es una "IP NAT"; en estos casos, para identificar cuál es la conexión con más probabilidades de corresponder al phisher deberá atenderse al puerto de acceso o salida de la red o a las horas coincidentes con los hechos denunciados.

En definitiva, todas estas diligencias de investigación podrán ser apoyadas, dependiendo de la complejidad del procedimiento y de la necesidad de su práctica, con la adopción de medidas tales como la entrada y registro en el domicilio del cracker identificado para el precinto de dispositivos -junto con los documentos físicos que apoyan su funcionamiento- y volcado de los datos contenidos en ellos, las intervenciones telefónicas, las labores de vigilancia policial ordinaria y la localización y destino final de los fondos sustraídos (tarea complicada en los asuntos de componente internacional, habida cuenta que, en estos casos, el phisher acostumbra a afincarse en Estados que carecen de instrumentos de cooperación judicial internacional con México).

A pesar de la exigencia de conocimientos que implica la instrucción de un procedimiento incoado por la presunta comisión de un delito cometido a través de las TIC, lo cierto es que las estadísticas arrojan datos que evidencian que la

mayoría de Jueces y Magistrados acusan una gran ignorancia en estas lides, que les aboca a la dependencia informativa de las manifestaciones vertidas en los informes emitidos por las unidades especiales de investigación tecnológica a petición propia, o a los realizados por el representante del Ministerio Público en el curso del procedimiento. Es preciso mencionar que este colectivo desarrolla sus funciones en un entorno en el que concurren una gran cantidad de trabajo y poco tiempo para desarrollarlo y en donde la mayoría refiere tener al menos un ordenador con Internet en su domicilio y utilizarlo para fines corrientes, lo que, en plena era cibernética hace necesaria la instauración e implementación de una formación tecnológica de calidad y gratuita a cargo del Estado a través del Poder Judicial que exceda de las labores propias del cargo. Solo de esta manera se podrán complementar los conocimientos jurídico-técnicos de Jueces y Magistrados con el fin de facilitarles la comprensión de la comisión de los delitos informáticos y guiar su proceder en la investigación de los mismos.

Asimismo, es de destacar la redacción de la LECrim como una de las principales culpables de la desadaptación de la Justicia para la instrucción y enjuiciamiento de estos delitos, toda vez que presenta una evidente desconexión de la realidad social actual, y, por ende, no ofrece los instrumentos adecuados y adaptados a las peculiaridades antes manifestadas para que el procedimiento llegue a buen puerto.

5.5 Derecho comparado: legislación Española

En el Código Penal Español no existe una regulación específica para los delitos informáticos. Aun así, podemos encontrar tipificaciones dentro de los siguientes apartados:

5.5.1 Delitos de naturaleza económica

Estos son los que afectan patrimonialmente a una persona, o le causan algún perjuicio económico. Aquí el delito más común, es la estafa informática. Está regulada en el artículo 248 del CP y diferencia dos tipos: los que utilizan ingeniería social pura y los que utilizan un código malicioso (malware) o de intrusión en sistemas de información. El primero es donde incluiríamos el Phishing.

Además se establece también una pena para los daños informáticos, reflejados en el artículo 264.2 del CP.

No solo se encuentran tipificaciones para el phishing, sino que a lo largo del código penal encontramos que también se castiga el delito contra la propiedad intelectual, delitos de empresa. Un delito que nos interesa es el de falsedades documentales (en este caso falsificación de soporte informático) para prestar apoyo a las diferentes transacciones económicas.

Por otro lado, el spam también está penado por nuestro código penal. Aquí también cabe el phishing o el fraude nigeriano cuando el spam tiene como

finalidad el fraude u otros fines delictivos, como dañar la reputación de una persona.

Situándonos en este delito (spam) y la relación con el phishing se puede decir que hay una relación directa porque el enviar correos masivos de forma fraudulenta puede ser una forma de captación bastante eficiente. Un dato importante es conocer que el porcentaje de correo electrónico no deseado que utiliza el phishing es bastante bajo en comparación de los otros fines del spam.

5.5.2 Reforma al Código Penal

El 30 de marzo del 2015 se publicó en el BOE una nueva reforma del código penal español que afecta a los delitos informáticos, entre muchas otras cosas. Este tema es de interés ya que, como se dijo a lo largo del documento, el phishing es uno de estos delitos. Esta reforma que afecta directamente al phishing, es la modificación del artículo 197, en sus apartados 1 y 2 y los nuevos artículos implementados 197 bis y ter, dónde se tipifica el black hacking, craking y técnicas de acceso no consentido. En estos se castiga la producción y la adquisición para el uso, importe o facilitación a terceros, programas informáticos para cometer delitos con ellos, y que además proporcione contraseñas de ordenador o códigos de acceso. El espionaje es también añadido a esta sección al igual que el sabotaje.

5.5.3 Legislación aplicable a delitos informáticos

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE).
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. (Directiva sobre la privacidad y las comunicaciones electrónicas):
- Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
- Constitución Española de 1978 en su artículo 18. 4 donde se establece que "La Ley limitará el uso de la informática para garantizar el honor y la

intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Propia Imagen.
- Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y Comercio (LSSI-CE).

5.5.4 Unidades de persecución del phishing

Como hemos visto, el phishing y en general los delitos informáticos están en continua evolución. Hoy en día las denuncias contra estos delitos son una gran mayoría y cada día son más las víctimas de estos delitos. Por tanto, hubo la necesidad de crear cuerpos especializados en estos temas para conseguir disminuir el número de ataques en la red y que los usuarios puedan navegar con mayor tranquilidad. No es un trabajo fácil. Se necesita de tiempo y sobretodo colaboración entre las diferentes unidades para compartir información y así actuar conjuntamente. A lo largo de los años se han ido creando cuerpos especiales tanto a nivel nacional como internacional. Los delitos informáticos no son un problema que solo ocurre en España, sino que es un tema grave a nivel mundial. La gran mayoría de los países tienen medios adecuados para erradicar estos delitos y una de las mejores opciones es trabajar con otros países en conjunto. A continuación se señalan los grupos especializados tanto a nivel nacional como internacional:

Nivel nacional

Brigada de investigación tecnológica de la Policía Nacional: se trata de una unidad especializada del cuerpo nacional de policía donde se investiga el delito, el delincuente y las diferentes pruebas para valorarlas y ponerlas a disposición judicial. Por tanto se necesita una información constantemente actualizada y que diferentes instituciones colaboren con ella para obtener estos datos. Por ejemplo, colabora con policías de otros países. Su ámbito de actuación se basa en todo tipo de delito informático.

Grupo de delitos telemáticos de la Guardia Civil: esta unidad no es nueva, sino que existe hace varios años. Su base consiste en la investigación de delitos que utilizan la red para llevarse a cabo. Tal y como avanzan las medidas para evitar la comisión de estos delitos, también avanza la tecnología y era necesario un grupo especializado que investigara cada tipo de delito individualmente y creara formas y medios para prevenirlo y combatirlo. Ofrece consejos para los usuarios de internet y advierte de todas las formas delictivas conocidas hasta el momento. Una de sus grandes mejoras es que facilitan un enlace para que las víctimas de estos fraudes puedan denunciar de forma directa.

Policías autonómicas: tanto los Mossos d'escuadra como la Ertzaina tienen cuerpos especializados en estos delitos.

Agencia Española de Protección de Datos: su función principal es velar porque se cumpla la Ley Orgánica De Protección de Datos de carácter personal.

Nivel internacional

EUROPOL: es una organización europea que pretende la colaboración de todos los países miembros de la unión para prevenir y luchar contra el crimen informático. Actúa por medio de los ELOs, recopilando información sobre los diferentes delitos e intercambiándola entre los diferentes países. Además crea análisis y estadísticas de los delitos para que todos los países miembros sean conocedores de ellos.

INTERPOL: esta unidad por su parte, creó 4 grupos especializados en delitos informáticos y su finalidad es estar al corriente de todas las actualizaciones y avances de estos fraudes.

G-8: es un grupo integrado por los países más ricos del mundo que crearon a su vez un subgrupo sobre delitos de alta tecnología. Aquí se muestran diferentes protocolos de participación de los países y diferentes colaboraciones con empresas privadas para la evitación de estos delitos.

CONCLUSIÓN

Única. El avance de la tecnología y los medios de comunicación ha traído consigo grandiosos beneficios a la sociedad, mismos que facilitan la realización de actividades cotidianas y que es muy favorable en muchos aspectos en la vida de una persona. Sin embargo, estos avances también facilitan que individuos carentes de todo sentido de moralidad busquen como cometer ilícitos y que por consiguiente algunos de los delitos comunes se trasladen a las redes, incluyendo el phishing.

Existen diversos tipos de esta estafa, que se realizan a través de diversos medios y cobra relevancia en los últimos años por el incremento en el uso de internet, abriéndose las puertas para que éste delito se cometa por dicho medio. Por lo anterior, la evolución tecnológica atrajo consigo ventajas como desventajas, y es que en internet y en la red se producen casi tantos delitos como en la vida real. Incluso muchos de ellos con mayores pérdidas económicas, como en el caso descrito. Al no existir un marco jurídico que regule la posibilidad de evitar que se cometa el siniestro, genera desconfianza en los usuarios, empresas o instituciones y se promueve la poca fiabilidad en usar los medios electrónicos, lo que a su vez produce un freno en la evolución de la economía digital. Todos esos avances que se consiguieron, con delitos de este tipo se quedan paralizados.

Tras haber detallado detenidamente acerca de éste delito y su alza en la incidencia en nuestro Estado de Chihuahua, considero pertinente que el Congreso del Estado legisle en favor de hacer valer el Estado de Derecho y se castigue ejemplarmente a quienes realicen esta práctica y que éstos propongan los elementos que se deben integrar al marco jurídico chihuahuense, para hacer valer el derecho a la protección de datos personales y evitar el mal uso de los mismos en perjuicio de los individuos.

BIBLIOGRAFÍA

Abreu, José Luis. "El método de la investigación Research Method." *Daena: International Journal of Good Conscience* 9.3 (2014): 195-204.

Aguirre, Juan Carlos, and Luis Guillermo Jaramillo. "El papel de la descripción en la investigación cualitativa." *Cinta de moebio* 53 (2015): 175-189.

Albarrán Martínez, E. E. . "Delitos cibernéticos". Transregiones, n.º 2, junio de 2021, pp. 93-104, https://revistatransregiones.com/web/index.php/tr/article/view/18.

Basto García, Marver. "Estudio sobre la ingeniería social y su impacto en las entidades estatales.". Repositorio Institucional UNAD. Universidad Nacional Abierta y a Distancia. 2020. Web. 9 nov 2021 https://repository.unad.edu.co/handle/10596/34150

Ferrando, Manuel García. "5. La encuesta." (1996).

Gelormini, Alejandro A. El delito informático y su incidencia en la administración tributaria. Diss. Universidad de Buenos Aires. Facultad de Ciencias Económicas., 1998.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. "Guía para Titulares de los Datos Personales". INAI. 2018. Web. 9 de nov 2021 https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-01_PDF.pdf

Leiva, Renato Javier Jijena. "Dominios, marcas y comercio electrónico en internet: anexo: la nueva ley chilena sobre la no protección de datos personales, nº

19628 del 28 de agosto de 1999." Informática y derecho: Revista iberoamericana de derecho informático 30 (1999): 365-418.

Lima de Luz, María. "Criminalia N 1-6 Año L." Delitos Electrónicos. Ediciones Porrua. México (1984).

Márquez Tomás, Mónica. "Análisis del delito de usurpación de identidad en México (Estudios legislativos)." (2019).

Mayan, María, and Nota Introductoria. "Una introducción a los métodos cualitativos." *Módulo de entrenamiento para estudiantes y profesionales. Alberta: International Institute for Qualitative Methodology* 34 (2001).

Miembros del Consejo de Europa y otros Estados. (2001): "Convenio de Cyberdelincuencia". Budapest.

Moliner, María. "Diccionario de María Moliner." Edición Digital (1996).

Plascencia Villanueva, R. Teoría del Delito, Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México, Serie G, Estudios Doctrinales Número 192, México, 2004.

Do Nascimento Fernández, L. (2021). Phishing: aspectos técnicos y procesales del delito estrella en tiempos de pandemia.

Leguizamón, M. (2015). El phishing. junio 23, 2022, de Repositori Universitat Jaume I Sitio web: http://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizam%c3%b3n_Mayra.pdf?sequence=1&isAllowed=y

Salazar, N., Lalinde, J. G., Andrea, N., Aristizábal, S., Guillermo, J., & Pulido, L. (2007). PROYECTO DE GRADO "PHISHING: LA AUTOMATIZACIÓN DE LA INGENIERÍA SOCIAL" POR. Edu.co. Recuperado el 23 de junio de 2022, de https://repository.eafit.edu.co/bitstream/handle/10784/2443/Salazar_Natalia_2007.pdf?sequence=1&isAllowed=y

Damián, E., Ramírez, S., Yezyd, A. P., & Donoso Meisel, E. (s/f). *ESTUDIO DE LA EFECTIVIDAD DE ATAQUES DE PHISHING SENSIBLES AL CONTEXTO.* Edu.co. Recuperado el 25 de junio de 2022, de https://repositorio.uniandes.edu.co/bitstream/handle/1992/19174/u433133.pdf?sequence=1&isAllowed=y

De Flores Cáceres, C. F. (2017). El phishing como comportamiento penalmente relevante [Licenciatura en Derecho, Pontificia Universidad Católica de Valparaiso]. Repositorio Académico de la Pontificia Universidad Católica de Valparaiso. http://opac.pucv.cl/pucv_txt/txt-4000/UCC4478_01.pdf

Cesar Llanos. Tratamiento de fraude en Internet, Historia del phishing. Octubre 12 2005.