UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

ESTUDIO JURÍDICO DE LA FIGURA DEL PHISHING EN EL SISTEMA FINANCIERO MEXICANO.

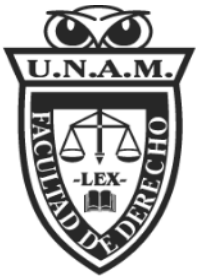
T E S I S

QUE PARA OPTAR POR EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A:

GEOVANNI TÉLLEZ ÁVILA
307286495



DIRECTOR DE TESIS:

DR. GERARDO RODRÍGUEZ BARAJAS.

CIUDAD DE MÉXICO, 2017

VNIVERSIDAD NACIONAL
AVTNOMA DE
MEXICO

FACULTAD DE DERECHO
SEMINARIO DE DERECHO MERCANTIL

. LIC. IVONNE RAMIREZ WENCE
DIRECTORA GENERAL DE LA ADMINISTRACION ESCOLAR
DE LA UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
P R E S E N T E.

El alumno: **GEOVANNI TELLEZ AVILA,** con número de cuenta: 307286495, realizó bajo la supervisión de este Seminario el trabajo titulado **"ESTUDIO JURIDICO DE LA FIGURA DEL PISHING EN EL SISTEMA FINANCIERO MEXICANO",** con la asesoría del DR. GERARDO RODRIGUEZ BARAJAS, que presentará como tesis para obtener el título de Licenciado en Derecho.

El mencionado asesor nos comunica que el trabajo realizado por dicho alumno reúne los requisitos reglamentarios aplicables, para los efectos de su aprobación formal.

En vista de lo anterior, comunico a usted que el trabajo de referencia puede ser sometido a la consideración del H. Jurado que habrá de calificarlo.

Por sesión del día 3 de febrero de 1998 del Consejo de Directores de Seminario se acordó incluir en el oficio de aprobación de tesis la siguiente leyenda que se hace del conocimiento del sustentante:

"El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad".

A t e n t a m e n t e,
"POR MI RAZA HABLARA EL ESPIRITU".
Ciudad Universitaria, a 07 de noviembre de 2017.

DR. ALBERTO FABIAN MONDRAGON PEDRERO.
DIRECTOR

c.c.p. Secretaría General de la Facultad de Derecho.
c.c.p. Archivo Seminario.
c.c.p. Alumno.
AFMP/*mrc.

ÍNDICE

ABREVIATURAS Y ACRÓNIMOS. IV
INTRODUCCIÓN..... VI

CAPITULO PRIMERO. DEL PHISING.

1.1 EVOLUCIÓN DE LAS TRANSACCIONES ECONÓMICAS Y SURGIMIENTO DEL PHISHING.....1
1.1.2. EVOLUCIÓN DE LAS TRANSACCIONES ECONÓMICAS. 1
1.1.3. SURGIMIENTO DEL PHISHING.....4
1.2.- ACEPCIONES DEL PHISHING Y CONCEPTO. 8
1.2.1. DEFINICIÓN ETIMOLÓGICA DEL PHISHING.....8
1.2.2. DEFINICIONES DE PHISHING.....9
1.2.3. DEL CONCEPTO DE PHISHING. 11
1.3.- CASOS MÁS COMUNES DE PHISHING. 13
1.4.- PHISHING Y DERECHO INFORMÁTICO. 31
1.5.- PHISHING Y DERECHO MERCANTIL.....38
1.6.- VULNERABILIDAD ANTE EL PHISHING DE LAS INSTITUCIONES FINANCIERAS.....40

CAPITULO SEGUNDO. REGULACIÓN DEL PHISHING EN MÉXICO Y EL MUNDO

2.1.- CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.....44
2.2.- CONVENIOS Y TRATADOS INTERNACIONALES.....49
2.3. LEGISLACIÓN FEDERAL.....55
2.3.1. LEY DE INSTITUCIONES DE CRÉDITO. 55
2.3.2. LEY GENERAL DE TÍTULOS Y OPERACIONES DE CRÉDITO. 60
2.3.3. CÓDIGO PENAL FEDERAL.....62
2.3.4. LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA.....64
2.3.5. LEY DE LA PROPIEDAD INDUSTRIAL. 67
2.4.- LEGISLACIÓN LOCAL. 70
2.5.- ANÁLISIS DE DERECHO COMPARADO DE LA FIGURA DE PHISHING CON RELACIÓN A MÉXICO. 74
2.5.1. ESTADOS UNIDOS DE AMÉRICA. 74
2.5.2. REPÚBLICA DE CHILE.....75
2.5.3. REPÚBLICA DE ARGENTINA. 77
2.5.4. ESPAÑA.....80

CAPITULO TERCERO. ASPECTOS Y CONSECUENCIAS JURÍDICAS DEL PHISHING.86

3.1.- SUPLANTACIÓN DE IDENTIDAD.....86
3.2.- ACCESO A INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES. 94

3.3.- SEGUROS DE PROTECCIÓN ANTI PHISHING. 102
3.4.- FRAUDE. 110
3.5.- LAVADO DE DINERO COMO CONSECUENCIA DEL PHISHING. 114

CAPITULO CUARTO. AFECTACIÓN ECONÓMICA AL SISTEMA FINANCIERO MEXICANO COMO CONSECUENCIA DEL PHISHING.

4.1.- REPERCUSIONES ECONÓMICAS DEL PHISHING. 123
4.2.- AFECTACIÓN A TARJETAHABIENTES O CUENTAHABIENTES. 129
4.3.- AFECTACIÓN A LAS INSTITUCIONES FINANCIERAS. 132
4.4.- AFECTACIÓN ECONÓMICA AL ESTADO. 136
4.5.- PROPUESTAS SOBRE MEDIDAS DE SEGURIDAD PARA EVITAR EL PHISHING. 141
4.5.1. ESTADO. 142
4.5.2. INSTITUCIONES FINANCIERAS. 146
4.5.3. CUENTAHABIENTES. 151

CONCLUSIONES. 153

FUENTES DE INVESTIGACIÓN. 158

BIBLIOGRAFÍA. 158
FUENTES ELECTRÓNICAS. 161
LEGISLACIÓN CONSULTADA. 165

ABREVIATURAS Y ACRÓNIMOS.

art. (s)	artículo, artículos
APWG	Antiphishing Working Group
cap. (s)	capítulo, capítulos
cfr.	Confrontar con, confróntese con
Col.	Colección
comp. (s)	compilador, compiladores, compilado por
CONDUSEF	Comisión Nacional para la Protección y Defensa de los Usua-
rios de los	Servicios Financieros
CNBV	Comisión Nacional Bancaria y de Valores
coord. (s)	coordinador, coordinadores, coordinado por
CPCol	Código Penal para el Estado de Colima
CPChi	Código Penal para el Estado de Chiapas
CPPDF	Código Penal Para el Distrito Federal
CPEUM	Constitución Política de los estados Unidos Mexicanos
CPF	Código Penal Federal
CSC	Convenio Sobre Ciberdelincuencia
DF	Distrito Federal
dir. (s)	director, directores, dirigido por
DOF	Diario Oficial de la Federación
ed. (s)	edición; editor, editores; editado por
et al.	*et alii:* y otros, y colaboradores
fig. (s)	figura, figuras
fracc. (s)	fracción, fracciones
frag. (s)	fragmento, fragmentos
HTML	*Hypertext Markup Lenguage*
HTTP	*Hypertexts and Links*
INACIPE	Instituto Nacional de Ciencias Penales
inc. (s)	inciso, incisos
inéd.	Inédito: no editado, no impreso, no publicado

infra	abajo, después [adverbio latino que remite a un contenido anotado posteriormente]
LIC	Ley de Instituciones del Crédito
LFPPIORPI	Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita
LPEA	Legislación Penal del Estado de Aguascalientes
loc. cit.	*loco citato.* en el lugar citado
núm.	Número, números, numeral, numerales
op. cit.	*opus citato:* obra citada
p., pp.	Página, páginas
párr. (s)	párrafo, párrafos
prgf. (s)	parágrafo, parágrafos
reimp.	Reimpresión, reimpreso por
rev.	Revisado por
s., ss.	Siguiente, siguientes
s. *d.*	*sin data:* sin fecha; sin dato de casa editora o de lugar
sec. (s)	sección, secciones
supra	arriba, antes [adverbio latino que remite a un contenido anotado anteriormente]
a.	tomo, tomos
tít. (s)	título, títulos
trad. (s)	traductor, traductores; traducido de, traducido por volumen, volúmenes

INTRODUCCIÓN.

Este trabajo de investigación tiene como finalidad hacer del conocimiento la importancia sobre la prevención, las medidas de seguridad y acciones que se deberán de implementar al realizar transacciones monetarias y bancarias utilizando los medios o plataformas digitales, con la misión de concientizar al público lector sobre los riesgos que existen en la web y con ello evitar ser víctima de los múltiples fraudes que se materializan con el uso de sistemas informáticos, para el caso concreto se estudiará la figura del “Phishing” y las repercusiones que proyecta en el sistema financiero mexicano mediante un análisis de la afectación patrimonial directa en sus partes integrantes, siendo éstas los clientes o usuarios de los servicios financieros, las instituciones financieras y el Estado como rector y protector del sano desarrollo de la economía en territorio nacional.

El dinero, principal medio de intercambio de la sociedad, a lo largo del tiempo ha sufrido distintas transformaciones en la forma de su circulación. La modernidad a través de sus múltiples avances tecnológicos han brindado día con día mayor seguridad en él flujo transacciones económicas que se realizan de manera cotidiana, por ejemplo en los elementos de seguridad que se incluyen en los billetes, transferencias directas a cuentas bancarias sin la necesidad de disponer del efectivo, inclusive la posibilidad de realizar pagos a través de smartphones que se encuentren vinculados a una cuenta bancaria evitando traer dinero físico en el bolsillo, entre muchas otras modalidades. A pesar de ello como en todo sistema pueden existir fallas o vulnerabilidad, situación que es bien aprovechada por algunas personas o corporaciones a efecto de obtener ganancias ilícitas, justo como sucede con la implementación de tecnología para la realización de transacciones monetarias.

En un inicio, en el trabajo propuesto se aborda la idea sobre el concepto de phishing, mediante el estudio de diversas hipótesis sobre su surgimiento y evolución, el análisis de múltiples definiciones propuestas por algunos doctrinarios y expertos, así como por entidades financieras con presencia en México y que son sensibles a este tema. Así mismo, se aborda el tema de las modalidades conocidas en las que se puede presentar esta práctica dando una breve explicación de cada una de ellas y la relación que existe entre el phishing con la ciencia jurídica utilizando como nexos principales el derecho mercantil y el derecho informático, recalcando la importancia en atender las vulnerabilidad con las que cuenta el sistema financiero mexicano a efecto de enfrentar cabalmente la implementación de tecnología y mitigar en lo posible los riesgos que conlleva la utilización de los medios tecnológicos.

Por lo anterior es de relevante importancia prestar atención en el desarrollo de las nuevas tecnologías ya que es un aspecto que no deja de lado al estudio de lo jurídico, que lamentablemente en nuestro país se encuentra de más rezagado tanto en doctrina, como legislación acerca de estos temas. De ahí surge la idea de enfocar este trabajo al estudio de la figura del “Phishing”, que si bien es tan solo un pequeño aspecto a estudiar, es de gran relevancia para la seguridad jurídica económica y patrimonial de quienes utilizan los medios electrónicos otorgados por una institución financiera como medio de ahorro o de disposición de efectivo, es por ello que en la segundo apartado de la investigación se realiza un análisis de las legislaciones Federales, Locales que podrían permitir en un futuro la implementación de medidas legislativas que conlleven el buen uso de los medios electrónicos en las transacciones monetarias. Además, se estudian ejemplos internacionales de como se ha abordado el tema en concreto y que puede ser una guía importante para estudiar el tema en México, así como la adopción y ratificación de ciertos tratados internacionales referentes al tema de la ciberseguridad.

En el tercer capítulo además de estudiar el caso en concreto de la figura del “Phishing” y sus múltiples fases mediante las cuales se compone este tipo de ataques, se abordarán temas de gran interés estrechamente relacionados con éste a

efecto de entender de manera integral su funcionamiento tales como: la regulación actual en el Estado Mexicano, su relación con el derecho informático y las instituciones financieras, protección de datos personales, suplantación de identidad, aspectos económicos de los delitos financieros y bancarios, el lavado de dinero como consecuencia del phishing, entre otros temas de relevancia jurídica.

Por último, se presentan datos e información relativas a la afectación económica del phishing en el sistema financiero mexicano y a sus partes integrantes, así como un análisis de las medidas a implementar para evitar este tipo de fraudes, proponiendo una serie de acciones que podrían ser viables para el Estado Mexicano y las autoridades reguladoras del sistema financiero, con la primordial finalidad de prevenir la comisión o consumación del phishing.

Los alcances que ha tenido el phishing se han visto reflejados en las múltiples pérdidas millonarias en todo el mundo, así mismo en la tendencia a la alza de su utilización para la obtención de recursos de manera ilícita pues las transacciones monetarias cada vez son más recurrentes mediante la utilización de sistemas informáticos que de alguna manera intentan facilitarnos, o hacer más cómodo nuestro estilo de vida, revisten cierta vulnerabilidad en algunos aspectos, por lo que si no se utilizan de manera responsable, prudente y consciente, pueden llegar a ser riesgosos no solamente para quien los utiliza de manera directa, que en el caso específico serían los tarjetahabientes o bien consumidores, en algunos casos el daño o daños a falta de regulación específica y de métodos de prevención implementados por las instituciones financieras, así como la supervisión de las autoridades encargadas de velar por el buen funcionamiento del sistema financiero, pudiesen repercutir de manera colateral en la estabilidad financiera de un Estado, país o en el peor de los casos a nivel mundial, situación que no sería la primera vez que se presenta derivada de aspectos económicos.

Esta investigación por sus características reviste un gran potencial de interés al ser un tema novedoso y que no es del conocimiento popular, situación que está por demás decirlo debe ser ampliamente difundida y divulgada.

CAPITULO PRIMERO
DEL PHISHING.

1.1 EVOLUCIÓN DE LAS TRANSACCIONES ECONÓMICAS Y SURGIMIENTO DEL PHISHING.

1.1.2 EVOLUCIÓN DE LAS TRANSACCIONES ECONÓMICAS.

La necesidad de supervivencia del ser humano lo ha dirigido a experimentar diversos tipos de interacciones sociales con la finalidad de obtener los bienes necesarios para su desarrollo, explotando recursos tanto naturales como intelectuales. En un principio los hombres únicamente tomaban del medio ambiente lo que necesitaban para subsistir, sin embargo, la acumulación de ciertos bienes les pareció buena idea con la finalidad de tener un esfuerzo menor en sus tareas diarias, por lo que comenzaron a crear un hábito de sedentarismo y de dominio sobre los bienes y personas que rodeaban sus alrededores, a mayor capacidad de acaparamiento sobre bienes y servicios se tiene la facilidad de ejercer mayor poder sobre los que tienen menor poder y capacidad económica.

Desde la época del Mercantilismo en la que se comienza a tener una preferencia por la tenencia y uso de los metales preciosos, la cual es conocida como creencia crisohedónica, la cual consiste en creer que la riqueza está representada por los metales amonedados y amonedables[1]. Es decir, esta doctrina económica establece que se tiene la creencia que la riqueza de una persona se mide por la cantidad de metales preciosos que posee, por lo que la acumulación de riquezas se ha vuelto más un aspecto elitista que uno práctico.

En la actualidad, el dinero, aunque en su mayoría se sigue utilizando de manera física como método de intercambio, también es una realidad que existe el dinero no físico o dinero virtual, que se sustenta en el poder adquisitivo de una persona conforme a sus ingre-

[1] Cfr. Gómez Granillo, Moisés, Breve Historia de las Doctrinas Económicas, 23ª Edición, Editorial Esfinge, México 2001, p. 27.

sos, así como del dinero real que posee y tiene ahorrado en una cuenta bancaria o en su colchón, así como los bienes que ha adquirido durante toda su vida. Derivado de esto, las diversas instituciones que cuentan con la autorización para desarrollar profesionalmente actividades económicas otorgan líneas crediticias con fines de lucro a sus clientes potenciales, mismas que a su vez se encuentran respaldadas por el patrimonio y liquidez de las mismas instituciones que otorgan el crédito.

Visto desde el punto de vista antropológico, es notable que el ser humano es capaz casi de cualquier cosa por la obtención de estos recursos que lo harán más rico y por ende poderoso, por lo que la utilización de cualquier medio o herramienta para lograr el fin es solo el principio de su cometido. El gran avance que ha obtenido la tecnología en los últimos sesenta años le brinda a la sociedad un sin número facilidades y diversas maneras de conseguir recursos económicos para su desarrollo, por supuesto que no se puede dejar de lado el paradigma de que hay quien utiliza estos recursos para su beneficio y en mayor escala para realizar contribuciones a la sociedad. Por otro lado, se encuentran aquellas personas que aprovechan sus conocimientos sin ningún tipo de escrúpulos con la finalidad de obtener mayores beneficios económicos con un menor esfuerzo, sin interesar si esta práctica se lleva a cabo de manera lícita o no.

Como ejemplo de esto, la Internet ha sido de los avances tecnológicos con mayor relevancia en los últimos años, por el sin número de beneficios que aporta al desarrollo de las interacciones sociales de la humanidad, se ha convertido en el medio de comunicación preferente, un registro permanente de información actual e histórica de casi todos los acontecimientos relevantes y no relevantes de la humanidad, un medio de entretenimiento, una interfaz de tipo comercial y no menos importante en una fuente de trabajo continua. A pesar de que su uso aún se encuentra restringido a gran parte de la población mundial, por aspectos de tipo económico, estructurales, en algunos otros políticos y en otros tantos religiosos, hoy en día un gran número de transacciones comerciales se realizan por este medio, así como también el pago o contraprestación de fuertes sumas de dinero es posible realizarlas en internet.

Dicho lo anterior y siendo un hecho real que la modernidad ha rebasado los esquemas del *modus vivendi* que solíamos llevar hace poco más de 20 años, debido a que la vida como la conocíamos ha tenido una evolución integral e inimaginable.

La comodidad que representa la nueva era, en muchos casos nos permite realizar acciones cotidianas de manera más segura, por ejemplo, la no disposición de dinero en efectivo para la realización de grandes transacciones monetarias. La banca electrónica ha sustituido el método habitual de las diversas transacciones monetarias, ahora el dinero se transfiere de una cuenta bancaria a otra de manera inmediata sin que siquiera se pueda percibir dicha situación, además esto de alguna manera otorga seguridad a los usuarios de estos servicios, debido a las altas tasas de inseguridad que se sufre en muchas partes del mundo, es preferible tener resguardados los recursos en una institución financiera y disponer de ellos de forma material, únicamente cuando sea absolutamente necesario, gracias a estos avances ya no es necesario cargar todo el tiempo con el dinero en efectivo con el temor latente de ser atacados por un delincuente.

Dicho esto, otro factor que se encuentra latente consiste en que son demasiados los esfuerzos realizados por aquellos que queremos un mejor mundo para vivir, las nuevas implicaciones tecnológicas buscan que la manera de hacer las cosas sea diferente, convirtiéndolas en actividades más fáciles, rápidas y seguras. Sin embargo, existen cierto tipo de personas que no tienen los mismos ideales, pues cometen atrocidades de manera deliberada en prejuicio de la sociedad, estos sujetos de alguna u otra manera siempre encuentran vías perspicaces y especializadas de continuar haciendo el mal, ejemplo de ello son la variedad de los delitos que se cometen en la red o con el empleo de herramientas tecnológicas para su comisión.

Debido a esto, es de relevante importancia y especial atención crear y emplear adecuadamente herramientas jurídicas necesarias para su prevención, regulación y en dado caso su penalización.

Lamentablemente en México son muy pocas las personas especializadas en temas relativos a ciberdelincuencia, derecho cibernético y demás materias especializadas en nuevas

tecnologías, debido a que es un tema poco explorado y explotado por su complejidad técnica, además de la poca importancia que se le presta a causa de que aparentemente en nuestro país son relativamente pocos los casos y pocas las personas que han sido víctimas de delitos cometidos en la red, los llamados delitos cibernéticos, sin darnos cuenta está es una problemática creciente en la que se debe poner énfasis a miras de crear mecanismos óptimos y oportunos a fin de crear conciencia acerca del peligro que puede representar el uso de dichas tecnologías, así como crear una serie de medidas preventivas.

Un ejemplo de este tipo de prácticas cibernéticas es el phishing, actividad la relativa a la suplantación de las entidades financieras o empresas que emplean servicios financieros como medio de pago a través de sitios web apócrifos, mediante los cuales los atacantes cibernéticos intentan inducir al error a los usuarios con la finalidad de sustraer sus datos personales de identificación ante dicha institución, por lo que se sirven de mensajes enviados mediante diversas interfaces digitales ubicadas en la red, con la finalidad de obtener un lucro indebido.

1.1.3 SURGIMIENTO DEL PHISHING.

Las primeras prácticas de phishing comenzaron en la década de los noventa, cuando un grupo de personas con conocimientos técnicos especializados llamados crackers, quienes utilizan ingeniosamente sus habilidades con sistemas computacionales con la finalidad de obtener información o introducirse ilegalmente en la red de datos entre otras actividades. El término phishing se utilizó por vez primera en el año de 1996, publicado en un artículo de Magazine 2600 “The Hacker Quartely”[2], revista americana especializada en dar a conocer información técnica relativa a los servicios y protocolos utilizados en internet, así como una serie de noticias generales sobre computadoras y sus avances tecnológicos[3].

[2] Cfr. https://proyectophishing.wordpress.com/2006/08/10/phishing-%C2%BFque-es-su-historia-y-modo-de-operar/ (Consultado 28/08/2017)
[3] Cfr. Russel Kay, Computer World. http://www.computerworld.com/article/2575094/security0/sidebar--the-origins-of-phishing.html (Consultado 18/08/2017 traducido por el autor de la tesis)

En el mismo año la compañía AOL (antes conocida como América Online), empresa proveedora de diversos servicios en internet quien tiene su sede en Nueva York, sufrió diversos ataques perpetuados por "phishers", quienes se hacían pasar como personal de la empresa con el propósito de robar las cuentas de los usuarios. De esta manera dichos individuos enviaban mensajes a distintos usuarios conocidos como "spamming", mediante los cuales solicitaban al cliente con diversas excusas mal intencionadas la revelación de sus contraseñas o credenciales electrónicas a efecto de obtener datos de facturación, los clientes al quedar inmersos en una situación de riesgo planteada por un sujeto que se ostentaba como trabajador de la empresa, accedían de buena fe a proporcionar los datos solicitados por temor a algún tipo de repercusión, no obstante, una vez que el usuario o víctima entregaba los datos se podían realizar acciones como el envío de spam a efecto de recabar más información como por ejemplo libretas de direcciones electrónicas y contactos, o bien información o contraseñas de índole financieras, a este proceso se le denominó como "AOHell", pues se desarrolló un proceso automatizado, con un algoritmo computacional para el envío de estos mensajes de manera desenfrenada o masiva[4]. El único método inmediato que implemento la compañía AOL a efecto de solucionar esta problemática fue la de incluir una leyenda en sus mensajes en la que refería a sus clientes que la empresa nunca le solicitará contraseñas o información de facturación[5].

El confort otorgado por los servicios que encontramos hoy día internet otorga cierta ventaja y comodidad a efecto de obtener distintos bienes o servicios según sea el caso, sin la necesidad de desplazamiento a las grandes cadenas de autoservicio o centros comerciales. Esto conlleva una serie de implicaciones inherentes, como lo es la disposición de un instrumento de crédito avalado por una institución financiera a efecto de poder realizar la compra, como es el caso de grandes empresas de subasta que encontramos en la red, verbigracia "E-Bay" o Amazon, que no se han escapado a este tipo de artimañas perpetuadas en la red. En el año de 2003, "E-Bay" quien utiliza un sistema complementario de pago a efecto de completar las transacciones de compraventa llamado "PayPal"[6], servicio mediante el cual se comenzaron a enviar correos electrónicos que simulaban aler-

[4] Cfr. Robinson, Daniel, A Brief History of Phishing http://www.brighthub.com/internet/security-privacy/articles/82116.aspx (Consultado 18/08/2017, traducido por el autor de la tesis)
[5] Cfr. http://www.phishing.org/history-of-phishing (Consultado 18/08/2017, traducido por el autor de la tesis)
[6] Véase: http://pages.ebay.es/aboutebay/thecompany/companyoverview.html (Consultado 24/09/2015)

tas a los usuarios de este servicio, con la novedad de que había un error en sus datos de facturación o registro, por lo que le solicitaban de nueva cuenta su usuario y contraseña, una vez obtenidos dichos datos, el atacante realizaba transacciones con la cuenta de la víctima con la finalidad de obtener una serie de bienes o servicios señalando la entrega a un nuevo domicilio.

Con el paso del tiempo, los ataques comenzaron con una tendencia de especialización, a efecto de conseguir mayor número de víctimas, tal como lo establece la firma de antivirus "Norton" de la siguiente manera:

> "*Durante el año 2005, los ataques de los phishers se hicieron mucho más complejos. Comenzaron a utilizar software de actividades ilegales junto con sus sitios web falsos, y aprovecharon vulnerabilidades conocidas de los exploradores de Internet para infectar los equipos víctima. Esta tendencia significa que con tan sólo hacer clic en el vínculo de un correo electrónico de phishing que conduce a un sitio web falso, es posible robar la identidad del usuario, dado que el phisher ya no necesita que el usuario introduzca su información personal; el caballo de Troya o el software espía que se implanta en el equipo capturará esta información la próxima vez que el usuario visite el sitio web legítimo del banco o de otro servicio en línea. Durante el pasado año, este tipo de software de actividades ilegales se hizo más selectivo (para capturar solamente la información solicitada por el phisher) y más sigiloso gracias a los rootkits y a otras técnicas de ocultación que les permiten mantenerse ocultos en el interior de un sistema infectado*[7]*.*

Conforme la sociedad va creciendo intelectual como tecnológicamente, no desaprovecha la oportunidad de utilizar las herramientas que nos brindan los avances tecnológicos, a pesar de ello, algunos dotados de habilidades específicas, parecen controlar o entender mejor el funcionamiento de éstas, algunos para bien, otros para mal. De tal manera que los delincuentes no quedan excluidos de esta regla, día con día perfeccionan sus métodos a efecto de comprometer a las víctimas engañándolos de una manera casi imperceptible, sus avances son tales que han optado por blancos más sustanciosos como es el caso de

[7] https://mx.norton.com/cybercrime-phishing (Consultado 25/08/2017)

las entidades financieras. Tal es así, que comenzaron a registrar dominios de páginas web similares a los de las entidades bancarias[8], al diseño y creación de páginas en internet con los logotipos y elementos idénticos al sitio original a fin de suplantar el sitio auténtico y hacer creer a la víctima que navega de forma segura en el sitio correcto y así sustraer su información.

Existe otro tipo de actividades además de las mencionadas con anterioridad ciertamente más complejas y técnicas relacionadas estrechamente a efecto de cometer este tipo de delitos o fraudes electrónicos, verbigracia, es el uso de las nuevas plataformas de mensajería instantánea en las que se puede reenviar contenido malicioso a los destinatarios o spam a fin de redireccionar a la víctima a sitios poco confiables en los que podrías ser presas de alguna estafa; o el caso de virus malicioso, un malware troyano con el nombre de “Trojan.Peskyspy” que permite al hacker infiltrarse y grabar las conversaciones mantenidas por medio del formato “VoIP” o voz por Protocolo de Internet, el cual es un recurso que permite que la voz viaje por las redes de internet, almacenando la información recibida en un paquete de datos, en lugar de enviarla de manera analógica a diferencia de las comunicaciones que comúnmente conocemos como la del teléfono, éstos pueden ser descargados en un formato mp3 y ser reenviados a cualquier lugar de la red[9]. Por lo que, si un computador se encuentra infectado con esta clase de virus informático, es muy probable que la información que se comparte por este medio pueda estar comprometida, lo que implica un riesgo notable por los datos que en dado caso pudiesen compartirse, aunado el mayor riego si son datos de seguridad como claves o credenciales que por causas de este método podrían terminar en manos equivocadas[10].

---

[8] Como ejemplo de esto podemos señalar que le sitio original de la Institución de Banca Múltiple Banamex S.A. de C.V. es https://www.banamex.com por lo que se registran algunos fonética y visiblemente similares como: www.banmex.com, www.banamexx.com, www.banamex1.com; o bien cuentas de correo electrónico como por ejemplo: banamex.assistence@hotmail.com; banamex1@yahoo.com, banmex@gmail.com; etc.

Véase:
https://www.banamex.com/es/personas/servicios/seguridad/ejemplos_phishing/demo_ejemplos_phishing.htm (consultado 18/09/2017)

[9] Misfud, E; Lerma-Blasco, Raúl V. Servicios en Red, Editorial McGraw-Hill, textos de ciclos formativos, pp.256, visible electrónicamente en: http://www.mcgraw-hill.es/bcv/guide/capitulo/8448171330.pdf

[10] Para mayor referencia véase: http://www.bsecure.com.mx/enlinea/espia-de-llamadas-voip/

Como se puede observar, a grandes rasgos, son muchas y detalladas las maneras en que algún sujeto puede ser víctima de este tipo de prácticas, por lo que ahora, después de este breviario histórico a manera de identificarnos *lato sensu* con la figura del Phishing entraremos de lleno a su estudio.

1.2.- ACEPCIONES DEL PHISHING Y CONCEPTO.

Derivado de párrafos anteriores hemos planteado de manera sucinta lo que es el phishing y en que consiste, sin embargo, para un mejor entendimiento y estudio de dicha figura es importante analizarla a profundidad en cada uno de sus elementos tanto objetivos como subjetivos, por lo que en primer término analizaremos dicha figura desde su perspectiva conceptual.

1.2.1. DEFINICIÓN ETIMOLÓGICA DEL PHISHING.

El término “Phishing” tiene dos orígenes principalmente, el primero de ellos deviene de la palabra inglesa “fishing” que al castellano se traduciría como pesca o pescando, refiriéndose específicamente a la pesca de credenciales o pesca de ingenuos susceptibles de ser víctimas de fraude, el segundo “phishing” es comúnmente utilizado por los hackers para sustituir la *f,* como raíz de la antigua forma de hacking conocida como “phonephreaking”[11], que es un término acuñado en la subcultura informática para denominar la actividad de comprensión del funcionamiento de diversas tecnologías, con la finalidad de penetrar ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de causar perjuicios a terceros o bien obtener una serie de beneficios que utilizan en su favor de manera ilegal[12].

Así mismo, se dice que el término “phishing” es la contracción de “*password harvesting fishing*” que se traduce como “cosecha y pesca de contraseñas”[13].

[11]Cfr.http://www.gytcontinental.com.gt/portal/portal/productos.asp?Option=4&idProd=FAQ&Category=Article&SubCategory=seguridad&idQ=21&State=1 (Consultado 28/08/2017)
[12] Cfr. https://hechoencu.wordpress.com/2008/04/07/phreaking-hacking-o-cracking-telefonico-delitos-informaticos/ (Consultado 28/08/2017)
[13] Cfr. http://www.victormiranda.com.mx/vmwp/sabes-que-es-phishing/ (Consultado 28/08/2017)

1.2.2. DEFINICIONES DE PHISHING.

El catedrático Diego Guerrero nos brinda una breve definición respecto del phishing que es la siguiente:

> "*Esta es una modalidad de estafa cuyo objetivo es conseguir la mayor cantidad posible de datos personales y bancarios, con el fin de ser utilizados posteriormente de forma fraudulenta...*"[14].

Aunque un poco limitativa esta definición, nos brinda un panorama general de la actividad como tal, en la que no se incluyen los elementos específicos de tal conducta, pero es acertada el señalar que los principales objetivos del ciber delincuente es la obtención de datos bancarios.

En México, la mayoría de las instituciones financieras, a través de sus sitios web, ponen a disposición de sus usuarios valiosa información sobre medidas de seguridad que éstos deben adoptar al realizar operaciones por medios electrónicos, específicamente cuando encuentren relacionadas con la banca electrónica, no obstante, dichas medidas pocas veces son atendidas y mucho menos divulgadas.

En los sitios web de dichas instituciones encontramos las siguientes definiciones de phishing:

> **BANAMEX. -** *"Es un tipo de fraude electrónico y una de las variantes de la ingeniería social, a través de la cual los delincuentes obtienen información detallada, personal y confidencial, principalmente relacionada con claves para el acceso a servi-*

[14] Guerrero, Diego, *Fraude en la red. Aprenda a protegerse contra el fraude en Internet,* Ed. Ra-Ma, 2010. p. 120.

cios bancarios y financieros, información y compra-venta de productos y servicios por internet"[15].

SANTANDER. - *"Es un tipo de spam que consiste en el envío masivo de mails cuyo objetivo es obtener información confidencial (números de cuentas, códigos de clientes, claves personales, entre otras) para después realizar actos ilícitos o fraudes"*[16].

HSBC. - "*El Phishing implica un mensaje electrónico que es enviado a tantas direcciones de correo electrónico de Internet como el defraudador puede obtener, presumiendo provenir de una organización legítima como un Banco, un servicio de pagos en línea, un minorista en línea, o similar.*

El correo electrónico solicita que el destinatario ponga al día o verifique su información personal y financiera, incluyendo la fecha de nacimiento, la información de conexión, los detalles de cuentas, los números de la tarjeta de crédito, los números de identificación personal (NIP), etc. Algunos mensajes electrónicos incluyen una amenaza de que, si no se actualiza o se valida causará, por ejemplo, que la cuenta sea congelada. El objetivo es inducir a destinatarios confiados, que resultan ser los clientes de la organización legítima que ha sido imitada, a responder al correo electrónico y proporcionar la información solicitada"[17].

Por su parte, la "Anti-Phishing Working Group[18]", (APWG por sus siglas en inglés), organización internacional constituida por diversas empresas, organizaciones gubernamentales, asociaciones religiosas y proveedores de servicios financieros, entre otros que han sido víctimas de diversos ataques relacionados con el phishing, cuyo objetivo es la colaboración a fin de disminuir el impacto de esta práctica y brindar seguridad en el ciberespacio[19], definen tal fenómeno de la siguiente manera:

---

15 https://www.banamex.com/es/personas/servicios/seguridad/ejemplos_phishing/demo_ejemplos_phishing.htm (Consultado 19/09/2017)

16 http://www.santander.com.mx/seguridad_nvo/seguridad.html (Consultado 16/05/2017)

17 http://www.hsbc.com.mx/1/2/es/pie-pagina/seguridad/phishing (Consultado 19/06/2015)

[18] http://www.antiphishing.org/about-APWG/ (Consultado 18/07/2017)

[19] Esta organización fundada en el año de 2003 tiene poco más de 3,200 miembros de más de 1700 compañías que utilizan la red como plataforma al rededor del mundo, dentro de las que se pueden destacar

" Los ataques de phishing recurren a formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras. Los ardides de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de seguridad social. Apropiándose de nombres comerciales de bancos, distribuidores y compañías de tarjetas de crédito, los phishers[20] a menudo convencen a los destinatarios para que respondan. Los subterfugios técnicos implican la instalación del crimeware[21] en ordenadores personales para robar las credenciales directamente, habitualmente utilizando troyanos[22] que captan las pulsaciones del teclado"[23].

La definición propuesta en el párrafo precedente es muy completa, debido al gran empeño que este grupo ha puesto en el estudio de dicha figura, del cual es posible destacar cuatro puntos o características importantes que facilitan el entendimiento de la figura del phishing, mismas que me permiten desarrollar una noción estructurada sobre el concepto de la figura en estudio, misma que se expone a continuación.

1.2.3. DEL CONCEPTO DE PHISHING.

---

empresas de seguridad cibernética tales como: Bit Defender, Symantec, McAfee, VeriSign, IronKey y Internet Identity; así como miembros de la industria financiera tales como: ING Group, MasterCard, Visa y la Asociación Americana de Banqueros.

[20] Denominación empleada para designar a los estafadores que utilizan esta técnica.

[21] Conjunto de amenazas de internet cuyo objetivo es la realización de delitos que permiten conseguir un beneficio económico, directa o indirectamente.

[22] Los troyanos no se pueden considerar virus ya que no se replican o no hacen copias de sí mismos. En realidad, son programas que llegan a un ordenador de forma totalmente normal y no producen efectos realmente visibles o apreciables (por lo menos en ese momento). Pueden llegar acompañados de otros programas que se instalan en el ordenador del usuario. Al activarse pueden dejar huecos en nuestro sistema, a través de los cuales se producen intrusiones.

[23] Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing, Instituto Nacional de Tecnologías de la Comunicación, España, octubre 2007. Puede consultarse en línea en: http://www.osimga.org/export/sites/osimga/gl/documentos/d/ogsi/doc_ext/ambito_estatal/estudio_sobre_usuarios_afectados_por_phishing_2007.pdf (Consultado 18/09/2017)

En primer lugar, se establece la hipótesis de que el phishing es un mecanismo de ingeniería social, en mi opinión, éste es el punto medular de la definición para comprender mejor la figura del phishing, conforme a lo siguiente.

La ingeniería social es un término comúnmente utilizado para describir un método ejecutado por un estafador que se auxilia de artilugios, tretas y técnicas sofisticadas mediante las cuales engaña y persuade a su víctima con la finalidad de que realice actos que normalmente no haría, como la de revelar datos confidenciales o privados, es decir es la técnica utilizada para obtener información personal y/o confidencial mediante engaños[24]. Para el caso en concreto, el objetivo del hacker o phisher es obtener información mediante el engaño, abusando de la ingenuidad o confianza de los usuarios, lo que les permite obtener diversos tipos de credenciales o contraseñas con las cuales automáticamente tienen acceso autorizado a un sistema de valores y a la información que reside en los sistemas computacionales, mismos que utiliza en su beneficio.

El segundo de ellos se refiere a la serie de mecanismos utilizados por los phishers a efecto de allegarse del mayor número de víctimas valiéndose de herramientas cibernéticas como pueden ser llamados "*Spam*"[25], así como la utilización de algunas otras técnicas brindadas por las tecnologías de la información como lo pueden ser virus informáticos que se utilizan para desarrollar ataques de phishing de forma masiva, a este punto se le define como automatización de procesos.

El tercer punto importante derivado de la definición es que los ataques se realizan mediante las de redes de comunicación electrónica, por conducto de cualquier dispositivo provisto de internet, los cuales en su mayoría aparecen en correos electrónicos, aunque esta aseveración no es limitativa, si es la más común.

El último de ellos se refiere a la suplantación que se realiza por los atacantes a distintas empresas o instituciones financieras con el objetivo de brindar confianza a la víctima, induciendo al mismo en el error al creer que se encuentra visitando un sitio legítimo y segu-

[24] Cfr. https://seguinfo.wordpress.com/category/ingenieria-social/page/11/ (Consultado 28/08/2017)
[25] Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

ro, mecanismo que ha sido perfeccionado de manera tal que dicha falsificación de sitios web es casi imperceptible para el ojo humano, aunado a la ofuscación que produce la noticia de que tus recursos financieros pueden estar en riesgo, es la combinación perfecta e ineludible para ser víctima en este tipo de engaños.

Una vez planteadas diversas hipótesis relacionadas con la práctica del phishing y habiendo analizado las principales características de dicha figura, procederé a proponer la siguiente definición:

El “Phishing” es una modalidad de fraude electrónico especializado basado en la implementación de medios tecnológicos, así como técnicas de ingeniería social, en la cual, quien la realiza, aplica el engaño a través de la suplantación de sitios web, manipulación informática, envío masivo de correos electrónicos que contienen una liga maliciosa que redirigen al usuario a sitios web apócrifos los cuales se hacen pasar por alguna institución financiera o empresa de confianza, con el único cometido de obtener de la víctima información detallada, personal, sensible y confidencial, sobre datos que frecuentemente se encuentran relacionados con información financiera, claves de seguridad para acceso a servicios financieros, bancarios, a sitios de compra-venta de productos y servicios en línea, entre otros, con la finalidad de utilizar de manera ilícita dicha información.

Derivado de las diversas definiciones estudiadas con anterioridad, se puede apreciar que cada una tiene su peculiaridad debido a las diversas características y circunstancias de modo y tiempo en el que fueron elaboradas, algunas de ellas, sobre todo las más novedosas, contienen elementos específicos que surgen de la creciente evolución y la dinámica especialización de las métodos implementados por los ciberdelincuentes, actitud que deben mantener debido a que cada vez los usuarios de la red van teniendo mayor conocimiento de este tipo de prácticas delictivas, siendo más difícil hacerlos caer en ellas.

1.3.- CASOS MÁS COMUNES DE PHISHING.

En la actualidad existe una gran tendencia de utilizar los medios electrónicos con la finalidad de realizar acciones cotidianas como la de comunicarse, comprar artículos de uso co-

tidiano, así como buscar información de distinta índole, información que en su mayoría es proporcionada por los mismos usuarios internautas, sin embargo, es poca la atención y muchas las medidas de seguridad que se deben tener en consideración al momento de utilizar la red a efecto de compartir cierta clase de datos, específicamente me refiero a aquellos datos que son de clase personal. El creciente aumento en el uso de dispositivos móviles y su fácil acceso a la red genera riesgos importantes para los consumidores, debido a que otorga la facilidad de compartir información en tiempo real, información que en muchos casos es de carácter sensible.

Sin duda alguna, todos los dispositivos provistos de conexión a internet en los cuales no se adopten las medidas necesarias de seguridad, podrían ser víctima de diversos tipos de ciberataques, que en la mayoría de los casos, ocurren mediante la utilización de los navegadores a través de la instalación de extensiones, o bien en la descarga de aplicaciones gratuitas que pueden contener virus maliciosos, así como también abrir los archivos adjuntos incluidos en los correos electrónicos, actividades en las cuales se pueden infectar los ordenadores con software malicioso, el cual es uno de los métodos más efectivos utilizados por los delincuentes con la finalidad de manejar a su antojo la información contenida el computador o bien manipular su funcionamiento para obtener una serie de datos confidenciales de la víctima, o redirigir a los usuarios a un sitio apócrifo en el que se soliciten los mismos, los cuales posteriormente son utilizados para la realización de algún tipo de fraude, precisamente de este punto es de donde se desprende el estudio de la figura de mérito, el phishing.

Cabe resaltar, que el perfeccionamiento de estas técnicas ha sido realizado de manera progresiva y de la misma manera los objetivos de los phishers y el destino de los ataques, en el entendido de que en un principio dichas amenazas tenían en la mira principalmente la obtención de datos de índole bancario afectando lastimosamente a las corporaciones del sistema financiero y a los usuarios de las mismas. Sin embargo, ante la proliferación de dichos ataques es evidente que las instituciones encargadas de velar por la seguridad propia y de sus clientes comenzaron a tomar las medidas de seguridad necesarias con la finalidad de prevenir este tipo de estafas, por lo que los delincuentes buscan nuevas ma-

neras y mercados crecientes donde perpetuar los ataques, por lo regular empresas más pequeñas y por ende menos protegidas.

Ejemplo de esto, son las distintas plataformas que encontramos en internet encargadas de ofrecer servicios en los que a menudo se realizan transacciones monetarias en línea como lo son, portales de sistemas de pagos, sitios de subasta, videojuegos en línea, agencias de viaje, tiendas de comercio electrónico, redes sociales, etc.

Aunado a esto, es importante destacar que existe un gran número de usuarios de dichas servicios que son menores de edad, quienes utilizan las diversas plataformas como medio de entretenimiento sin ningún tipo de supervisión, quienes de alguna manera con o sin consentimiento de sus padres tienen acceso a diversos datos sensibles que podrían encontrarse en peligro de ser divulgados por el poco conocimiento y cuidado de su manejo, pues difícilmente un menor podrá discernir que está siendo víctima de un ataque, o cuales son los límites de seguridad en la red, es por esto que los atacantes en aras de lograr de manera más eficiente sus objetivos, se dan a la tarea de realizar ataques más personalizados y técnicas más llamativas así como especializadas.

Las diversas vertientes tecnológicas de manera innovadora día con día evolucionan de manera exponencial, nos dejan asombrados a los consumidores con su rapidez, pues en poco tiempo dejan completamente obsoletos los productos que eran de lo más novedosos hace uno o dos años. De la misma manera los phishers continuamente aumentan su grado de sofisticación y profundidad en la perpetuación de sus ataques, por lo que es muy complicado enumerar todos los tipos de combinaciones de escenarios y fraudes en los que se presenta el phishing, o hacer una clasificación de los mismos, referente al tema, los coautores Marcus Jakobsson y Steven Myers es su obra "*Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft"* enumeraran los seis principales tipos de phishing que más se dan en la práctica[26], mismos que han sido explicados y desarrollados por el honorable Observatorio de la Seguridad de la Información, de la siguiente manera y que al mismo tiempo iré comentando conforme a mí entendimiento:

[26] Marcus Jakobsson y Steven Myers, "*Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Editorial Wiley, 2007. (Traducido por el Instituto Nacional de Tecnologías de la Comunicación de España op. cit. p. 40)*

"...1.- Phishing engañoso – Deceptive Phishing

Esta es la forma primitiva de phishing. Aunque en sus inicios (cuando el objetivo básico era la captura de cuentas de AOL) la herramienta de comunicación utilizada eran las aplicaciones de mensajería instantánea, en la actualidad la forma más habitual de desarrollar este tipo de delito (o al menos de iniciarlo) es mediante el correo electrónico. Precisamente, un típico ataque de esta variedad de phishing comienza cuando el phisher envía un correo electrónico falso.

El procedimiento es relativamente sencillo. Consiste, básicamente, en el envío, generalmente masivo, de un correo electrónico en el que es suplantada una empresa o institución legítima y de confianza para el receptor, por lo que este atendiendo una "llamada a la acción" incluida en dicha comunicación electrónica pulsará en el enlace contenido en el correo electrónico siendo desviado, de manera inconsciente, a un sitio web fraudulento.[27]"

Es posible señalar que dicha modalidad se constituye como la más empleada dentro de los diversos tipos de phishing, lo anterior en virtud de que las víctimas son engañadas utilizando un sitio web o correo electrónico masivo en el que se indica a los receptores la existencia de alguna circunstancia que puede perjudicar la integridad de las cuentas bancarias del destinatario, esto comúnmente se hace mediante el envío de mensajes intimidantes que advierten de una problemática en éstas, como pueden ser: cargos no reconocidos, intentos de acceso a sus cuentas desde ubicaciones no habituales, la realización de algún cambio no autorizado en la información de la misma, etc.

Ésta situación, incita a las víctimas para acceder a un enlace (link) donde supuestamente podrán solucionar el problema que les fue comunicado por un remitente que ellos consideran fidedigno; lo anterior, aunado a la preocupación ocasionada por considerar que su patrimonio y sus datos se encuentran comprometidos, ocasiona que los destinatarios accedan al sitio web engañoso empleado por los "phishers" y proporcionen toda clase de in-

[27] Ídem.

formación confidencial, la cual será recolectada y posteriormente utilizada para la comisión de algún ilícito.

De igual forma, existe una amplia gama de delitos que pueden cometerse a partir de la información sensible obtenida, mismos que van desde la venta de las bases de datos recolectadas, la realización de compra de productos o contratación de servicios por Internet, transferencias electrónicas de fondos, solicitud de créditos de todo tipo, apertura de cuentas adicionales y, en general, la obtención de productos financieros adicionales.

Además, se explica en el trabajo aludido, que existen diversas vertientes mediante las cuales se pueden propagar ataques de phishing utilizando diferentes herramientas, que dentro de las más comunes se encuentran las siguientes:

> *"Dentro de esta tipología de phishing existen también distintas variantes. Una de ellas, relativamente común, es enviar mensajes de correo electrónico que, a través de HTML, replican con más o menos precisión la pantalla de autenticación de la entidad a la que están suplantando, evitando, de esta forma, que el usuario tenga que pulsar un link y utilizar el navegador web para realizar la acción. Mediante esta técnica se hace más difícil que el destinatario detecte el engaño.[28]"*

Es así, que al pulsar el link que se indica en los mensajes a efecto de realizar la acción tendiente a solucionar la problemática, éste te redirigirá a una sitio web suplantado de alguna institución o empresa con buena reputación, mismo que al contener la características propias de quien dice ser el destinatario, agregará confianza sobre la veracidad del tal hecho, esto se logra mediante múltiples técnicas informáticas de engaño y ocultamiento como se describe a continuación:

> *"Las técnicas comprenden desde el uso de la dirección IP numérica en lugar del nombre de dominio[29], al uso de pequeñas rutinas realizadas mediante lenguaje de*

[28] Ídem.
[29] La dirección IP está formada por una serie numérica de cuatro grupos entre 0 y 255 separados por puntos y que identifica un ordenador conectado a Internet. Obviamente, este sistema no se utiliza para la navegación por las dificultades que supondría recordar esta serie de memoria. En su lugar, el DNS (Domain

programación (ej. en JavaScript) que esconden la barra de direcciones del navegador, pasando por el uso de lo que se denomina el "ataque de un dominio primo", esto es, el registro de un nombre de dominio similar al de la organización a la que se está suplantando para realizar la estafa (por ejemplo, "www.entidadfinanci.era.es" en lugar de "www.entidadfinanciera.es".

Otra variante dentro del ataque a través de correo electrónico consiste en mensajes tengan como finalidad la instalación de algún tipo de software malicioso. Este se ejecutaría en el ordenador del destinatario cuando este ingresa en el sitio web falso y confunda, de alguna forma, al usuario. No obstante, esta categoría entraría dentro del siguiente tipo de phishing, que se analizará seguidamente.[30]"

Lo anterior, únicamente se refiere a la primera parte del engaño, que, a resumidas cuentas, lo que ocurre en esta etapa es la suplantación de una institución o empresa de buena reputación, mediante la adopción o usurpación de sus logotipos, tipografías, colores, diseños, etc., envían mensajes a múltiples destinatarios indicando cierta problemática, en el que insertan una liga o "link", el usuario debido al temor, curiosidad o incertidumbre procederá a realizar la acción que indica en el mensaje al creer que proviene de una fuente fidedigna, peor no lo es todo, reviste importancia analizar la segunda parte del engaño, que como bien se describe en el estudio citado, pueden presentarse los siguientes casos:

"Las principales argucias utilizadas por este tipo de estafadores en los sitios web fraudulentos son:

a) En ocasiones los estafadores programan sus webs de tal forma que si el usuario utiliza un navegador que no tiene la vulnerabilidad que se pretende explotar, redireccionan al usuario a la web legítima, evitando ser descubiertos.

Name System o Sistema de Nombres de Dominio) traduce esos números a direcciones web, tal y como normalmente las utilizamos en los navegadores, que son fáciles de reconocer y recordar.

[30] Ídem.

b) Camuflarse a la hora de suplantar la web legítima de la compañía. Incluso, muchos sitios web fraudulentos simulan el proceso de envío de los datos, tal y como sucedería en la versión legítima, y redireccionan al usuario a la página de la empresa suplantada una vez que los datos han sido facilitados. De esta manera las víctimas no saben que han sido objeto de un fraude.

c) Uso de certificados SSL falsos: una URL que comienza con el protocolo "https://", en lugar de "http://", indica que la información está siendo transmitida a través de una conexión segura y que la compañía está provista de un certificado Secure Sockets Layer (SSL). Algunos sitios web fraudulentos utilizan este protocolo y suele combinarse con la utilización de direcciones IP en lugar de la URL habitual. Curiosamente, los navegadores suelen desplegar mensajes en los que se avisa al usuario de que el certificado es inválido o que no coincide con el nombre del sitio. Sin embargo, la mayoría de usuarios suelen ignorar estos mensajes, pensando que es un error de su navegador y caen en la trampa.

d) Uso de una barra de dirección falsa, que puede contener la dirección légitima del sitio, pero sin ningún efecto sobre la web que se está visitando.

e) Uso de ventanas emergentes: el sitio fraudulento redirecciona al usuario a la web real de la institución suplantada y, simultáneamente, despliega una ventana, fraudulenta, que solicita y recoge los datos. Por ello, resulta de gran utilidad activar los bloqueadores de pop-ups que incorporan la mayoría de los navegadores actuales.

f) Deshabilita el botón derecho del ratón, el cual, despliega un menú que permite, entre otras cuestiones, verificar las propiedades de las web visitadas.

g) Introducir mensajes para evitar que el usuario entre en la web suplantada, obteniendo así el tiempo suficiente para completar el fraude. Los delincuentes más avanzados tecnológicamente utilizan aplicaciones software para bloquear el acceso del usuario (al menos desde el ordenador infectado) al sistema.[31]"

Es así como se ha podido detectar hasta el momento, la manera en que los estafadores logran realizar su cometido, no obstante, frecuentemente se desarrollan nuevos esquemas y herramientas que permiten perfeccionar los medios de estafa, desarrollando nuevas habilidades que permiten encontrar las vulnerabilidades tanto técnicas, como sociológicas o humanas, pues como puede apreciarse, el phishing, continúa teniendo un gran éxito negativo, al inducir a los usuarios de los medios tecnológicos a caer en este tipo de engaños.

Existe una vertiente del phishing que en los últimos años también ha cobrado relevancia, por la simple y única razón de que su realización es menos compleja, pues el medio de convicción se realiza con una llamada telefónica, en la que el intermediario se hace pasar por un miembro de alguna institución de renombre, a esta se le conoce como "vishing" y los académicos del ITECOM, nos brindan una breve descripción de este supuesto:

"El vishing utiliza el teléfono como herramienta. Se basa en el uso de un tipo de software denominado "war dialers" cuya función es realizar la marcación de teléfonos desde un ordenador, utilizando la tecnología de telefonía sobre IP. Una vez que el usuario atacado descuelga se activa una grabación que trata de convencerle o bien de que visite un sitio web para dar sus datos personales o bien de que directamente "confirme" sus datos en la misma llamada. El verdadero problema de este tipo de ataques es la confianza que la población tiene en el teléfono y en el uso que tradicionalmente han hecho de él las empresas legítimas."

Como se puede observar, en el tipo de phishing previamente expuesto, el elemento común es el engaño, o la inducción al error. A continuación, se estudiaran las demás tipologías que los doctos han podido identificar.

[31] Ídem.

El siguiente tipo, o tipología, se refiere al desarrollo de un programa computacional, un "software", que permita la ejecución de un programa dentro del ordenador, mediante el cual permita al estafador descubrir una vulnerabilidad en el sistema, o bien obtener información directamente de la computadora, a esta tipo de phishing se le ha denominado como "Phishing basado en malware" o "Phishing basado en software malicioso" y el observatorio de la seguridad de la información lo definió como se muestra a continuación:

"2.- Phishing basado en software malicioso – Malware-Based Phishing

Con este tipo de phishing nos referimos de forma general a cualquier variante de este delito que implique la ejecución de un software malicioso en el ordenador de la víctima.

La propagación de este tipo de phishing puede depender tanto de las técnicas de ingeniería social como de la explotación de una vulnerabilidad del sistema. En el primero de los casos, el ataque debe conseguir, como paso previo, que el usuario realice alguna acción que permita la ejecución del malware en su máquina: abrir el archivo adjunto de un correo electrónico, visitar una web y descargar el programa. Las técnicas sociales para conseguir que el usuario actúe de este modo son, al igual que en el caso anterior, muy diversas, si bien este método suele inclinarse más por la promesa de algún contenido llamativo para el destinatario.

En lo que se refiere a la explotación de vulnerabilidades del sistema, la amenaza es mucho más difícil de combatir, ya que existen variantes en las que la actuación del usuario es mucho menor. Así, aunque muchas de las estafas se basan en que sea el usuario el que, de una u otra manera, introduzca la aplicación en su máquina, también es posible que los delincuentes aprovechen fallos en la seguridad del sistema de un sitio web legítimo para introducir software malicioso que les permita llevar a cabo su objetivo.[32]"

[32] Ídem.

Como se mencionaba, la tendencia de este tipo de ataque es el de la intromisión directa en el sistema computacional de la víctima, con la utilización de malware que el mismo usuario ejecuta, los cuales son dispersados con los mensajes o correos electrónicos que ya se mencionaban, éstos, en lugar de contener una liga o link, contienen un documento adjunto el cual al ejecutarse, permiten la descarga del mismo, permitiendo el acceso al equipo, lo que puede conllevar a distintas implicaciones, dentro de las cuales, para efecto del estudio del phishing, uno de los más usuales es la de la sustracción o robo de datos confidenciales. Dentro de los diversos programas existentes, el instituto enumera los siguientes:

"…

• *Keyloggers y Screenloggers. Los keyloggers son programas cuya función es el registro de las pulsaciones que se realizan en el teclado. La aplicación en el ámbito del phishing es evidente: estas aplicaciones suelen estar programadas para ponerse en funcionamiento cuando la máquina en la que están instaladas accede a alguna web registrada por el programa (entidad financiera, subasta online). En ese momento, graba todo lo que se teclea en el ordenador y, posteriormente, lo envía al delincuente que de esta forma consigue su propósito de robar información confidencial.*

Existen versiones más avanzadas que también capturan los movimientos de ratón. Algunas entidades, conscientes de la existencia de este tipo de programas y de su posible aplicación delictiva han introducido contramedidas como la disposición de teclados en pantalla para evitar las pulsaciones de teclado en la introducción de contraseñas.

Los screenloggers realizan la misma función, pero, en lugar de capturar pulsaciones de teclado, capturan imágenes de la pantalla que son remitidos al atacante.

• *Secuestradores de sesión (Session Hijackers). Este tipo de aplicaciones operan una vez que el usuario ha accedido a alguna web registrada por el software, esto es, no roba datos, sino que directamente actúa cuando la víctima ya ha accedido a su cuenta corriente su sesión en una subasta. Estos programas suelen ir "disfrazados" como*

un componente del propio navegador. Esta forma de phishing puede realizarse tanto mediante la instalación del malware en el ordenador del destinatario de la estafa, como mediante la técnica del "man in the middle" o intermediario[33]*.*

• *Troyanos web (web Trojans). Son programas maliciosos que aparecen inesperadamente, en forma de ventanas emergentes, sobre las pantallas de validación de páginas web legítimas, con el objetivo de conseguir datos confidenciales. En este caso, la finalidad que persiguen es hacer creer al usuario que está introduciendo la información en el sitio web real, cuando en realidad lo que está haciendo es introducirlo en este software que, posteriormente, remite los datos al delincuente, con las consabidas consecuencias. El phishing parece la aplicación "natural" de este tipo de programas fraudulentos.*

• *Ataques de reconfiguración de sistema (System Reconfiguration Attacks).* Este tipo de ataques se efectúan a través de la modificación de los parámetros de configuración del ordenador del usuario. Existen diversas formas de realizar estas acciones. Una de ellas consiste en modificar el sistema de nombres de dominio, tal como se explicaba en el caso anterior. Otra posibilidad al alcance de los delincuentes es la instalación de lo que se denomina un "proxy", a través del cual se canalice toda la información que sale y entra de la máquina del usuario. Esta forma de ataque se corresponde también con la técnica del "man in the middle" (MitM).

• *Robo de datos (Data Theft).* También existen códigos maliciosos cuya finalidad consiste en recabar información confidencial almacenada dentro de la máquina en la que se instalan y remitirla al delincuente (direcciones, números de identidad, claves).[34]"

De lo anterior, se destaca que quienes desarrollan esta tipo de estafas, son personas con conocimientos técnicos muy avanzados, pues tienen la capacidad de desarrollar un programa que permita ejecutar diversas acciones encaminadas a cometer un ilícito y no

[33] Ataque en el que el delincuente es capaz de leer, insertar o modificar a voluntad los mensajes entre dos partes sin que ninguna de ellos conozca que el canal entre ellas ha sido violado.
[34] Ídem.

tendrá escrupulos en utilizar sus conocimientos a efecto de obtener un beneficio derivado del desconocimiento de quienes utilizan medios informáticos, sobre todo en la protección de la información sensible que se mantenga en éstos, es importante, seguir la recomendaciones que se brindan a los usuarios, no únicamente a las que se refieren a la manera del uso para su manutención, sino también, a aquellas que protejan la integridad de la información.

Otro de los artifices que es utilizado por los ingenieros sociales, es aquel en el que mediante la barra de búsqueda o de navegación al introducir un motor de búsqueda, éste es interceptado y transformado en otro, a este proceso comúnmente se le denomina como "pharming" y es utilizado para prácticas del phishing, específicamente a efecto de redireccionar del sitio legítimo que queremos visitar a uno que ha sido suplantado, para un mejor entendimiento la organización ha brindado la definición que se propone a continuación:

> *"3.- Phishing basado en el DNS o "Pharming" (DNS-Based Phishing)*
>
> *Dentro de esta rúbrica se incluyen todas aquellas formas de phishing que se basan en la interferencia del proceso de búsqueda del nombre de dominio (la traducción de la dirección introducida en el navegador a la dirección IP). Sin duda, el pharming, denominación habitual de esta forma de llevar a cabo este tipo de delito, supone un peligro aún mayor que algunas de las otras variantes que se han analizado, ya que la colaboración de la víctima es menor y, además, el disfraz empleado por los delincuentes parece más real.*
>
> *Como se señalaba al hablar de ciertos tipos de código malicioso, cuando un usuario navega por la Red recurre a la utilización de direcciones URL, relativamente fáciles de recordar (por ejemplo, www.inteco.es). Sin embargo, estas direcciones tienen que ser traducidas a lo que se denominan direcciones IP. Esa traducción se realiza, en los sistemas operativos de diversas formas. Por un lado, existen los denominados Servidores de Nombres de Dominio (Domain Name Server o DNS) que cumplen explícitamente esta función. Cuando un usuario desea acceder a un sitio web*

envía una petición a uno de estos servidores que transforman la URL introducida en la barra de direcciones del navegador en la dirección IP. El proceso es transparente para el usuario.

Otra forma de llevar a cabo esa transformación es mediante el fichero hosts. Este fichero -incluido en el sistema operativo, almacena la información de las páginas que el usuario ya ha visitado- con el fin de evitar la consulta al servidor DNS y acelerar el proceso. Además, en esta misma línea, la memoria caché del navegador también conserva información de las webs visitadas, siempre con el fin de reducir el tiempo de respuesta para la navegación.[35]"

Por lo descrito anteriormente, es importante verificar con la premura y atención necesaria de que los sitios que son visitados en internet sean los fidedignos, así como reconocer los elementos de seguridad con los que deben de contar las páginas, al verificarlas en las barras de navegación, pueden encontrarse colores, mensajes o signos que indican alertas. Además, es recomendable, no seguir enlaces sugeridos en motores de búsqueda, sino que lo correcto, sería dirigirse a la dirección de internet de la página.

El siguiente método, es el aquel que tiende a infectar directamente los sitios de las entidades o instituciones con el empleo de malware, mediante los cuales se intentará buscar ciertas vulnerabilidades y por así decirlo "secuestrar el sitio" con la finalidad de ejecutar ciertas acciones que perjudiquen directamente a los usuarios. Los catedráticos de la organización presentan la siguiente clasificación:

"4.- Phishing mediante introducción de contenidos (Content-Injection Phishing).

Esta modalidad consiste en introducir contenido malicioso dentro de un sitio web legítimo. Dicho contenido puede tener diversas modalidades: redirigir a los visitantes a otra página, instalar algún tipo de malware en el ordenador de los usuarios, etc. Básicamente, existen tres categorías principales de phishing mediante introducción de contenidos, a partir de las cuales surgen un número indefinido de variantes:

[35] Ídem.

• Asalto al servidor legítimo por parte de hackers que se aprovechen de una vulnerabilidad para modificar o introducir contenido malicioso en el sitio web.

• Introducción de contenido malicioso en el sitio a través de lo que se denomina una vulnerabilidad de "cross-site scripting", también conocido como XSS. El cross-site scripting es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envío de datos sin validación alguna, aceptando el envió de scripts completos, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el sitio o en el equipo de un usuario. Este tipo de vulnerabilidad puede afectar tanto a la aplicación web como a los usuarios que activen esa secuencia de comandos de forma involuntaria.

• Acciones maliciosas que pueden ser llevadas a cabo en un sitio a través de una vulnerabilidad de introducción de SQL (SQL injection vulnerability). Esta es una forma de provocar que sean ejecutados comandos de bases de datos en un servidor remoto que conlleven la filtración de datos confidenciales. Al igual que en el caso anterior, esta vulnerabilidad se debe a la ausencia de filtros adecuados en el servidor que impiden dicha ejecución.[36]"

En este caso, quien se encuentra en vulnerabilidad es la institución y por ende sus clientes. La entidad por conducto de sus técnicos debe desarrollar los mecanismos necesarios a efecto de brindar seguridad y mantenimiento constante a los servidores que mantienen activas las páginas, esto con la finalidad de proteger a sus clientes y/o usuarios, sobre todo en aquellos casos en los que dentro de las mismas exista flujo de información de carácter confidencial, como es el caso de los servicios de banca en línea o compras por internet.

Por consiguiente, una de las clasificaciones propuestas es aquella en la que existe un intermediario entre el sitio real y el usuario, se le denomina "man in the middle" o lo que es

[36] Ídem.

lo mismo “un hombre en medio”. Para este caso, lo que se intenta es crear una interrupción entre los sistemas de comunicación de las partes para que antes de que se concluya la transferencia de datos, quien se encuentra en medio pueda tener acceso a ellos antes de que lleguen a su destino final y así lograr la sustracción de los mismos. Los expertos han definido este fenómeno de tal forma:

> *“5.- Phishing mediante la técnica del intermediario (Man-in-the-middle Phishing o MitM)*
>
> *Aunque en muchas de las clasificaciones consultadas se considera ésta como una categoría dentro de los tipos de phishing, en realidad se trata de una técnica para efectuar el ataque. Como su propia denominación indica, implica el posicionamiento del phisher entre el ordenador del usuario y el servidor web legítimo. De este modo el delincuente se hace con la capacidad de filtrar, leer, e incluso modificar la información que se transfiere desde el puesto del atacado al servidor y viceversa, sin que las partes sean conscientes de la violación de su seguridad. Las consecuencias de esta actuación pueden ser tanto el robo de información confidencial, para su uso o venta posterior, o, directamente, el secuestro de la sesión (session hijacking), en cuyo caso podrá o no robar esa información. Nuevamente, el problema de esta variante es que el usuario no puede detectar que está siendo víctima de un delito ya que, aparentemente, todo funciona de forma correcta.[37]“*

Por último, la siguiente clasificación es una de las más utilizadas que consiste en registrar dominios o nombres de páginas web muy similares a los reales, para con ellos intentar confundir a los usuarios y redirigirlos a un sitio que no es el legítimo. Lo anterior se logra infectando diversos motores o plataformas de búsqueda tales como “Google” o “Yahoo”, en el que sitúan a sus sitios por encima de los fidedignos, una vez en éstos se espera que la utilicen como si de la real se tratara. Los integrantes de la organización aludida no explican lo siguiente:

[37] Ídem.

"6.- Phishing de motor de búsqueda (Search Engine Phishing)

Nuevamente más que un tipo de phishing es, en sí mismo, uno de los ardides empleados por los delincuentes para hacer que el usuario caiga en su trampa. Los delincuentes crean páginas web para productos o servicios falsos, las introducen en los índices de los motores de búsqueda y esperan a que los usuarios visiten las páginas para realizar compras y, por tanto, proporcionen información confidencial o directamente realicen transferencias bancarias. Normalmente las falsas ofertas tienen condiciones sensiblemente mejores a las ofrecidas por empresas legítimas, con el objetivo de atraer al máximo número de víctimas posible.

En este ámbito han tenido mucho éxito los fraudes en los que los phishers se han hecho pasar por bancos que ofrecen tipos de interés muy superiores a los ofrecidos por las entidades financieras reales. Las víctimas encuentran estos falsos bancos online a través de buscadores y, ante tal oferta, no dudan en abrir una nueva cuenta e introducir sus datos bancarios para realizar una transferencia...[38]"

La información proporcionada con anterioridad explica de manera clara, aunque un poco técnica, los diferentes tipos de ataque, que como se mencionó en párrafos anteriores no son la totalidad de ellos por la infinidad de combinaciones que se pueden utilizar para perpetuar un ataque, pero si son las más utilizados por los delincuentes para realizar phishing.

Ahora bien, es importante diferenciar entre los tipos de ataques y el lugar o lugares en que se materializan dichas estafas, es decir los sitios o plataformas web de los que se valen los ciberdelincuentes para lograr su cometido, en las cuales, aprovechándose del renombre de ciertas empresas, utilizan o suplantan sus sitios web debido a la gran tendencia, fama o buen desempeño de sus servicios[39], pues es un mercado numeroso debido al interés que mantienen los usuarios en su utilización, por lo que me permito enumerar los siguientes:

---

[38] Ídem.

[39] Cfr. http://www.malware.unam.mx/es/content/un-vistazo-la-situaci%C3%B3n-de-phishing-y-malware-en-m%C3%A9xico-abril-%E2%80%93-junio-2015. (Consultado 09/09/2017)

1.- Plataformas bancarias. Son los sitios más concurridos por los phishers, en estos los atacantes buscan robar números de tarjetas bancarias, NIP'S de seguridad, nombres de usuarios, contraseñas, códigos, etc.

2.- Plataformas de pago online. Dentro de las más utilizadas se encuentran la de Pay Pal, Visa y Master Card.

3.- Redes sociales. En estas se precisa principalmente obtener datos privados, robar cuentas de usuarios y la suplantación de identidad, los ejemplos más conocidos se dan en Facebook, Twitter, Linkedin, Instagram, etc.

4.- Páginas de compraventa y subastas en línea. En estas el móvil es robar cuentas de usuario para obtener beneficios materiales, o utilizar los datos robados como medio de estafa. Los sitios más vulnerables ante esta situación son sitios como Amazon, eBay, etc.

5.- Juegos online. Muchas de estas plataformas utilizan extensiones o items para hacer más atractivo el juego, mismas que se compran a en línea utilizando una tarjeta de crédito, uno de los ejemplos más conocidos es el de World of WarCraft, League of Legends o Sims[40].

6.- Soporte técnico y de ayuda de empresas y servicios. Dentro de los más conocidos se encuentran las de Apple, Yahoo, Gmail, Outlook, etc. en las que se les solicita a sus usuarios reactivar su cuenta introduciendo sus datos.

7.- Servicios de empresas públicas y privadas. Valiéndose de la reputación y seriedad de dichas empresas, utilizan la tima para engañas a los clientes y así les entreguen información confidencial o bien los estafan planteando una situación de riesgo.

[40] Cfr. https://malware.unam.mx/es/content/steam-plataforma-de-videojuegos-objetivo-de-phishing-y-malware (Consultado 01/09/2017)

8.- Plataformas de almacenamiento en la nube. El cometido más común es el de apropiarse de la información contenida en estos servidores para después venderla, así mismo utilizan la imagen de estas empresas para cometer el delito de la forma tradicional. Como ejemplo de estas empresas tenemos a Dropbox, Google Drive, etc.

9.- Servicios de mensajería o paquetería. Envían mensajes a los usuarios alertando sobre un posible envío, o un paquete que no ha podido ser entregado y le solicitan diversa información para que se subsane la omisión. Ejemplos de estos lo son DHL, Estafeta, etc.

10.- Falsas ofertas de empleo. Utilizan la necesidad de los usuarios, o engañan con propuestas de trabajo irresistibles, con la final de obtener datos personales que son utilizados posteriormente con fines fraudulentos.

Son múltiples los sitios en la red en los que debemos de conducirnos con premura, asegurando de manera fehaciente que los mensajes o correos electrónicos de esta índole que se reciban realmente provengan de los sitios reales, dejando entre dicho que ninguna de estas empresas solicita a sus clientes este tipo de información, pues utilizando el razonamiento de manera lógica ellos ya poseen ésta, por lo que debemos desconfiar en todo momento de este tipo de amenazas. Es recomendable contar con algún tipo de antivirus con la finalidad de prevenir intrusiones directas en las computadoras.

De manera explicativa más no limitativa, en párrafos precedentes se describen los supuestos en los que se desarrolla el phishing como una práctica ilegal en el mundo cibernético, que se traducen en daños e implicaciones de tipo jurídico en la vida real.

Una vez planteada la forma operacional y el estudio de sus principales características, es de relevante importancia hacer notar que en materia regulación tecnológica, México se encuentra sumamente rezagado en estudios doctrinales, legislación, políticas públicas y prevención, por lo que es necesario prestar especial atención en este rubro, debido a la elevada tendencia del uso de estos medios en todas y cada una de las acciones humanas

que por supuesto son creadoras de consecuencias jurídicas, por lo que ahora es pertinente analizar la relación del phishing con algunas áreas jurídicas.

1.4.- PHISHING Y DERECHO INFORMÁTICO.

Como se mencionó con anterioridad, son muchas las personas y empresas que día con día, dedican su tiempo, conocimientos y esfuerzos a efecto de transformar el mundo con sus ideas visionarias, creando, diseñando y mejorando las herramientas tecnológicas que hoy día tenemos a disposición a efecto de hacer más fáciles las distintas tareas que llevamos a cabo los seres humanos en nuestra vida cotidiana. Seguramente muy pocos somos capaces de percibir los enormes avances que ha tenido la tecnología en poco más de sesenta años, que es el tiempo en el que se han gestado la mayoría de los descubrimientos, a lo que ahora llamamos postmodernidad. Sin embargo, es de vital importancia que a la par de estos asombrosos descubrimientos que evolucionan rápidamente, también lo hagan las leyes, ya que, como todas las ciencias, en materia jurídica no puede quedarse rezagado y debe mantener un enfoque evolutivo, pues debe de adaptarse al nuevo entorno que se gesta en la sociedad.

Es por esto que la ciencia del derecho al ser una disciplina dinámica, tiene la necesidad de cubrir los aspectos más relevantes que se van presentando en la sociedad, tal es el caso de la informática, ciencia que ha evolucionado de manera inimaginable para muchos, pues ésta, ha creado un lazo con la mayoría de las actividades de manera positiva como negativa, pues es un hecho conocido que si bien facilita de manera preponderante las actividades que desarrollamos día con día, también puede tener un uso en perjuicio de la sociedad, por lo que existe la primordial necesidad de que la ciencia jurídica se aboque al estudio y la regulación de esta área especializada, con la finalidad de tener un mejor y mayor control sobre su uso en aras de respetar los derechos de su uso, aplicación y divulgación de la manera más segura posible.

Algunos tratadistas señalan que el derecho de la informática es una categoría propia de la ciencia jurídica que obedece sus propias reglas, debido a que surge de una inevitable respuesta social al fenómeno informático, por ende, éste se considera como un derecho exis-

tencialista en tanto que su existencia precede a su esencia[41], es decir que gracias a los nuevos descubrimientos y a las implicaciones tecnológicas, se pueden concebir dichas actividades como un punto importante a considerar para su regulación, pues por su gran atractivo logran captar la atención de la mayoría de la sociedad, quien en el afán de experimentar nuevas formas de interactuar utiliza este tipo de medios en su beneficio, por lo que es posible deducir que a partir de su creación surge la imperiosa necesidad de plantear las reglas necesarias a fin de que su uso no violente derechos de terceros.

Es pertinente señalar, que los esfuerzos realizados para regular la actividad informática se han venido dando en un ámbito global, pues debido a las características que reviste dicha ciencia, rebasa las barreras geográficas, pues su funcionamiento no obedece reglas de usos y costumbres específicas de alguna región o una cultura, debido a que su uso se amplía de manera inimaginable por la red de Internet, pero antes de hablar de este fenómeno tecnológico, conviene hablar específicamente acerca de lo que es el derecho informático y por qué su consideración y aplicación es tan importante para el desarrollo de la sociedad.

El doctor Julio Téllez Valdés, define al derecho de la informática como un conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática[42], entendiendo por informática el estudio que definen las relaciones entre los medios (equipo), los datos y la información necesaria en la toma de decisiones desde el punto de vista de un sistema integrado[43], es decir, que es un conjunto de conocimientos científicos y una serie de técnicas que permiten el proceso automático y racional de diversa información mediante el uso de las computadoras.

De tal manera, que el tratamiento de las computadoras implica una gran correlación en la actualidad con casi la mayoría de las disciplinas y se contemplan una serie de implicaciones de orden social, económico y por supuesto el jurídico.

---

[41] Vivant, Michel y otros. *Droit de l'informatique, Paris. Ed. Lamy.*
[42] Téllez Valdés, Julio, Derecho Informático, 4ª Edición, Editorial Mc Graw Hill, México 2009.
[43] Mora, Jose Luis y Enzo Molino, Introducción a la Informática, Editorial Trillas, México.

Ahora bien, dicho lo anterior es importante no confundir el derecho informático con la informática jurídica, si bien la primera es un sistema de leyes encargado de regular las aplicaciones técnico científicas de la informática y sus elementos en el entorno social, la segunda se refiere específicamente al procesamiento de datos e información de índole jurídica para su conservación en medios electrónicos que permiten hacer más fácil su manejo, archivo y divulgación con la ayuda de estos medios y aplicaciones computacionales.

Ahora bien, es importante considerar al derecho informático como una disciplina jurídica autónoma, pues existen una serie de fuentes y elementos distintivos que la colocan a la par de otras disciplinas jurídicas como es el caso de la legislación, que a pesar de que en México no se encuentra provisto de un código específico referente al tratamiento del Derecho informático, la materia es tratada en diversos ordenamientos jurídicos debido al fuerte nexo y su interdisciplinariedad con otras áreas jurídicas como en materia constitucional, civil, penal, laboral, fiscal, procesal, internacional, etc., además de que existen diversos ordenamientos jurídicos internacionales, que en un esfuerzo por unificar las reglas aplicables al fenómeno informático, han creado diversas comisiones para darle seguimiento y tratamiento al tema.

Así mismo, existe una serie de disposiciones pronunciadas por diversos tratadistas respecto al tema por lo que se puede deducir que tiene su propia doctrina, además de las diversas disposiciones y pronunciamiento de los tribunales en los que se han plantado diversas controversias de orden legal suscitados por la informática que se han traducido en disposiciones legales y jurisprudencia.

Dentro de las principales cuestiones respecto al tratamiento de las diversas disposiciones y reglas jurídicas aplicables al derecho informático, existen diversas problemáticas que hay que tener en consideración para su estudio e implementación, pues estas normas tienen la finalidad de prevenir y en su caso aplicar medidas coercitivas, dentro de las más relevantes el académico Téllez Valdés enumera la siguiente clasificación, mismas que me permito explicar brevemente:

- Regulación de la información como bien: Pues la digitalización de los datos y su tratamiento tiene un innegable carácter económico, por los que son susceptibles de ser objetos del comercio.

- Protección de datos personales: Debido a la digitalización y conservación de diversos datos sensibles, es menester tener especial cuidado en la divulgación de dicha información, pues bien podría causar un atentado a los derechos fundamentales debido al mal manejo y cuidado de los mismos.

- Flujo de datos transfronterizos: Debido a la gran facilidad que la digitalización ofrece a la transmisión de datos, es prioridad del Estado determinar las facilidades y restricciones sobre la distinta información que debe o no compartirse fuera del país.

- Protección de programas: Políticas enfocadas a la disminución y el tráfico de material protegido por restricciones intelectuales o derechos de autor, distribuidos o reproducidos en medios electrónicos.

- Delitos informáticos: Normas preventivas y coercitivas hacia la comisión de diversos ilícitos mediante el uso y la implementación de computadoras o programas cibernéticos.

- Contratos informáticos: Utilización de medios digitales como forma de manifestación de la voluntad susceptibles de ser atribuidas derechos y obligaciones que preponderantemente tengan un carácter económico.

- Implementos informáticos como medio probatorio: Estipulación del alcance que tienen los diversos medios tecnológicos como soporte probatorio, la veracidad de los mismos y la manipulación de las pruebas para su exacto estudio y calificación[44].

[44] Cfr. Téllez Valdés, Julio, Derecho Informático, Op. cit., pp. 59-60.

De lo previamente expuesto resalta la importancia de tener muy presente le estudio de la informática y sus aplicaciones en el ámbito jurídico, pues la trascendencia de esta materia se ha apropiado prácticamente de todas las ciencias y de algún modo el Estado a través de sus instituciones y demás mecanismos de gobierno es responsable de salvaguardar la integridad de los usuarios de los medios electrónicos, pues a pesar de ser ventajosos por los distintos motivos que ya han señalado a lo largo de este trabajo, también revisten cierto riesgo si no se toman las medidas y cuidados pertinentes.

Uno de los aspectos más importantes sobre los riesgos de la informática es el relativo a la comisión de conductas ilícitas cometidas utilizando un ordenador informático, pues la complejidad de estos, aunado a las diversas y variadas posibilidades que ofrece su buen manejo, la convierten en una herramienta los suficientemente poderosa a fin de llevar a cabo distintos tipos de delitos. Sin embargo, la computadora por sí misma es una herramienta estática que contiene información detallada en la cual se pueden ejecutar diversos programas para su funcionamiento en el mismo, lo que realmente le da el poder dinámico a dicha herramienta, es la conectividad que provee el servicio de internet, debido a que prácticamente gracias a este medio de transferencia de datos, los computadores o medios electrónicos pueden conectarse con cualquier otro en el mundo que se encuentre provisto del mismo servicio, por lo que para el estudio de este trabajo se analizará brevemente la figura del internet.

Según el Consejo Federal de la Red (FNC -Federal Networking Council- por sus siglas en inglés) en el año de 1995, estableció las bases para unificar el concepto de Internet, ellos lo definieron de la siguiente manera:

> *"Internet a un sistema global de información que está relacionado lógicamente por un único espacio de direcciones global, basado en el protocolo de Internet (IP) o en sus extensiones; es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles son IP; y emplea, provee o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas"*[45].

[45] http://www.tsi.com.pe/historia9.htm (Consultado 12/08/2015)

Cabe señalar que esta definición es bastante técnica, debido a que utiliza conceptos que no son regulares en el habla cotidiana, para mayor entendimiento, es posible decir que internet es una red de redes, que permite que diversos ordenadores se encuentren interconectados a la mayor red mundial, entre las que figuran líneas telefónicas, fibras ópticas y enlaces por radio, con la finalidad del envío y la recepción de datos codificados.

Una de las características más importantes del internet es que no tiene un control central, es decir, no existe un órgano matriz que dirija la información a un lugar en específico, consecuencia de esto es que la red de información puede provenir de cualquier lugar mundo, por lo que en la red la identidad de los usuarios es totalmente desconocida, hecho de suma relevancia debido a que la sociedad y el orden jurídico se encuentran sustentados sobre la identidad de las personas, pues se sabe realmente con quien se está tratando, es decir, la interacción es con un sujeto identificable o cognoscible. Dicha situación ocasiona una seria ventaja a los delincuentes para cometer todo tipo de conductas ilícitas en perjuicio de los usuarios de la red, quienes se escudan en el anonimato.

De lo anterior deriva como sub rama del derecho informático el estudio de los delitos informáticos, que evidentemente se relaciona estrechamente con la ciencia penal, al implicar actividades criminales, los diversos Estados han intentado de manera poco afortunada encuadrar este tipo de delitos en las figuras típicas de carácter tradicional tales como robos, hurtos, fraudes, falsificaciones, estafas, sabotajes, etc. Es necesario actuar de manera inmediata con la finalidad de darles el tratamiento especial que merecen por las características específicas que revisten este tipo de ilícitos.

Como se han mencionado con anterioridad existen diversas organizaciones globales que han mantenido los esfuerzos para el estudio de dichas prácticas, los cuales han desarrollado una serie de lineamientos y descripciones de los diversos tipos de actividades ilegales relacionadas con los sistemas informáticos, sin embargo, ninguna de ellas ha propuesto hasta la fecha un concepto referente a los delitos informáticos. El catedrático Calderón Martínez, propone la siguiente: "*por delitos informáticos se entienden aquellas conductas ilícitas de acuerdo con la ley penal cometidas en contra o con la ayuda de los sistemas in-*

formáticos que pueden ser perpetradas de un lado del planeta a otro, con efectos globales o locales..."[46].

Por su parte el experto en derecho informático Julio Téllez Valdés, propone la siguiente definición: "*son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (Concepto atípico) "Conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" (Concepto típico)[47].*

Otro concepto es el ofrecido por la abogada Ivonne Muñoz, quien en su obra define a los delitos informáticos como "*aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información cuya consecuencia sea el daño directo o indirecto en ellos, así como el mal uso de ellos.*[48]"

Derivado de los conceptos enumerados en párrafos precedentes, situamos a la figura del phishing como uno de los tantos delitos informáticos que se ejecutan en contra de los usuarios de la red, situación que por demás es materia de estudio del Derecho informático adminiculado estrechamente con el Derecho penal, categoría que de manera práctica se le ha denominado a esta ciencia por diversos juristas como "Derecho penal informático". Sin embargo, el o los sujetos pasivos víctima de este ilícito, además de ser usuarios de los diversos servicios que ofrece internet, también lo son de diversas instituciones financieras, que como ya se ha mencionado, ofrecen a los usuarios de la banca diversos instrumentos financieros que permiten realizar transacciones monetarias de manera sencilla por conducto de la red.

De tal manera que si los usuarios del sistema financiero sufren un menoscabo en su patrimonio derivado de un ilícito cometido utilizando la red, quienes deberán de otorgar la asesoría a fin de resolver dicha problemática son las instituciones bancarias emisoras de los diversos productos financieros, pues derivado de su función, al ser las encargadas de velar por la seguridad de los recursos monetarios depositados de manera benévola por los

[46] Calderón Martínez, Alfredo. Delito informático: reto para los sistemas penales del mundo; El Derecho en la Era Digital, 1ª Edición, Editorial Porrúa, México 2013.
[47] Téllez Valdés, Julio, Derecho Informático, 4ª Edición, Editorial Mc Graw Hill, México 2009. pp. 104-105.
[48] Muñoz Torres, Ivonne, Delitos Informáticos Diez Años Después, 1ª Edición, Editorial Ubijus, México 2009. pp. 18-19.

usuarios, es de suma importancia que cuenten con diversos mecanismos y procedimientos adecuados para enfrentar dichas situaciones, además de que mediante avisos públicos deberán de brindar la información necesaria a sus clientes con la finalidad de prevenirlos de dichas conductas.

La lógica de todo esto reviste en que la afectación directa que repercute a la víctima de phishing, de manera indirecta tendrá un impacto en la institución financiera que haya emitido el instrumento de crédito o avale las transacciones monetarias en la red y una vez que la falta de activos derive en una deuda incobrable por así llamarle, es el Estado, quien como máximo rector de las leyes y asuntos de índole económico, así como financiero, deberá de afrontar los estragos ocasionados por los delincuentes cibernéticos, pues al ser el pilar del funcionamiento, equilibrio y estabilidad económica del país, debe de mantener una actitud protectora que inhiba los estragos de dichas prácticas, sin embargo, dicho proteccionismo derivará en una afectación directa a la sociedad, quien de manera noble terminará respondiendo por los daños causados por las actividades ilícitas perpetuadas por medio de una computadora desde cualquier parte del mundo.

1.5.- PHISHING Y DERECHO MERCANTIL.

El derecho mercantil, se encarga de velar por el estudio de las relaciones comerciales atendiendo a la calidad de los sujetos quienes las realizan, el objeto susceptible de comercio, la relación contractual que vincula a las partes y el o los procedimientos que se han instaurado para su comisión, haciendo de ella una de las ciencias jurídicas más importantes que rigen las actividades naturales del hombre.

Sin duda, dichas actividades como se ha venido mencionando, se han adaptado de manera constante a los cambios industriales y tecnológicos, pues la capacidad de los comerciantes para comprar y vender bienes y servicios se ha incrementado de manera exponencial gracias a la implementación en sus métodos comerciales de las TICs[49] (Tecnolo-

[49] Este término se refiere a las diversas técnicas y herramientas tecnológicas, que permiten a los usuarios transmitir, procesar, almacenar información a través de medios digitales, mismas que se expresan en imágenes, audio y textos.

gías de la Información y la Comunicación) ya que en nuestros días ya no es suficiente elaborar bienes de manera masiva para solventar las necesidades de la población, sino que también es necesario distribuirlas a gran velocidad a lo ancho y largo del globo terráqueo.

Es por ello que ha sido necesario implementar las medidas y providencias necesarias con la finalidad de tutelar el bien jurídico de los sujetos comerciales, pero no por esto quiere decir que la implementación de estas tecnologías afecte en sí el acto de comercio, pues en esencia continúa siendo el mismo, únicamente hay que adecuar la normatividad y establecer un parámetro para aprovechar las ventajas que nos ofrecen dichos avances tecnológicos, verbigracia, el comercio electrónico, en el cual no es indispensable que los sujetos se encuentren de manera presencial para realizar cierta negociación pues es posible realizarla vía correo electrónico, un sitio web, o por teléfono celular.

Otro aspecto importante que ha impactado en las transacciones comerciales, es el método para liberar las obligaciones adquiridas por los negociantes, pues con la digitalización de la banca, la disposición de medios con chip electrónico como tarjetas de crédito o el denominado *e-cash,* o dinero electrónico, han hecho que las transacciones de grandes capitales de dinero se hagan de manera inmediata y segura, pues no es necesario trasladar los valores de un lado a otro físicamente, con el riesgo de que en su trayecto ocurran incidentes que puedan afectar su valor, empero, la aplicación de este tipo de innovaciones puede crear ciertas confusiones o errores, además de los distintos supuestos delictivos que se pueden presentar como fraudes o estafas electrónicas, así como clonación de los medios de pago como tarjetas de crédito, o cuentas electrónicas, por lo que es necesario reformular el marco normativo del sector bancario y financiero.

Precisamente es este el punto en donde converge la relación del phishing con el derecho mercantil, pues derivado de las relaciones comerciales en las que se utilicen ciertos medios electrónicos, así como medios de pago digitales cabe la posibilidad de ser una víctima potencial de este tipo de estafa o fraude, por lo que las instituciones financieras en conjunto con los mecanismos legislativos, deben de servirse de la experiencia con la finalidad de prevenir, atacar y castigar este tipo de conductas que ponen en gran peligro la estabilidad financiera de la sociedad.

Es decir, se deberían adoptar las medidas necesarias para que los sujetos de comercio desenvuelvan sus actividades dentro de un ámbito de seguridad jurídica y técnica, pues al ser los medios digitales un tanto complejos en su elaboración, más no en su funcionamiento o utilización, en obviedad de razón para que sean accesibles al público en general, de tal manera que se necesita atención especializada para su tratamiento, pues quienes cifran, crean, o bien quienes conocen bien dichos instrumentos en ciertos casos podrían llegar a manipularlos en su beneficio, las cuales se traducen en ganancias lucrativas que a falta de legislación no tuviesen el carácter de ilegales.

1.6.- VULNERABILIDAD ANTE EL PHISHING DE LAS INSTITUCIONES FINANCIERAS.

En el primer semestre año del dos mil quince, se han registrado al menos 50 millones de ataques de phishing alrededor de todo el mundo, en América Latina Brasil es uno de los países más afectados por dicha actividad ilegal con un porcentaje del 18% de los ataques recibidos, mientras que en México las estadísticas se encuentran entre un 8% y 11% según la empresa informática karspersky[50], como actualización para 2016, la cifra aumentó a 398 millones de ataques detectados, de los cuales el 47% pertenece a ataques perpetuados en contra del sector bancario[51], situación que por más es alarmante debido a que dichas estadísticas han sido arrojadas únicamente para América Latina, por lo que nuestra Nación, en porcentajes, es una de las más afectadas en todo el mundo debido a que no existen las medidas y mecanismos suficientes que permitan la prevención, difusión y erradicación de dicha práctica.

Es alarmante encontrar diferentes tipos de notas acerca de estos delitos en los que se puede apreciar que los ciberdelincuentes en un solo ataque pueden robar más de novecientos millones de euros a diferentes instituciones financieras alrededor de todo el mundo, tal como es como se narra en un artículo publicado en la revista Quo, el atraco referido, se califica como una operación sin precedentes, pues para realizarlo, los hackers in-

[50] http://www.cnnexpansion.com/tecnologia/2015/06/03/rompase-en-caso-de-phishing-que-hacer-antes-y-despues (Consultado 17/02/2015).
[51] http://www.bbc.com/mundo/noticias-37286420 (Consultado 28/10/2017)

fectaron los ordenadores de la entidad financiera con la utilización de *malware,* para dar paso al uso de la técnica conocida como phishing, que emula un software legal con el fin de capturar las contraseñas, saber los horarios de operación y recogidas de dinero de los cajeros automáticos, así como acceder a los sistemas de video vigilancia[52].

Dada esta situación se puede apreciar que utilización de los diversos medios tecnológicos para la realización de las diversas operaciones monetarias en los portales web de las diversas instituciones financieras, supone cierto riesgo para los usuarios y para la misma institución, pues al no contar con un sistema de protección adecuado y personal capacitado con conocimientos técnicos actualizados y las habilidades necesaria que les permitan prevenir o detectar dichos ataques, situación que facilita en gran medida la actividad del hacker para poder perpetuar este tipo de delitos sin problema alguno puesto que, para perpetuar este tipo de fraudes únicamente se necesita de un computador con conexión a internet y conocimientos de informática, todo sin siquiera tener que desplazarse de un lugar a otro, situación que está por demás decirlo, pone en una situación comprometida a todas las instituciones financieras del mundo, pues los hackers buscan las vulnerabilidad de los sistemas informáticos, mediante las cuales aprovechan para recabar los datos necesarios para poder efectuar las actividades fraudulentas.

Además del menoscabo económico que sufren las instituciones financieras es importante resaltar que otro de los objetivos de los *phishers* es la obtención de información, misma que se traduce en una base de datos personales, los cuales evidentemente tienen cierto valor económico en el mercado. Según un sondeo practicado por la empresa de seguridad *Fortinet*[53]*,* solo el 22% de los consumidores mexicanos confía en el manejo que hacen las instituciones financieras de sus datos personales en el entorno cibernético, lo que nos indica un gran grado de desconfianza de los usuarios hacia las instituciones financieras respecto al resguardo de su información privilegiada. Aunado a esto, la digitalización de los medios financieros, como de la banca electrónica, a los usuarios no les queda más alternativa que la utilización de los mismos, pues los métodos tradicionales se han ido inutili-

[52] http://www.quo.es/tecnologia/un-grupo-de-hackers-roba-900-millones-de-euros-a-100-bancos (Consultado 17/02/2015).
[53] http://www.cnnexpansion.com/mi-dinero/2015/05/20/mexicanos-desconfian-de-la-ciberseguridad-de-sus-bancos (Consultado 18/09/2017)

zando de manera gradual, por lo que también se hace necesario que los cuentahabientes se hagan conscientes de que existe una enorme problemática respecto del uso de los medios electrónicos, pues su utilización debe de ser de manera responsable, así mismo deberán ser más asertivos a la hora de elegir el servicio financiero a aquel que les brinde una mayor protección, para que de tal manera la competencia de unas y de otras incentive la alza en la calidad y medidas de seguridad que ofrecen las entidades financieras.

Por su parte en México según datos recabados por la CONDUSEF (Comisión Nacional para la Protección y Defensa de los Usuarios de los Servicios Financieros) en lo que va del primer semestre del año 2015, los reclamos ante dicha institución por fraude y suplantación de identidad ascienden aproximadamente a 118 millones de pesos, además se reporta que se han atendido un millón seiscientos ochenta y tres mil seiscientas sesenta y un quejas por fraude y suplantación de identidad las cuales representan el 68.7% del total de quejas presentadas ante esa institución que equivalen en su totalidad a 2 millones 451 mil 370 quejas atendidas en su totalidad,[54]muchos de los cuales se han perpetuado a través de medios electrónicos.

Lo más grave del asunto es que aunque la mayoría de los atacantes tiene la ideología de desfalcar únicamente a las instituciones financieras sin perjudicar a los usuarios, de alguna manera esto se vuelve imposible, dado que en muchos casos los fraudes son realizados a tarjetas de débito, las cuáles en buena parte se encuentran ligadas a cuentas de nómina, es decir las cuentas en las que los trabajadores reciben su salario, por lo que aunque en algún momento dado sea procedente la reclamación del fraude ante la entidad bancaria, al momento las cuentas de los usuarios quienes son el pilar de las instituciones financieras en su calidad de usuarios, se ven afectados de manera directa, pues quedan sin la oportunidad de disfrutar de su dinero, pues éste ya ha sido transferido a otro lugar creando serios daños y perjuicios a la sociedad en general.

Es por todo esto que las entidades reguladoras del sistema financiero así como las mismas instituciones, deben de trabajar en conjunto para establecer las medidas de seguridad

[54] http://www.jornada.unam.mx/ultimas/2015/09/14/fraudes-financieros-crecieron-14-este-ano-condusef-164.html (Consultado 18/09/2017)

adecuadas para prevenir, informar, identificar y erradicar este tipo de fraudes electrónicos que tanto daño hacen a la estabilidad económica de la nación, poniendo en riesgo el patrimonio de miles de familias de mexicanos que utilizan estos productos financieros como medio de ahorro, pago y otros, conforme las exigencias que se van presentando de manera ininterrumpida debido a la globalización y digitalización del mundo.

CAPITULO SEGUNDO.
REGULACIÓN DEL PHISHING EN MÉXICO Y EL MUNDO.

Como tal no existe un marco normativo en nuestro país que regule la figura del phishing, para su análisis dogmático es de suma importancia para este trabajo de investigación, proponer y analizar las vías legales que se deberán de adoptar para en algún momento conseguir su regulación a efecto de prevenir, difundir, identificar, materializar jurídicamente y erradicar dicha figura, por lo que en este capítulo se estudiarán diversas disposiciones normativas que se han ido introduciendo los diversos ordenamientos legales alrededor de mundo, específicamente los del Estado Mexicano, regulando de una manera generalizada las diversas prácticas cometidas utilizando medios informáticos. Además, es importante analizar las diversas disposiciones internacionales que contemplan dentro de su sistema jurídico este tipo de actos jurídicos cometidos en la red, experiencias que podrán ser adaptadas y homologadas a la legislación aplicable.

2.1.- CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

México está rezagado en el estudio jurídico de las disciplinas informáticas, en su implementación y los riesgos que conllevan su utilización. En la Carta Magna se han ido adecuando a diversos preceptos tanto de la parte orgánica como en la dogmática, cuestiones relacionadas con las nuevas tecnologías, protección de datos personales, etc. hechos que son de suma importancia, pues al ser la constitución el pilar de nuestra organización política como sociedad, en ella se deberán de establecer las bases necesarias para la protección de la ciudadanía mediante la delimitación y reconocimiento de los derechos humanos relacionados con tales tecnologías, hasta la implementación por parte del estado en su organización, así como en sus procesos para un mejor desempeño en las atribuciones de gobierno.

Existen distintos preceptos en la Constitución General de la República que se encuentran de alguna manera vinculados con la figura del phishing, pues al ser en especie una actividad que se configura realizando diversas acciones para su comisión, tiende a transgredir diversas esferas jurídicas, en específico de los derechos fundamentales que se encuentran contenidos en la primera parte de dicho ordenamiento, como lo es el caso de la obtención de información personal o confidencial de los usuarios sin consentimiento alguno, el prejuicio económico que soslaya los derechos fundamentales, el abuso de las tecnologías para la comisión de actividades ilegales en perjuicios de terceros, así como al sistema financiero.

Así mismo, la norma suprema establece la organización de la nación bajo un sistema federativo en el cual, otorga a cada uno de los estados que la conforman la capacidad y las atribuciones para crear sus propias regulaciones atendiendo a las diversas características usos y costumbres de cada región, poniendo siempre como base las prerrogativas contenidas en la misma, pues las normas que rigen en los estados jamás podrán ser contrarios a los principios contenidos en la Constitución así como a los tratados internacionales de los que México sea parte.

Por lo que atendiendo a las máximas que se encuentran establecidas en dicho ordenamiento, los estados por conducto de sus organismos y autoridades competentes deberán de ocuparse de las necesidades que día con día surgen en la vida cotidiana, como lo es todo lo relacionado con el auge de las nuevas tecnologías, así como sus implementaciones en todos los ámbitos de la sociedad. Uno de los principales rubros a estudiar y desarrollar, son los contenidos en las legislaciones penales, puesto que la actualización de los delitos cometidos en medios electrónicos cada vez es más recurrente, los estados además de ubicar y delimitar dichas conductas deberán buscar la coordinación con la federación y los municipios a efecto de implementar las medidas más eficientes para su prosecución, siempre haciendo lo concerniente dentro del marco de la ley.

El artículo 6° constitucional, además de garantizar la libertad de expresión a través de cualquier medio, así como la obtención de información que sea susceptible de ser de

dominio público, en su párrafo tercero establece de manera determinante que es obligación del Estado garantizar el derecho de acceso a las tecnologías de la información y comunicación, dentro de los cuales expresamente se encuentra incluido el de banda ancha e internet. Dada dicha prerrogativa, derivado de los antecedentes planteados de la figura del phishing, internet es el medio idóneo para la comisión de dicha especie de fraude, por lo que no es suficiente que se garantice a la población el acceso a una conexión a la red informática, sino que además deberán de establecerse las medidas necesarias para que su utilización no conlleve un riesgo para los usuarios, que, en lugar de representar una ventaja, resulte en un perjuicio o riesgo para estos.

El artículo 25° constitucional en su segundo párrafo, menciona como obligación del estado velar por la estabilidad de las finanzas públicas, así como del sistema financiero, este último para el tema que nos atañe es de primordial atención, pues el phishing ataca directamente de manera lastimosa a la estabilidad de las instituciones financieras y por ende a la estabilidad económica de los usuarios y del país. El estado debe en total coordinación con los organismos rectores y reguladores del sistema financiero mexicano como lo son la Comisión Nacional Bancaria y de Valores, el Banco de México, así como la Secretaría de Hacienda y Crédito Público, La Comisión Nacional para la protección y defensa de los usuarios de los servicios financieros, deben de encontrar y plantear los mecanismos que permitan mantener en un estatus equilibrado y saludable las finanzas del Estado Mexicano, detectando de manera inmediata las situaciones que ponen en riesgo a las instituciones financieras, cómo es el caso de los delitos patrimoniales que se efectúan en la red.

La clave para lograr una buena implementación de los mecanismos en beneficio de la estabilidad financiera es que tanto instituciones como estado persigan el mismo objetivo e ideología de mantener saludable el desarrollo económico con aras de crecimiento equitativo y no solo personal. Es importante resaltar puntos específicos en los cuales debe prestarse mayor atención y áreas de colaboración entre unos y otros, pues si alguno de los dos se encuentra corrompido o en busca de intereses diversos, será más fácil para los delincuentes penetrar en un sistema resquebrajado y más difícil que un país crezca económicamente de una manera constante y adecuada.

Dentro de la parte orgánica de la constitución específicamente hablando del artículo 73°, de dicho ordenamiento, se encuentran contenidos los rubros principales respecto de los cuáles el Congreso de la Unión debe y tiene la facultad de legislar. La fracción XVII, de dicha disposición normativa, determina que el Congreso deberá de fijar las leyes necesarias con la finalidad de regular acerca de las vías generales de comunicación, tecnologías de la información, dentro de las cuales se encuentran incluidas la banda ancha y el internet, que para el caso específico de nuestro tema de tesis, es de suma importancia debido a que este apartado nos da la oportunidad de ahondar en los diversos temas relevantes del mundo tecnológico, pues no debe entenderse únicamente sobre el desarrollo de la infraestructura y desarrollo de dichos medios, sino deberá ser un trabajo legislativo inclusivo, en el cual se deberán de abarcar y ahondar en todas las posibilidades y vertientes en las que deriva el uso de las nuevas tecnologías.

Por otro lado la fracción XXIII, establece la facultad al congreso de legislar respecto diversas disposiciones de coordinación entre la Federación, el Distrito Federal (ahora Ciudad de México), los Estados y los Municipios en materia de seguridad pública, pues para la prosecución, investigación, prevención, sanción y erradicación de delitos cometidos con el uso de medios electrónicos, es de suma importancia se creen dependencias especializadas encargadas de perseguir dichas conductas antijurídicas, con la finalidad de salvaguardar el bienestar de la sociedad en común dentro de todos sus rubros, pues al ser estas actividades innovadoras y de veloz desarrollo, se necesita la investigación inmediata de los nuevos métodos que utilizan los ciberdelincuentes, así como una extensa coordinación a fin de detectarlos y difundir información importante que pueda ayudar a disminuir el impacto de dichas prácticas en los tres órdenes de gobierno.

Otra de las grandes problemáticas que auxilian a que la figura del phishing prospere, es la gran fuga de diversa información con el carácter de personal que con el paso del tiempo ha sido obtenida por diversas instituciones públicas y privadas, pues dicha información como ya se ha mencionado con anterioridad, representan o se pueden traducir en un bien susceptible de comercialización, por lo que en la Constitución Política

de los Estados Unidos Mexicanos, se ha establecido como un derecho fundamental la protección y manejo responsable de dicha información con diversos mecanismos que permiten a las personas tener acceso a dichos datos, así como a su rectificación, oposición a su divulgación, entre otras cuestiones. El artículo en comento en su fracción XXIX-O, atribuye al Poder Legislativo la facultad de legislar en materia de protección de datos personales en posesión de particulares, así como la fracción XXIX-S, en materia de protección de dichos datos personales en posesión de las autoridades, entidades, órganos, y organismos gubernamentales en todos los niveles de gobierno.

El tráfico de dicha información facilita la actividad delictiva, pues la filtración, fuga, robo o transmisión sin consentimiento de esos datos transgrede directa e indirectamente diversas esferas jurídicas dependiendo el caso en específico, pues al tener perfectamente identificados los datos personales de cada persona, como lo pueden ser números telefónicos o estados de cuenta bancarios en los cuales se puede obtener información detallada respecto del monto económico del que es susceptible cada persona, además de la institución bancaria de la que es cuenta habiente, conlleva a que los ataques de phishing cuenten con una mejor elaboración y sean más personalizados, por lo que su margen de error disminuye considerablemente y tienen más oportunidad de consumar el delito favorablemente.

Se aprecia que aunque son pocas, las diversas prerrogativas y facultades que se encuentran consagradas en la Constitución General, son suficientes para poder elaborar un sistema normativo que nos permita regular de manera adecuada la práctica del phishing en la mayoría de rubros posibles, preceptos jurídicos, así como medidas y mecanismos eficientes que limiten de manera contundente el tráfico de información, situación que debe de ser por más atendida, pues las grandes bases de datos de información hoy en día se encuentran resguardadas en archivos electrónicos, mismos que no necesitan de una espacio físico considerable para ser trasladados de un lugar a otro, o bien que sean sustraídos mediante intrusiones a los sistemas computacionales por algún hacker con la intención de venderlos o utilizarlos para fines ilegales que al final del día se transmiten en un lucro indebido.

Otra de las prerrogativas que concede nuestra norma superior es la oportunidad de adoptar diversos ordenamientos o suscribir tratados o convenios internacionales de diversa índole, pues la experiencia de otros estados puede ayudarnos a sentar las bases para una mejor regulación y entendimiento de los fenómenos tecnológicos que en su mayoría ya se presentaron y desarrollaron en algún país del primer mundo, por lo que su inclusión en nuestro sistema jurídico de alguna manera debería de permitir que los daños sean menores, mismos ordenamientos que estudiaremos en el apartado siguiente.

2.2.- CONVENIOS Y TRATADOS INTERNACIONALES.

En los últimos años se han estado realizando esfuerzos significativos tanto de instituciones públicas, como privadas, para el desarrollo de sistemas y de regulaciones especializadas que nos permitan tener una mayor seguridad al navegar en la red, siendo algunos de los puntos primordiales la protección de información y datos contenidos en sistemas informáticos. Dentro de las agendas de los grandes paneles internacionales se discuten temas acerca del desarrollo económico de las naciones, así como de seguridad nacional, actividades que hoy en día se desarrollan en su mayoría con la implementación de sistemas computacionales, por lo que es necesario desarrollar diversos mecanismos para su implementación, de tal manera que se permita exitosamente el crecimiento de los países en vías de desarrollo.

Algunos de los principales organismos internacionales como los son: La Organización de las Naciones Unidas, el G-8, La Unión Europea, La Organización para la Cooperación y Desarrollo Económico (OCDE), La Organización de los Estados Americanos (OEA), entre otras organizaciones internacionales y regionales han puesto en diversas ocasiones el asunto de la ciber seguridad sobre las mesas de discusión, no obstante, la falta de regulación y legislaciones acerca de estos temas dentro de los países más afectados, es lo que dificulta en mayor parte la armonización de los mecanismos adecuados para la correcta solución de dicha problemática.

Existe un gran reto en el ámbito jurídico nacional e internacional para propiciar las defensas adecuadas contra los delitos cometidos con el uso de sistemas tecnológicos e informáticos, como se ha mencionado en repetidas ocasiones los cibercriminales constantemente se encuentran diseñando y desarrollando una serie de nuevos ataques y técnicas para la comisión de diversas actividades ilícitas por medios informáticos, actividad que se ha venido dando desde su aparición, pues es un instrumento que permite de manera fácil y anónima obtener ganancias ilícitas.

La tarea que deben de seguir de manera determinante y urgente los Estados, una vez que dentro de sus políticas internas definan el ámbito de la ciber seguridad como importante o prioritaria, es la de adherirse a los diversos convenios o tratados internacionales existentes, lo cual facilitará de manera importante la adecuación de la legislación interna, así como el tema de coordinación entre los Estados firmantes con la finalidad de un mejor manejo de la información y protección de datos que se transfieren mediante el internet.

El Consejo Europeo en diversos argumentos manifiesta la importancia de la adhesión de los Estados a los tratados internacionales de esta índole, de la siguiente manera:

> "En primer lugar, esta clase de delitos no tienen fronteras para ser cometidos; en segundo lugar, afectan bienes intangibles tales como datos e información electrónica; en tercer lugar, la conexión a Internet da al delincuente anonimato al utilizar herramientas informáticas avanzadas para ocultar su identidad; y, finalmente, las pruebas para comprobarlo son difíciles de recabar, más cuando el delito se ha cometido en otra jurisdicción distinta a la de la víctima afectada"[55].

Una vez que quedó plasmada la importancia de los tratados internacionales para el estudio de la figura jurídica del phishing, nos enfocaremos a estudiar brevemente los diversos ordenamientos internacionales que de manera oportuna establecen las bases para el tratamiento de esta figura delictiva y de otros delitos que afectan de manera inminente al mundo entero.

[55] Octopus, 'Organized crime in Europe: the threat of cybercrime', Council of Europe, 2005, pp. 81-212.

El ordenamiento Internacional más importante es el denominado “The Convention on Cybercrime” (ETS) 185, la cual en español se le conoce como “Convenio sobre Ciberdelincuencia” o “Convención sobre Delitos Informáticos” o “Convenio sobre cibercriminalidad de Budapest” este último nombre dado por haber sido discutido en Budapest el 8 de noviembre del año 2001, y abierto a firma el día 23 del mismo mes por el Comité de Ministros del Consejo de Europa en la sesión Nº 109, entrando en vigor hasta el primero de julio de 2004.

La relevancia de dicho convenio radica en que fue el primer acuerdo internacional en el que se establecieron de manera determinante todos los aspectos relevantes de la legislación sobre ciberdelincuencia dividiéndolo en tres áreas específicas las cuales son: Derecho Penal, Derecho Procesal y Cooperación Internacional. Además de abarcar de manera importante aspectos tales como seguridad de información y tratamiento de delitos contra la confidencialidad, Integridad y disponibilidad de datos, así como de los sistemas informáticos.

Otro de los aspectos importantes es que le Consejo Europeo cuenta con un gran número de miembros, para ser precisos, son 47 Estados los que lo conforman, mismos que trabajan de manera conjunta con 8 estados observadores entre los que se encuentra México, quien participa como observador desde el primero de diciembre de 1999. Sin embargo, México únicamente ha exteriorizado la intención de adherirse a dicha convención, a pesar de haber sido invitado abiertamente desde el 31 de enero de 2007, sin que hasta la fecha se haya realizado[56].

Dentro de las principales preocupaciones que motivaron la elaboración de dicho convenio, es la preocupación que se tiene derivada del riesgo que se generó a partir de la digitalización, globalización de las redes e información electrónica sean utilizados para cometer delitos informáticos, por lo que es importante y necesario aplicar con carácter prioritario una política penal, en aras de proteger la estabilidad financiera del país, contra los delitos cibernéticos, acciones que según el mismo convenio, serán posibles

[56] Cfr. http://www.excelsior.com.mx/hacker/2016/12/07/1132670 (Consultado 10/09/2017)

adoptando una legislación adecuada que además de tipificar dichos delitos, fomente la cooperación internacional contra la ciberdelincuencia.

Dicho ordenamiento, busca complementar de manera armónica otros convenios o tratados multilaterales en el aspecto informático, dentro de la convención se establecen diversos aspectos como el de la libertad en los sistemas informáticos, como el de expresión, búsqueda, comunicación y obtención de información en internet, en atención a lo dispuesto en las diversas convenciones de Derechos Humanos. Otros de los aspectos relevantes son aquellos como los de propiedad intelectual, pornografía infantil, así como cooperación y asistencia jurídica internacional.

Otro de los rubros importantes del Convenio de Budapest, es que establece el funcionamiento adjetivo que deberán de adoptar los países firmantes, es decir el aspecto procesal, en la cual guía a los suscriptores a legislar y adoptar las medidas necesarias para tipificar en su derecho interno cuestiones de prácticas tales como acceso ilícito a un sistema informático, intervención ilícita de datos informáticos, interferencia en los datos informáticos, interferencia en sistemas informáticos, así como el abuso de dispositivos de dicha índole[57]. Por otra parte, también establece los principales delitos cometidos con el uso de la red, como lo son la falsificación a través de medios informáticos, el fraude informático, pornografía infantil y aquellos relacionados con infracciones a la propiedad intelectual y derechos afines.

También, establece el grado de responsabilidad de las personas o corporaciones que cometan dichas prácticas ilícitas, así como las posibles sanciones que deberán de ser aplicadas a los infractores. Dentro de los principales aspectos a consideran son los relativos a la tentativa y complicidad, la responsabilidad de las personas jurídicas en aspectos penal, civil y administrativos.

Por último, el aspecto predominante relativo a la colaboración internacional en el cual se establece que las partes desarrollarán métodos esenciales para la obtención, con-

[57] Cfr. http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf (Consultado 12/09/2017)

servación y difusión de la información que pueda ser relevante para una investigación, así como la implementación de un sistema que funcione 24/7, a efecto de dar atención a las solicitudes realizadas por otro estado en un aspecto de colaboración para perseguir una actividad criminal.

Para efectos prácticos respecto del estudio de la figura del phishing en dicho convenio, existen dos artículos principales que dan pie a la elaboración de la legislación pertinente para su prosecución siendo en primer lugar el artículo 7º relativo la falsificación informática en el cual se establece lo siguiente:

> "*Articulo 7- Falsificación Informática. - Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos de datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal*[58]*."*

Dicho precepto puede encuadrar al estudio de la figura del phishing, pues como se mencionó en el capítulo anterior del presente trabajo, uno de los elementos que produce el engaño a la víctima, es la falsificación de los logos o sitios web de las instituciones bancarias comerciales reconocidas, con la finalidad de que se consideré que el mensaje que está recibiendo es fidedigno y acceda a proporcionar la información que se solicita, por lo que la falsificación de dichos componentes constituye de manera tajante un elemento esencial para la integración de la figura del phishing.

Por otra parte, el artículo 8° de la Convención de Cibercriminalidad señala las características que habrán de cumplirse para que se materialice el fraude informático de la manera siguiente:

[58] Ibidem p. 6

> "Articulo 8- Fraude Informático. - Las partes adoptaran las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen prejuicio patrimonial a otra persona mediante:
>
> a. La introducción, alteración, borrado o supresión datos informáticos:
> b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona[59]."

De tal manera puede observarse que se considerará como fraude informático a cualquier acción encaminada a obtener un beneficio económico de manera ilegítima mediante el uso de sistemas computacionales, situación en la que encuadra a la perfección el phishing.

Un segundo ordenamiento legal en el cual México tiene injerencia es el "Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia" mismo que fue firmado por el Procurador General de la República, Jesús Murillo Karam, documento que se abrió a firma el 28 de mayo de 2014[60], el cual tiene como objeto reforzar la cooperación mutua de las partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia.

De tal manera que dicho ordenamiento únicamente sirve de base para la organización y cooperación internacional en un ámbito adjetivo o procesal, pues delimita los pasos o medidas a seguir para solicitar la cooperación o envío de información relativa a algún crimen cometido por medios electrónicos o para la recolección y aseguramiento de las pruebas que ayuden a su prosecución, a comparación del convenio de Budapest en el cual si contiene derecho sustantivo.

---

[59] Ídem.
[60] Cfr. http://www.elfinanciero.com.mx/sociedad/mexico-suscribe-convenio-iberoamericano-contra-la-ciberdelincuencia.html (Consultado 12/09/2017)

Existen pocos ordenamientos internacionales relacionados con México en materia de ciberdelincuencia, aunque no son determinantes para que en el ámbito local se elaboren las legislaciones pertinentes para el tratamiento de estas conductas antijurídicas, si son importantes, pues como se ha mencionado en ocasiones anteriores el internet rebasa cualquier frontera y los ataques pueden ser perpetrados desde cualquier ordenador en cualquier parte del mundo.

Con las recientes reformas en materia de telecomunicaciones, se ha abierto la puerta para que de manera inmediata México pueda adherirse al Convenio de Budapest, tal y como se mencionó en el "TALLER SOBRE LEGISLACIÓN EN MATERIA DE CIBERDELINCUENCIA EN AMÉRICA LATINA" coauspiciado por el Gobierno Mexicano y el Consejo de Europa, en el que se mencionó que se encuentran dadas las condiciones políticas y jurídicas para que pueda concluirse dicho proceso, lo cual permitirá al país colocarse a la vanguardia a fin de responder a las necesidades de la sociedad en el combate a la ciberdelincuencia[61].

2.3. LEGISLACIÓN FEDERAL.

2.3.1. LEY DE INSTITUCIONES DE CRÉDITO.

Esta ley general, cuya última reforma en diversas disposiciones ha sido publicada el 17 de junio de 2016[62], aunque en obvio de repeticiones, tampoco contempla aspecto alguno referente a la figura del phishing, no obstante lo anterior, ha sufrido una serie de cambios en su apartado de delitos, la última de ellas realizada el 26 de junio de 2008[63], referente a conductas típicas cometidas mediante la utilización de medios electrónicos, específicamente de aquellas de falsificación, producción, reproducción, distribución, fabricación, comercialización, alteración, posesión, adquisición, utilización, etc. de tarjetas expedidas por el Sistema Bancario Mexicano utilizadas como instrumentos de pago.

---

[61] https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf (Consultado 18/09/2017)

[62] Cfr. http://www.diputados.gob.mx/LeyesBiblio/pdf/43_170616.pdf (Consultado 12/09/2017)

[63] Ibídem pp.286-288.

La cadena delictiva de la falsificación de tarjetas bancarias es cometida por bandas de crimen organizado, inicia con los delincuentes que se dedican a conseguir ilícitamente la información contenida en las tarjetas, la cual se obtiene generalmente en establecimientos que dentro de sus métodos de aceptación de pago es la de recibir dichas tarjetas que se encuentran afiliadas a diversas instituciones bancarias emisoras de dichas tarjetas[64]. Los delincuentes utilizan un aparato llamado "skimmer", que es un lector de memorias del tamaño de un localizado o un teléfono celular, en el cual con solo deslizar la banda magnética que contienen las tarjetas en dichos aparatos, permite reproducir o clonar la identidad de la tarjeta.

En segundo lugar, se encuentran aquellos que se encargan de la operación tecnológica, pues son expertos en programas de computación, que se encargan de falsificar las tarjetas bancarias traspasando la información obtenida por el "skimmer" a una nueva para posteriormente transmitir la propiedad o venderás a usuarios de mala fe. El tercer momento se presenta a la transmisión de estos plásticos falsificados a terceros de mala fe, que deciden adquirir dichos instrumentos apócrifos con la finalidad de adquirir bienes y servicios en prejuicio de las instituciones emisoras de tarjetas, así como de los tarjetahabientes[65].

La importancia de esta reforma es la de mitigar este tipo de fraudes, que aunque no tienen nada que ver con la figura en estudio, ocasionan pérdidas millonarias a las instituciones emisoras de las tarjetas, a los negocios y a los tarjetahabientes, por consiguiente, se vuelve inmediatamente necesario que mediante los instrumentos jurídicos necesarios se brinde completa certidumbre a las empresas y familias mexicanas que utilizan como medio de pago autorizados por el sistema bancario, no obstante, la proliferación de diversas conductas especializadas cometidas mediante el uso de medios electrónicos como lo es el phishing, dejan completamente obsoleta la legislación planteada casi de manera inmediata, pues como se ha mencionado los métodos utilizados por los ciberdelincuentes cada vez se vuelven más elaborados.

[64] Cfr. http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/667-clonacion-de-tarjetas (Consultado 12/09/2017)
[65] Cfr. https://www.bbva.com/es/skimming-la-estafa-la-clonacion-tarjetas/ (Consultado 12/09/2017)

Cabe precisar que para que esta reforma tuviese mayor impacto, además se modificó el artículo 194, del Código Federal de Procedimientos Penales en su fracción VIII[66], para que los delitos contenidos en los artículos 112 bis, 112-Ter, 112-Quáter y 113-Bis de la Ley de Instituciones de Crédito fuesen considerados como delitos graves, pese a que al día de hoy éste ordenamiento se encuentra derogado por el actual Código Nacional de Procedimientos Penales, en el cual ya no se encuentra contenido un catálogo de los delitos mencionados, en palabras de la licenciada Mónica Daniela Velázquez, lo explica de la siguiente forma:

> "…una vez que se inician las reformas en materia penal, con la Creación del Código Nacional de Procedimientos Penales, y su entrada en vigor, quedan abrogadas las leyes adjetivas en la materia que correspondían a la legislación aplicable en cada una de las entidades federativas.
>
> El problema radicara (sic) al momento en el que este nuevo Código, no se estable un catálogo, y mucho menos una definición de que es un delito grave, al contrario, solo encontramos una referencia de ellos en lo relacionado a la prisión preventiva y a los casos de urgencia, como se citan en los artículos 167 y 150 respectivamente.
>
> El Código Nacional de Procedimientos Penales, persigue objetivos claros como lo es lograr que la impartición de justicia sea justa y económica, así como la aplicación del principio pro homine. Sin embargo, bajo estos objetivos es posible encontrar inconvenientes en la aplicación del mismo; ejemplo de ello es la poca claridad y con ello la falta de certeza en la determinación de los delitos graves.[67]"

[66] Véase artículo 194 Código federal de procedimientos penales, ordenamiento derogado. (Consultado 12/09/2017) https://www.juridicas.unam.mx/legislacion/ordenamiento/codigo-federal-de-procedimientos-penales#7496

[67] http://perezmacedo.com/artículos-de-interés/delitos-graves-en-el-codigo-nacional-de-procedimientos-penales/ (Consultado 12/09/2017)

Dicho lo anterior, queda un mejor entendimiento del panorama general de las trasformaciones que han sufrido las diversas legislaciones aplicables conforme al nuevo sistema de justicia penal instaurado en el país, en el que se deja al arbitrio de cada entidad federativa desarrollar el catálogo de delitos que sean considerados como graves en sus legislaciones locales. Ahora, es pertinente entrar al estudio de los preceptos contemplados en la Ley de Instituciones de Crédito que pueden ir ad hoc con el análisis de la figura del phishing.

El artículo 111 Bis, es de especial atención para nuestro estudio, debido a que contiene diversos elementos que concuerdan con la conducta antijurídica del phishing, pues determina que las personas que se ostenten por sí o a través de otra persona o por medio de nombres comerciales, por cualquier medio de publicidad se ostenten frente al público como intermediario o entidad financiera, sin contar con la autorización para constituirse, funcionar, organizarse u operar con tal carácter, según sea el caso, sin autorización emitida por autoridad competente serán acreedores de uno a seis años de prisión[68].

Lo relevante para el caso en concreto es que este precepto establece que los sujetos que se ostenten por nombres comerciales, por ejemplo los de las instituciones bancarias o tiendas de prestigio, o por medio de publicidad, como perfectamente lo puede ser la internet, se ostenten como intermediario o entidad financiera sin contar con las autorizaciones respectivas, los atacantes se ostentan ante las víctimas como la legítima entidad financiera a efecto de obtener información privilegiada para después utilizarla de manera fraudulenta, sin embargo, en este punto es en donde queda inaplicable esta norma para nuestro fin, pues el móvil de este artículo se refiere únicamente a la oferta ilegal de servicios financieros al no contar con las autorizaciones correspondientes.

Por otra parte, la disposición 112 Bis en su fracción III, sanciona a los sujetos que sin causa legitima o sin consentimiento, obtenga, comercialice o use la información de los clientes, cuentas u operaciones de las tarjetas de crédito emisoras de las tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier

[68] Véase artículo 111 Bis Ley de Instituciones de Crédito:http://www.diputados.gob.mx/LeyesBiblio/pdf/43.pdf

otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero[69].

Como se ha dicho con anterioridad la información para preparar la elaboración de los ataques de phishing puede obtenerse de diversas fuentes, una de ellas es directamente de las bases de datos de las instituciones financieras, ya sea con el fin de comercializar con ella, o bien se encuentren coludidos con otra persona especialista en ese tipo de ataques, evidentemente la pena se establecerá en el grado de participación o comisión de la conducta. Otro aspecto que contiene esta norma es que es específica al señalar que la protección a los instrumentos de pago o de información no es únicamente para las instituciones mexicanas sino también las del extranjero, esto nos da la pauta de que se tiene entendimiento que el sistema de pagos es de carácter mundial, así como también lo son las conductas de phishing que pueden ser perpetradas desde cualquier sitio del planeta que tenga acceso a un computador con conexión a internet.

Por último, el artículo 112 Quáter, en sus dos fracciones dispone las penas y sanciones de aquellos que sin causa legítima o sin consentimiento accedan a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema financiero mexicano, para obtener recursos económicos, información confidencial o reservada, o bien altere o modifique el mecanismo de funcionamiento de dichos equipos para la disposición de efectivo de los usuarios del sistema bancario mexicano[70].

De lo anteriormente expuesto, se desprende que la ley prevé el uso de medios electrónicos como método inminente para acceder a las bases de datos o mecanismos tecnológicos del sistema bancario mexicano, así como la manipulación que se hace a los cajeros automáticos utilizados por millones de usuarios de los servicios financieros, mediante la utilización de aparatos electrónicos con la finalidad de obtener información confidencial o reservada, o bien la obstrucción de éstos para la disposición de efectivo, empero, el ordenamiento únicamente pone especial atención a la infraestructura patri-

[69] Véase artículo 112 Bis F. III Ley de Instituciones de Crédito: http://www.diputados.gob.mx/LeyesBiblio/pdf/43.pdf
[70] Véase artículo 112 Quáter F. I y II Ley de Instituciones de Crédito: http://www.diputados.gob.mx/LeyesBiblio/pdf/43.pdf

monial tecnológico del sistema bancario, sin prestar atención en las extensiones de las misma, pues si bien ofrecen servicios en locales legalmente establecidos y autorizados que cuentan con esta tecnología, también lo hacen con páginas web a las cuales se accede mediante un ordenador personal o equipo tecnológico con conexión a internet, mismo que se vuelve un método de comunicación entre la institución bancaria y el usuario del servicio.

Hecho por el cual debería de protegerse por igual a dichas comunicaciones electrónicas, que aunque no son realizadas por personas autorizadas por la institución financiera, si lo es por alguien que se está ostentando como tal ya sea accediendo sin consentimiento a sus equipos o aplicaciones o bien imitando la página en un acto de suplantación, con la finalidad de inducir al error a los clientes de dicha institución, para así obtener información confidencial o reservada, que tiene como finalidad la obtención de recursos económicos, de manera que, tal conducta lesiona gravemente el patrimonio, reputación de las entidades financieras, así como la estabilidad económica de los usuarios de los servicios financieros.

En mi opinión es en la Ley de Instituciones de Crédito, podría ser el ordenamiento adecuado para regular la conducta antijurídica del phishing, pues en esta encontramos diversos elementos que podríamos adecuar de manera práctica para su regulación, además de que, al ser una ley especializada en el ámbito financiero, se adecua de manera hermética para su aplicación.

2.3.2. LEY GENERAL DE TÍTULOS Y OPERACIONES DE CRÉDITO.

En el mismo tenor de la ley estudiada con anterioridad de igual manera el 26 de junio de 2008, sufrió una serie de reformas con la finalidad de tipificar la clonación de instrumentos de crédito utilizados como medio de pago[71], la diferencia radica en que los preceptos regulados en esta ley en comparación con la Ley de Instituciones de crédito, es que en este ordenamiento jurídico se refiere primordialmente a tarjetas de servicio, de crédito o en general, de instrumentos utilizados en el sistema de pagos para la adquisi-

[71] http://www.diputados.gob.mx/LeyesBiblio/pdf/145_130614.pdf Última reforma publicada en el Diario Oficial de La Federación el 13 de junio de 2014. (Consultado 12/09/2017)

ción de bienes y servicios emitidos en el país o en el extranjero, por entidades comerciales no bancarias.

Es decir, que estas tarjetas denominadas de servicio son emitidas por empresas comerciales no bancarias en virtud de un contrato que regula el uso de las mismas, mediante las cuales las personas físicas o morales afiliadas a dicha empresa comercial, quienes pueden utilizarlas para la adquisición de bienes o servicios dentro de los establecimientos de dicha empresa emisora o alguna de sus filiales conforme las reglas de operación se los permita[72].

En el caso de este ordenamiento, son pocas las cuestiones que nos quedan por analizar con relación a la figura antijurídica del phishing, aunque, hay ciertos puntos que vale la pena resaltar.

En la fracción III del artículo 432, de la ley en estudio se refiere a que cometerá la conducta tipificada a quien obtenga, comercialice o use la información sobre clientes u operaciones de las entidades emisoras, se dijo con anterioridad, respecto de cómo es posible utilizar dicha información para cometer un ataque de phishing, es importante resaltar que la fuga de información de dichas entidades comerciales no bancarias es más susceptible, pues a diferencia de las instituciones bancarias, los comercios no cuentan con estándares de seguridad tan sofisticados, ni con la infraestructura para el manejo y resguardo de dicha información, por lo que se vuelve más vulnerable y un objetivo más fácil para aquellos que buscan obtener algún lucro indebido con dicha información.

Aunque por otro lado, la afectación económica en comparación con las instituciones de crédito es menor en cierto grado, pues si bien existen múltiples establecimientos comerciales que otorgan estas facilidades de pago a sus clientes, los montos de las líneas de crédito la mayoría de veces son mucho menores a las otorgadas por las instituciones bancarias, a la par de que se limita su utilización dentro de la misma empresa

[72] Ibídem. Véase art. 432 de la Ley General de Títulos y Operaciones de Crédito: http://www.diputados.gob.mx/LeyesBiblio/pdf/145_130614.pdf

comercial, lo que achica el margen de acción de los ciberdelincuentes al no ser tan beneficiosas para su cometido.

2.3.3. CÓDIGO PENAL FEDERAL.

El 17 de mayo de 1999, se publicó en el Diario Oficial de la Federación un decreto mediante el cual se adicionaron diversas disposiciones al Código Penal Federal, modificando el Título Noveno, al cual se le agregó el capítulo II denominado "Acceso ilícito a sistemas y equipos de informática"[73], en atención a diversos factores, pues se entiende que la tecnología informática es un instrumento que facilita a la sociedad su desarrollo económico y cultural, por lo que mediante su empleo y regulación es importante en aras del desarrollo nacional.

El avance logrado en los últimos años en el sector tecnológico ha permitido que un creciente número de personas tengan acceso a diversos tipos de herramientas tecnológicas, mismas que se utilizan día a día para llevar a cabo todo tipo de actividades, desde las comerciales, las industriales, de comunicación, educativas, culturales y hasta financieras. Tal es el caso, que muchas de esas actividades únicamente pueden realizarse mediante el uso de medios electrónicos, o es necesario el uso de sistemas informáticos o equipos tecnológicos para su oportuna ejecución.

Existen diferentes conductas que revisten el carácter de ilícito perpetuadas con la utilización de los sistemas informáticos o utilizando medios electrónicos, mismos a la que la doctrina jurídica se ha encargado de nominar "delitos informáticos", dentro de los más comunes encontramos: la destrucción, robo o alteración de información, el acceso no autorizado a computadoras o sistemas electrónicos, el sabotaje por medios computacionales, interceptación de correos electrónicos o telecomunicaciones, transferencia ilícita de fondos y fraudes electrónicos.

Dicha reforma se gestó en virtud de la inminente necesidad de proteger la privacidad e integridad de la información contenida en sistemas y equipos de cómputo, almacena-

[73] http://dof.gob.mx/nota_detalle.php?codigo=4948419&fecha=17/05/1999 (Consultado 12/09/2017)

miento o procesamiento de información, situación por la cual es de relevante importancia sancionar aquellas personas que sin derechos alguno que les asista, accedan a los equipos de terceras personas con el propósito de vulnerar la privacidad de la información, dañarla, alterarla, sustraerla o de alguna manera provocar su pérdida[74].

Además, de tener una consideración especial a las Instituciones del Estado, otorgando penas mayores cuando las conductas son cometidas en perjuicio de éstas, a tal grado de que puedan tener un fuerte impacto en el desarrollo de la economía, en la seguridad nacional o en las relaciones comerciales.

Sin duda, uno de los sectores más vulnerables y más atacados por este tipo de prácticas son las instituciones financieras, pues los recursos y la información que se maneja dentro de estas es el blanco perfecto para los atacantes, por lo que se adicionaron diversas disposiciones en las cuales se aumentan las penas de manera considerable, hasta en una mitad, cuando las conductas previstas sean cometidas por personal o miembros de dichas instituciones.

Este punto es de suma relevancia para el estudio del phishing, pues si bien sabemos que son diversas las formas, diversos los recursos por medio de los cuales los atacantes obtienen la información para efectuar los ataques de phishing, una de las más comunes es la filtración de información confidencial de las instituciones financieras, pues ayuda a que estos ataques sean más elaborados y precisos, me explico.

Se debe tener en mente, que la mayoría de estos ataques son recibidos en su mayoría por medio de un correo electrónico, o de servicios de mensajería que se encuentran ligados a una dirección de e-mail. Los usuarios de los servicios financieros otorgan de buena fe a la institución financiera de su preferencia ciertos datos necesarios para la apertura de una cuenta o un préstamo, etc. dentro de los cuales se proporcionan nombres, direcciones, teléfonos, así como cuentas de correo electrónico como medio de

[74] Cfr. http://transparencia.senado.gob.mx/historico_respuestas/content/2005/1-abril/F601.pdf (Consultado 07/09/2016)

contacto o de envío de diversa información relativa al servicio prestado por dicha institución, verbigracia el envío mensual del estado de cuenta.

Como se ha mencionado, con anterioridad la información reviste la calidad de un bien susceptible de aprovechamiento económico, por lo que no es muy descabellada la idea que le pueda surgir a un funcionario de la institución financiera de poder comerciar con ella y venderla con el propósito de diversos fines, entre los cuales podría ser bien para producir ataques de phishing, pues por lo menos con esta información ya se cuenta con tres elementos esenciales para su comisión los cuales son: Nombre, Institución Financiera de la que es cuentahabiente y un correo electrónico al cual enviar el ataque, situación que vuelve por demás vulnerable a la víctima por la exactitud de sus datos y es más probable que el fraude se efectué de manera exitosa.

Derivado de la iniciativa presentada para la modificación de los preceptos antes mencionados, pretender proteger los bienes jurídicos tuteados de la privacidad y de la integridad de la información, sin embargo, al ser la informática un instrumento en constante evolución existe una gran carencia de tipos adecuados a diversas conductas como lo es el phishing, por lo que sus autores quedan impunes, desembocando en un gran perjuicio patrimonial en los diversos estratos sociales.

2.3.4. LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA.

Esta ley publicada en el Diario Oficial de la Federación el 7 de noviembre de 1996, tiene como primordial objeto establecer las reglas referentes a la investigación, persecución procesamiento, sanción y ejecución de las penas, por los delitos cometidos por algún miembro de la delincuencia organizada dentro del territorio nacional[75]. De conformidad con este ordenamiento en su artículo segundo, cuando tres o más personas se organicen de hecho para realizar, en forma permanente o reiterada alguna de las con-

[75] Cfr, Ley Federal Contra la Delincuencia Organizada, última reforma publicada en el Diario Oficial de la Federación 07/04/2017. P. 1. Puede consultarse en línea en la siguiente liga: http://www.diputados.gob.mx/LeyesBiblio/pdf/101_070417.pdf (Consultado 13/09/2017)

ductas previstas en este artículo, serán sancionados como miembros de la delincuencia organizada[76].

Existe una amplia lista de las conductas que se encuentran consideradas para ser susceptibles de ser ejecutadas por un conjunto de personas con el carácter de crimen organizado dentro de los diversos ordenamientos generales y especializados a nivel federal, mismas conductas que se encuentran enumerados en el artículo segundo de dicha ley a lo largo de sus siete fracciones, dentro de los más importantes destacan: Terrorismo, delitos contra la salud, falsificación de moneda, tráfico de armas, órganos o de personas, corrupción de menores, turismo sexual, trata de personas, secuestro de personas, entre otros[77].

Para el caso en concreto respecto del análisis jurídico de la figura del phishing, existe una conducta delictiva dentro de las contempladas en el crimen organizado que es importante analizar, me refiero a la contemplada dentro de la fracción primera del artículo 2°, nos remite específicamente a conductas tipificadas en el Código Penal Federal, norma 400 Bis, que se refiere a operaciones con recursos de procedencia ilícita, que aunque este ordenamiento previamente ya fue estudiado, ahora es importante que lo analicemos desde el punto de vista de la delincuencia organizada.

Las operaciones realizadas con recursos de procedencia ilícita, se refiere al cause o destino que se le den a los diversos recursos, derechos o bienes de cualquier naturaleza, que resulten como el producto del desarrollo de una actividad antijurídica calificada como delito, es decir es el manejo de diversos bienes con el conocimiento de que son procedentes de la realización de una conducta ilícita, así mismo existen indicios fundados o certeza de que provienen directa o indirectamente, o representan ganancias derivadas de la comisión de un delito y no pueda acreditarse su legítima precedencia.

Como se mencionó con anterioridad el phishing es una actividad antijurídica compleja, por lo que para su ejecución se requieren de diversos elementos imprescindibles, uno

[76] Ídem.
[77] Ídem. Véase artículo 2, Fracciones I a VII, Ley Federal contra la Delincuencia Organizada: http://www.diputados.gob.mx/LeyesBiblio/pdf/101.pdf pp.2-4.

de ellos se presenta al final, pues el objetivo es la disposición de los recursos derivados de dicha práctica, por lo que el ciber delincuente a manera de protección lucubra, imagina o inventa diversas maneras para deshacerse de los recursos por conducto de terceros, con la finalidad de obtener nuevos que ya no contengan alguna huella digital o electrónica que pueda llevar a su rastreo, haciéndolo casi imposible.

El artículo en cuestión menciona que serán acreedores a las penas correspondientes a aquellos sujetos quienes adquieran, enajenen, administren, custodien, posean, cambien, conviertan, depositen, retiren, den o reciban por cualquier motivo, inviertan, traspasen, transfieran o transporten, dentro del territorio nacional, de éste al extranjero o a la inversa o bien oculten, encubran, o pretendan hacerlo respecto de la naturaleza, origen, ubicación, destino, movimiento, propiedad o titularidad respecto de los recursos, derechos o bienes cuando tengan conocimiento de que proceden o representan el producto de una actividad ilícita[78]. A pesar de que son mucho los supuestos que se contemplan en el código respecto al destino de dichos recursos, en la práctica será muy difícil encuadrarlo debido a que en nuestra legislación no se encuentra contemplada la figura del phishing.

Por otra parte, en el tercer párrafo de la fracción II, señala que en el caso que las conductas previstas en el artículo en análisis, se utilicen servicios de instituciones que integran el sistema financiero, para proceder penalmente se requerirá una denuncia previa ante la Secretaría de Hacienda y Crédito Público.

> *"…En caso de conductas previstas en este Capítulo, en las que se utilicen servicios de instituciones que integran el sistema financiero, para proceder penalmente se requerirá la denuncia previa de la Secretaría de Hacienda y Crédito Público.*
>
> *Cuando la Secretaría de Hacienda y Crédito Público, en ejercicio de sus facultades de fiscalización, encuentre elementos que permitan presumir la comisión de alguno de los delitos referidos en este Capítulo, deberá ejercer respecto de los*

[78] Véase artículo 400 Bis Fracción I y II, Código Penal Federal, p. 113, última reforma publicada en el Diario Oficial de la Federación 26/06/2017: http://www.diputados.gob.mx/LeyesBiblio/pdf/9_120315.pdf ((Consultado 13/09/2017)

mismos las facultades de comprobación que le confieren las leyes y denunciar los hechos que probablemente puedan constituir dichos ilícitos[79].

Dichas facultades serán ejercidas por la secretaría por medio de sus diversos organismos y serán perseguidos e investigados por la procuraduría fiscal de la federación, en coordinación con las demás autoridades que pudiesen tener interés jurídico o bien se requiera de su opinión para el caso en concreto.

En el caso del phishing en la mayoría de los casos los recursos obtenidos provienen de las cuentas emitidas por una institución bancaria, que sin duda alguna son integrantes del sistema financiero a que se refiere el artículo en cuestión, por lo que la Secretaría de Hacienda y Crédito Público en ejercicio de sus facultades que ha sido investida por el ejecutivo de la unión en coordinación con los demás órganos rectores del sistema financiero, así como las diversas organizaciones bancarias, en observancia a dicha conducta delictiva debería de proponer las reformas pertinentes para la integración y regulación del phishing con la finalidad de resguardar la estabilidad del sistema financiero mexicano.

2.3.5. LEY DE LA PROPIEDAD INDUSTRIAL.

La importancia de las marcas comerciales en los mercados globales es el aspecto de diversificación y el uso de signos distintivos, que les permite diferenciarse eficientemente entre los diversos productos, servicios, establecimientos y empresas, es decir, hace que las empresas puedan distinguirse de los de la competencia, haciéndolos únicos mediante signos distintivos que los hagan únicos. A esta imagen comercial se le denomina comúnmente como "*trade dress*" que es el conjunto de signos distintivos que integran a un comercio y que lo caracterizan, el Estado con la implementación de diversas herramientas jurídicas se ha encomendados la tarea de tutelar jurídicamente estos aspectos englobados en los derechos de propiedad Industrial.

Para llevar a cabo dicha protección, dentro de la Ley de la Propiedad Industrial, publicada en el Diario Oficial de la Federación el 27 de junio de 1991[80], se completan una

[79] Ídem.

serie de conductas que se consideran ilícitas contenidas en el capítulo II, denominado "De las Infracciones y Sanciones Administrativas", tal como su nombre lo dice, la transgresión las diversas conductas enumeradas en las fracciones que conforman el artículo únicamente son sancionadas administrativamente ya sea mediante multas, clausuras de establecimientos o arrestos administrativos, sin embargo, estás podrán tomar el carácter de delito conforme a lo establecido en el artículo 223[81], fracción primera de dicha ley, a quien reincida en las conductas previstas en las fracciones II a XXII del artículo 213[82] de esta Ley, una vez que la primera sanción administrativa haya quedado firme.

La importancia en el análisis de esta Ley en relación con la figura del phishing es que uno de los elementos por los que se configuran los ataques de esta índole, es que el atacante valiéndose de diversos medios como lo son la utilización de signos distintivos, elementos operativos y de imagen de una empresa o alguna institución bancaria, intenta inducir al error a los usuarios a una confusión, error o engaño, por hacer creer o suponer la existencia de una relación entre el titular de los derechos protegidos y el usuario no autorizado[83], con la finalidad de obtener cierta información privilegiada, principalmente usuarios y contraseñas con los que posteriormente, se utilizan sin autorización para obtener un lucro indebido.

Como se puede apreciar, la fracción XXVI no se encuentra contemplada dentro de los supuestos que puede calificar como delito en caso de reincidencia, además de que el capítulo III "De los Delitos" no la contempla en ninguno de sus apartados por lo que en caso de materializarse su comisión únicamente sería sancionable de manera administrativa, siendo claro que este tipo de prácticas tienen un gran impacto en la estabilidad del sistema financiero y la economía del país, ya que su actuación no solo se limita a la utilización de los signos distintivos, sino que existen ciertos casos que llegan a falsificar a la perfección los sitios web de las entidades financieras.

---

[80] Ley de la Propiedad Industrial, última reforma publicada en el Diario Oficial de la Federación 01/06/2016. Puede consultarse en línea en la siguiente liga http://www.diputados.gob.mx/LeyesBiblio/pdf/50_010616.pdf (Consultado 13/09/2017)
[81] Ídem. P. 59.
[82] Ídem. Pp. 55-58.
[83] Ídem. P. 56 Véase artículo 213 fracción XXVI.

Aunque el artículo 223 en su fracción II, califica como delito la falsificación, en forma dolosa de marcas protegidas por esta ley, este precepto contiene un elemento que descarta la posibilidad de adecuar dicha conducta a este tipo penal, al mencionar que la finalidad es la especulación comercial[84], pues el phishing no busca la adquisición de un bien para después obtener un mayor beneficio que dependa de los diversos factores del mercado, si no pretende la obtención de bienes o servicios inmediatos, o bien la transferencia de dichos recursos a un tercero a cambio de una contraprestación económica en menor valía.

Como bien tuvimos a estudiar el artículo 111 bis, de la Ley de Instituciones de Crédito contempla como delito la ostentación de las personas frente al público como intermediarios o entidades financieras mediante la utilización de nombres comerciales o cualquier medio de publicidad, en mi opinión no queda bien delimitado a que casos en específico se refiere, por lo que se infiere que únicamente es para ofrecer servicios financieros al público en general, a diferencia del phishing que busca utilizar la imagen, los signos distintivos, así como los elementos operativos de la marca de las instituciones bancarias para inducir al error a los usuarios y así obtener la información privilegiada, pues con este método es como se engaña a los usuarios de dichos servicios, estos dos artículos con una serie de adecuaciones se complementarían de manera óptima para la regulación del phishing tanto en su tipificación como en las sanciones, pues por una parte la Ley de Instituciones de crédito otorga sanciones corporales y por el otro la Ley de Propiedad Industrial multas considerables en caso de realizar los actos descritos, que afectan en gran medida al sistema financiero mexicano.

La legislación federal debe contemplar claramente este tipo de delitos en todas sus modalidades, es claro y de suma importancia que exista regulación efectiva que pueda aplicarse a nivel federal, pues es un hecho común que las autoridades se encuentren con dificultades jurídicas a la hora de consignar a un sujeto que cometa este tipo de conductas, pues se requiere de terminología adecuada y de una buena aplicación de los ordenamientos para poder castigar a quien cometa estos ilícitos, aunque no deja-

[84] Ídem. P. 58 Véase artículo 223 fracción II.

mos de lado que el primer paso primordial debe de darse en los procesos de investigación y prosecución de estas conductas por parte de las autoridades correspondientes.

2.4.- LEGISLACIÓN LOCAL.

Dada la proliferación de los diversos delitos cometidos a través de medios electrónicos, algunos de los diversos Estados de la República Mexicana se han dado a la tarea de incluir en sus diversas legislaciones estas prácticas, pues es importante que estas conductas sean atenidas por todos los órdenes de gobierno, pues como se ha dicho en reiteradas ocasiones pueden ser ejecutadas desde cualquier lugar, situación que emana de la preocupación por la globalización, los avances tecnológicos y la sofisticación de la delincuencia. Dichas reformas, se han enfocado y deberán de enfocarse principalmente en la delimitación de las conductas realizadas, así como los métodos para su prevención, investigación, prosecución; en los ámbitos procesales y de competencia, así como los acuerdos de colaboración con las diversas entidades de gobierno, mediante la implementación de tecnología y capacitación del personal en estos rubros.

Es importante destacar que en todos los Estados de la república en menor o mayor medida dentro de sus legislaciones penales se han dado una serie de reformas que contemplan algunas de las conductas delictivas más recurrentes como lo son, la pornografía infantil, la revelación de secretos, la extorsión electrónica, el acceso ilícito a sistemas informáticos, clonación de instrumentos de crédito, violación de correspondencia, entre otros.

Para el caso en concreto, no se encuentra ninguna disposición al respecto de la figura del phishing, sin embargo en diversas legislaciones como lo son las de los Estados de Baja California Sur, Colima, Distrito Federal (hoy Ciudad de México), Estado de México, Guanajuato, Hidalgo, Michoacán, Nuevo León, Puebla, Querétaro, Quintana Roo, Sinaloa y Yucatán, califican como acto ilícito la obtención de información relacionada con los instrumentos de crédito, venta de información relacionada con el instrumento de crédito y el uso de la información relacionada con el instrumento de crédito. Todas estas previsiones se relacionan con los pasos que conforman el phishing, desde la obten-

ción de información, la comercialización y, en el caso que principalmente afecta al titular, el uso de la información obtenida[85].

En el siguiente cuadro haremos referencia a la legislación y los artículos en que se encuentran contempladas las conductas citadas en el párrafo precedente:

LEGISLACIONES ESTATALES.	
Código Penal para el Estado de Baja California Sur	Artículo 195, fracciones IV y V.
Código Penal para el Estado de Colima	Artículo 201, fracción VI
Código Penal para el Distrito Federal (Hoy Ciudad de México)	Artículo 336, fracciones VI y VII
Código Penal del Estado de México	Artículo 174, fracción VI
Código Penal del Estado de Guanajuato	Artículo 234-a, fracción VI
Código penal para el Estado de Hidalgo	Artículo 265 Bis, fracción VI
Código Penal del Estado de Michoacán	Artículo 203 Bis, fracción VI
Código Penal para el Estado de Nuevo León	Artículo 242 Bis, fracción V
Código Penal del Estado Libre y Soberano de Puebla	Artículo 245 Bis, fracción V
Código Penal para el Estado de Querétaro	Artículo 232 Bis, fracción V
Código Penal para el Estado Libre y Soberano de Quintana Roo	Artículo 189 Bis, fracción IV
Código Penal para el Estado de Sinaloa	Artículo 271 Bis, fracción VI
Código Penal del Estado de Yucatán	Artículo 284 Bis, fracción VI

[85] Cfr. Muñoz Torres, Ivonne, Delitos Informáticos Diez Años Después, 1ª Edición, Editorial Ubijus, México 2009, p.93.

Ahora bien, me gustaría prestar especial atención a un ordenamiento que como consecuencia de la reforma constitucional en materia penal de 18 de junio de 2008, ha decidido transformarse completamente en atención a dicho decreto, creando un código penal único, en el cual, se tiene enfocado en un aspecto totalmente funcionalista, ejemplo de ello es que si bien dije que no existía ningún ordenamiento en México que contemplara la figura del phishing, el nuevo Código Penal para el Estado de Colima, publicado en el periódico oficial “El Estado de Colima" el 11 de octubre de 2014, es la excepción a la regla, pues en su artículo 201, fracción VII titulada “Manipulación indebida informática” establece los elementos principales de la figura del phishing y lo equipara con el delito de fraude.

> “***ARTÍCULO 201****. Se considera fraude y se impondrá pena de cuatro a once años de prisión y multa por un importe al equivalente de cuatrocientos cincuenta a mil días de salario mínimo, en los siguientes casos:*
>
> ***I. a VI. …***
>
> ***VII. Manipulación indebida informática.*** *Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener lucro indebido[86].”*

El artículo en estudio es muy claro, pues dispone en primer término se especifica que las personas que alcancen un lucro indebido mediante el uso de algún medio informáti-

[86] Código Penal para el Estado de Colima, pp. 91-93. Última reforma publicada en el periódico oficial “El Estado de Colima” 10 de septiembre de 2016.

co, telemático o electrónico serán acreedores a las mismas sanciones aplicables al delito de fraude. Estas tres palabras encuadran perfectamente en nuestra definición de phishing, pues el medio informático por el cual se obtiene la información es la red de internet, el medio telemático al caso en concreto se refiere al correo electrónico mediante el cual se intenta engañar a la víctima y el medio electrónico es el ordenador o dispositivo con el cual se lleva a cabo la hazaña.

Se puede observar que, para configurar esta práctica el phisher se vale no solo de uno, si no de los tres medios para lograr su cometido. Enseguida el dispositivo legal nos describe una serie de acciones que pueden realizarse a través de dichos medios, las cuales son tendientes a realizar una acción fraudulenta, como lo es usar la red de redes para montar sitios espejos o de trampa para obtener información determinante y utilice dichos datos de manera no autorizada, así como la suplantación de identidades.

Se ha explicado en varias ocasiones que los ciber criminales a efecto de dar mayor credibilidad a sus engaños, crean sitios web idénticos a los de instituciones financieras o empresas de prestigio, copiando logos, colores y diseños, mediante los cuales se ostentan como la legítima institución y solicitan a los clientes de buena fe algunos datos sensibles con algún pretexto relacionado con la seguridad de su cuenta o evitar algún tipo de fraude, conductas que por sí mismas encuadran a la perfección en el supuesto jurídico en estudio, pues al obtener dicha información, el delincuente puede sin ningún tipo de restricción utilizarla para obtener un lucro que no es debido.

Considero que el Código Penal para el Estado de Colima, se encuentra por mucho, mejor actualizado en temas referentes a nuevas tecnologías y en otros aspectos en comparación a sus semejantes de otras entidades federativas, por lo que debería ser considerado como ejemplo a seguir con la finalidad de que se cuente con legislación moderna y uniforme que nos ayude a conseguir de manera eficiente la persecución de los diversos delitos patrimoniales que tanto afectan la estabilidad de la economía mexicana, así como su procesamiento en caso de que pueda detener al culpable.

2.5.- ANÁLISIS DE DERECHO COMPARADO DE LA FIGURA DE PHISHING CON RELACIÓN A MÉXICO.

Al ser una conducta que puede ser ejecutada desde cualquier parte del mundo, los países deben de asumir las responsabilidades legales con la finalidad de perseguir el fraude especializado denominado phishing, que afecta en gran medida a las instituciones bancarias. Por lo que deben de incluir en sus legislaciones, las medidas pertinentes a efecto de prevenir y erradicar dichas conductas, así como establecer las medidas de colaboración con otros estados a fin de que se facilite la prosecución en general de los delitos cometidos con el uso de medios electrónicos.

Son diversos los países que dentro de su legislación han adoptado las medidas legislativas pertinentes que pretenden disminuir y atacar directamente este tipo de conductas que afectan de manera importante la estabilidad financiera global. Es importante para este estudio jurídico de la figura del phishing, analizar algunos de los puntos relevantes que han tomado en consideración algunos estados en su legislación, pues bien, su experiencia puede ayudar de manera integral a su implementación y aplicación de diversas medidas en nuestro país, por los que brevemente se expondrán algunas de las medidas adoptadas por diversos países alrededor del mundo.

2.5.1. ESTADOS UNIDOS DE AMÉRICA.

Los estragos económicos consecuencia del phishing, comenzaron a crear cierta incertidumbre entre los usuarios de los servicios financieros y cierta preocupación latente por parte del gobierno, por estarse enfrentando una situación difícil de combatir por las implicaciones técnicas que con lleva este tipo de fraude. Se estima que las pérdidas a causa de este tipo de fraude entre 2004 y 2005, en los Estados Unidos asciende aproximadamente en novecientos veinte nueve millones de dólares. Justo en el año de 2004, se llevó a cabo el primer juicio en este país por la práctica conocida como “phishing”[87].

[87] Cfr. https://seguinfo.wordpress.com/2006/11/14/el-numero-de-ataques-de-phishing-se-duplica-en-estados-unidos-3/ (Consultado 13/07/2017)

El juicio se llevó a cabo ante la "Federal Trade Commission" o "Comisión Federal de Comercio" (traducido al español), en el que se le atribuyó a un joven de 17 años, la creación de una página que era muy similar a la de la empresa AOL, con la finalidad de obtener de manera indebida números de tarjetas de crédito. Este caso, entre otros tantos demostraba el crecimiento exponencial de dicha práctica, en la que se utilizaba el robo de identidad para obtener datos sensibles.

Dicho lo anterior en el año 2005, el Senador Demócrata Patrick J. Leahy, presentó una ley en la que se determinaban las penas que pagarían aquellos que fueran sorprendidos enviando ataques de phishing, a la cual se le denominó "The Anti-Phishing Act of 2005"[88], en esta se estableció que aquellas personas que crearan páginas web falsas de alguna empresa o enviaran e mails de corte fraudulento se harían acreedores a multas hasta $250,000 dls. y hasta 5 años en prisión[89].

A diferencia de México, en los Estados Unidos de América si existe una ley específica que regula la figura del phishing, incluso se determinan las penas que deberá de cubrir aquellas personas que incurran en dicha práctica, además de que en algunos de sus estados contemplan dicha figura dentro de sus legislaciones locales[90]. Además, cuentan con sitios en línea especializados, algunos privados, algunos otros implementados por el gobierno, en los cuales ofrecen una serie de información, ejemplos y recomendaciones con la finalidad de evitar ser víctima de dichas estafas, así mismo ofrecen a los ciudadanos un espacio en el cual se pueden reportar este tipo de ataques[91].

2.5.2. REPÚBLICA DE CHILE.

Cómo tal, Chile no posee legislación específica destinada al castigo del phishing, pues en el tema de justicia de dicho país, se estima como una parte especializada del fraude

[88] https://www.congress.gov/bill/109th-congress/senate-bill/472/text (Consultado 13/09/2017)
[89] http://www.washingtonpost.com/wp-dyn/articles/A63749-2005Mar1.html (Consultado 13/09/2017)
[90] http://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx (Consultado 13/09/2017)
[91] http://www.onguardonline.gov/phishing (Consultado 13/09/2017)

si es cometido a través de medios informáticos como es el caso de la Ley 19.223[92], en la cual se tipifica las figuras penales relativas a la informática, promulgada el 28 de mayo de 1993, por el Ministerio de Justicia, la cual contiene únicamente cuatro artículos en los que se delimitan a grandes rasgos las actividades ilícitas que pueden efectuarse con la implementación de medios computacionales.

El artículo segundo de dicha Ley, especifica que aquel que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presido menor en su grado mínimo a medio, lo que quiere decir que este artículo pretende proteger la información confidencial contenida en medios informativos, así como la prevención de su mal encause, situación que hemos estudiado a lo largo de este trabajo académico.

Además, para el caso especial del phishing, los organismos judiciales valiéndose de los criterios jurisprudenciales han determinado que esta práctica también puede ser homologada como espionaje informático.

Por otra parte, la Ley 20.009[93], en la cual se "Limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas", promulgada el 18 de marzo de 2005, por el Ministerio de Hacienda de la República de Chile. Esta Ley en sus cuatro artículos como bien lo dice el título, define el procedimiento a seguir e por los usuarios, así como de la institución financiera emisora de la tarjeta en caso de robo, hurto o extravío. Por otra parte, en dicha Ley, en su artículo quinto, establece un listado de las conductas que se consideran como uso fraudulento de tarjeta de crédito o débito.

Para el caso en concreto que nos ocupa existen dos incisos, el d) y e) de la Ley en estudio que pueden ser homologados con la figura del phishing pues establecen que a quien use, venda, exporte, importe o distribuya los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen operaciones de compra o de

[92] http://bcn.cl/1m196 (Consultado 13/09/2017)
[93] http://bcn.cl/1mzuk (Consultado 13/09/2017)

acceso al crédito o débito que corresponde exclusivamente al titular o bien negociar en cualquier otra forma con dichos datos, será acreedor a las penas indicadas. Si bien, en el phishing no se obtiene de manera material la tarjeta bancaria, si se obtiene información confidencial que puede ser utilizada o distribuida para la obtención de un beneficio económico indebido.

Aun cuando no existen leyes específicas relativas al phishing, se han adoptado medidas tendientes a la prevención y castigo del fenómeno de los delitos informáticos, por lo cual en el año 2000, la Policía de Investigaciones de Chile PDI, crea la Brigada Investigadora del Cibercrímen Metropolitana, misma que se divide en tres áreas de trabajo: Delitos contra menores en internet, Delitos Computacionales e Investigación Forense informática[94] en la cual su misión fundamental es la de investigar los ilícitos en los cuales se utilicen ordenadores como medio de comisión.

Otro de los aspectos importantes es que, con el uso de diversas redes sociales, dicho organismo entabla contacto directo con aquellas personas que deseen obtener orientación en caso de sospechar que pueden ser una víctima potencial, método que resulta efectivo, pues con la denuncia directa del ciudadano se tiene el reporte inmediato de ataques de phishing, creando confianza entre los consumidores. Dentro de dicha brigada se publicó además una cartilla diseñada especialmente para estandarizar una metodología para el levantamiento de evidencias informáticas, que homologa el procedimiento que utilicen los diversos funcionarios que concurren a los distintos sitios de sucesos informáticos[95].

2.5.3. REPÚBLICA DE ARGENTINA.

En el caso particular de este país se han dado una serie de cambios progresivos entorno a la regulación de ilícitos cometidos a través de medios electrónicos. El cuatro de junio de 2008, fue sancionada la Ley 26.388, de delitos informáticos, la cual no es una

[94] http://www.pdichile.cl/jenadec/cibercrimen/index.htm (Consultado 13/09/2017)
[95] Maldonado Ayala, Esteban, Ol.clPhishing y Pharming: Una aproximación desde el Cibercrimen. http://docplayer.es/5876513-Ol-clphishing-y-pharming-una-aproximacion-desde-el-cibercrimen.html (Consultado 13/09/2017)

ley especial, pues no regula este tipo de delitos en un cuerpo normativo separado del Código Penal con figuras propias y específicas, sino que es una ley que modifica, sustituye y adiciona algunas figuras típicas al Código Penal actualmente en vigencia con el objeto de regular las distintas actividades tendientes a la comisión de ilícitos con la implementación de nuevas tecnologías[96].

En lo referente a la figura del phishing la Ley 26.388, en su artículo noveno ha tenido a bien regular lo concerniente a nuestro estudio en el que se establece lo siguiente:

> *"ARTICULO 9º — Incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente:*
>
> *Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos[97]."*

Para mejor entendimiento de la adición que se efectuó como inciso 16, es importante analizar lo que se establece en el texto de los artículos 172 y 173, ubicados en Libro Segundo, Título Sexto, Capitulo IV, denominado "Estafas y otras defraudaciones" del Código Penal Argentino:

> *"Art. 172.- Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negación o valiéndose de cualquier otro ardid o engaño.*
>
> *Art. 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:*

[96] http://www.delitosinformaticos.com/06/2008/noticias/la-incorporacion-de-los-delitos-informaticos-al-codigo-penal-argentino# (Consultado 13/09/2017)
[97] http://www.oas.org/juridico/PDFs/arg_ley26388.pdf (Consultado 13/09/2017)

Inciso 1º el que defraudare a otro en la substancia, calidad o cantidad de las cosas que le entregue en virtud de contrato o de un título obligatorio...[98]"

Es posible apreciar, aparentemente en este artículo se tiene por tipificada por completo la figura del phishing, sin embargo, algunos docentes jurídicos acertadamente no lo consideran así, pues mencionan que, al estar equiparado al delito de fraude especializado conforme al cuerpo normativo previamente analizado, se requiere de un elemento típico esencial para que se configure la conducta básica de la figura del fraude, que es el perjuicio patrimonial.

Por lo que en Argentina no está penada como delito autónomo la llana obtención de los diversos datos sensibles a través de medios electrónicos con fines de defraudar[99], lo que deja totalmente sin regulación a la primera etapa del phishing en la que se obtienen dichos datos, que sin duda los medios por los cuales los obtiene dicha información rompen sin duda una serie de disposiciones específica, ejemplo de ello, sería la suplantación de identidad de las instituciones financieras.

En septiembre de 2011, se sometió a revisión un proyecto de ley a la Comisión de Justicia y Asuntos penales de la Cámara de Senadores, a efecto de subsanar dicha situación, por lo que se pretendía hacer una adhesión más al Código Penal mediante la siguiente enmienda[100]:

"… (S-5557/11) PROYECTO DE LEY. - ARTÍCULO 1º: Incorporarse como Artículo 157 ter. Del Código Penal de la Nación el siguiente:

Art. 157 ter. - Será reprimido con prisión de un mes a dos años o multa de diez a cien mil pesos a el que:

---

[98] http://www.oas.org/dil/esp/Codigo_Penal_de_la_Republica_Argentina.pdf (Consultado 13/09/2017)
[99] http://blog.segu-info.com.ar/2011/02/phishing-tipo-penal-en-argentina-y-sus.html (Consultado 13/09/2017)
[100] Cfr. http://www.informaticalegal.com.ar/2011/09/15/proponen-que-el-robo-de-datos-por-internet-se-prevea-en-el-codigo-penal-argentino/ (Consultado 13/09/2017)

1.-Mediante cualquier forma de ardid o engaño, indebidamente obtuviere o capturare datos personales, financieros o confidenciales.

2. Con fines ilícitos, diseñare, programare, desarrollare, vendiere, ejecutare, facilitare o enviare un dispositivo, sistema o programa informático, destinados a la indebida obtención o actuar de datos personales financieros o confidenciales…"

Sin embargo, dicha enmienda no ha prosperado, por lo que sigue sin considerarse como un ilícito la mera obtención de datos personales, financieros o confidenciales, mediante el uso de las nuevas tecnologías, específicamente de los medios informáticos, sino que para que se configure como delito debe existir el prejuicio patrimonial.

2.5.4. ESPAÑA.

Como se estudió con anterioridad, los Estados miembros de la Unión Europea por conducto del Consejo de Europa han establecido diversas medidas que se han adoptado en lo referente a la lucha contra el fraude cometido con ayuda de medios electrónicos, por lo que cada miembro es responsable de adoptar las medidas necesarias a efecto de garantizar que dichas conductas ilícitas no se produzcan de manera deliberada dentro de su competencia territorial, por lo que el Gobierno Español adicionó al Código Penal el 22 de junio de 2010, en su artículo 248 la reforma siguiente:

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

2.- También se consideran reos de estafa:

a) Los que, con ánimo de lucro, valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro[101]*…"*

De tal manera que, con esta adición al Código Penal Español, se establece un medio alterno, diverso al de la estafa convencional que se realiza de manera interpersonal, pues plantea que también es equiparable al fraude cuando dicha actividad es realizada mediante la manipulación de medios electrónicos o algún artificio similar en el cual se consiga una transferencia no consentida por el titular de la cuenta, de cualquier activo patrimonial, siempre y cuando cause un perjuicio a la víctima.

Por otro lado, recordemos que el phishing tiene diversos momentos, es decir, que se deben de configurar diversos supuestos a fin de que se configure por completo y se obtenga el beneficio económico, por lo que se requiere de una organización de sujetos para que puedan llevarse a cabo cada una de las etapas, por lo que el ordenamiento en estudio, en el capítulo de daños, articulo 264, se refiere a los daños causados a los datos que obren en sistemas informáticos o al acceso de los mismos sin autorización. En su fracción segunda refiere a un incremento en las penas en diversos supuestos, para el tema que nos atañe son los siguientes:

"Artículo 264.

1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

[101] Ley Orgánica 10/1995, 23 de noviembre, del Código Penal. https://www.boe.es/diario_boe/txt.php?id=BOE-A-1995-25444 (Consultado 13/09/2017)

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1. Se hubiese cometido en el marco de una organización criminal…[102]"

Como puede apreciarse, dicho Código reconoce en algunos ilícitos cometidos a través de medios electrónicos, que estos pueden realizarse por parte de una organización criminal, además este artículo sería aplicable si, para cometer el ilícito de phishing el cual tiene diversas modalidades, si se insertara un malware a que permitiera el envío masivo de correos electrónicos, que causara algún daño al equipo de cómputo, tal como en el caso del pharming.

En lo referente a la obtención de los datos confidenciales a través del engaño, tal como es el caso de las legislaciones previamente estudiadas no existe regulación específica, los abogados Samuel Guerrero y Pau Vidal realizaron el siguiente análisis en la revista "LAWYERPRESS":

"2. Fase de recogida o "pesca" de información en forma de datos personales de los usuarios: Aun accediendo el sujeto activo a información íntima o secreta de la víctima, el desarrollo de la conducta propia del "phishing" supondría la inaplicación del artículo 197.3 CP ya que a la información a la que se accede viene proporcionada por el propio sujeto pasivo; esto sí, mediante un ardid o técnica "informática o artificio semejante", de manera inconsciente y subrepticia[103]."

El artículo 197, inicia el capítulo referente al descubrimiento y revelación de secretos, señala lo siguiente:

"Artículo 197.

[102] Ídem.
[103] Guerrero, Samuel. Colab. Vidal Pau, "El "Phishing" como delito de estafa informática, Lawyerpress, Madrid 2013. http://www.lawyerpress.com/news/2013_07/3107_13_005.html

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior[104]."

Del análisis de lo anterior es posible destacar, que el ciber criminal obtiene diversos datos de tipo confidencial a través del uso de medios informáticos con una serie de trucos o artimañas para tal motivo, sin embargo, no los obtiene per se, pues no accede directamente a una base de datos de manera física ni remota utilizando un ordenador, si no

[104] Ley Orgánica 10/1995, 23 de noviembre, del Código Penal. https://www.boe.es/diario_boe/txt.php?id=BOE-A-1995-25444 (Consultado 13/09/2017)

que mediante el engaño coacciona a la víctima para que se los entregue de mutuo propio, razón por la cual queda sin aplicación el referido artículo, así mismo la cesión de dichos datos que menciona la fracción tercera queda excluida automáticamente, al no encuadrar exactamente en el tipo penal.

Una vez consumado el acto, se necesita la transferencia de los activos patrimoniales a que se refiere el artículo 248, pero como se ha referido, dicho móvil delictivo está muy bien planeado, por lo que transferir dinero a cuentas propias de los delincuentes, sería demasiado obvio, por lo que transfieren el botín a cuentas de terceros, lo que se le conoce como blanqueamiento de capitales, figura que se encuentra tipificada en el código penal español en el artículo 300 y 301, en el que delimita el grado de participación, así como el desconocimiento o irresponsabilidad del tercero, dependiendo el grado de participación y las suma recibida.

Así las cosas, no existe aún en el marco jurídico español, una normativa integral que permita castigar el delito del phishing, situación que como en el resto de los países incluido México a falta de una legislación adecuada, deberá ser resuelto por los altos tribunales con el dictado de los diversos criterios jurisprudenciales, así como por la doctrina.

Su equiparación con el delito de Fraude no es suficiente, pues implica una serie de acciones diversas para alcanzar en su totalidad su fin, no solo el engaño a las víctimas potenciales. Se necesitan de esfuerzos conjuntos internacionales para regular los diversos aspectos informáticos, no solo en lo referente a el phishing, si no a todas las actividades que se realizan utilizando medios informáticos, pues es obligación de los Estados otorgar plena seguridad jurídica a los usuarios de dichos medios.

En México, existe una importante iniciativa de Ley en este rubro, propuesta por la Cámara de Diputados en la que se pretende adecuar el Código Penal para castigar los delitos informáticos, dentro de los cuales se tiene considerado al phishing, pero de igual manera que en los demás países se equipara al delito de fraude, dejando insubsisten-

tes y desprotegidas las demás etapas del phishing, dicha propuesta radica en lo siguiente:

> *"También se equipará al delito de fraude y se sancionará con pena de seis meses a tres años de prisión y de 100 a 400 días multa, a quien valiéndose del error en que se encuentra la víctima provoque que revele o ponga a su disposición información o datos de carácter personal, patrimonial o financiero a los que no tenga derecho a acceder, utilizando para tales fines sitios o direcciones de correo u otros medios electrónicos creados por él mismo o por un tercero*[105]*…"*

Sin duda, queda mucho por hacer y el tiempo para implementar acciones es muy reducido, pues día con día se perfeccionan los métodos existentes y se crean otros nuevos, por lo que las legislaciones de los Estados no pueden quedarse rezagadas.

[105] Boletín 4934, Adecuan el Código Penal para castigar delitos informáticos. http://www3.diputados.gob.mx/camara/005_comunicacion/a_boletines/2012_2012/003_marzo/28_28/4943_adecuan_el_codigo_penal_federal_para_castigar_delitos_informaticos (Consultado 14/09/2017)

CAPITULO TERCERO.
ASPECTOS Y CONSECUENCIAS JURÍDICAS DEL PHISHING.

3.1.- SUPLANTACIÓN DE IDENTIDAD.

El concepto de identidad es propiamente referente al conjunto de rasgos específicos de un individuo o de un grupo específico. Con el creciente desarrollo de las nuevas tecnologías, específicamente hablando de la red de redes a la cual conocemos como internet, ha dado la posibilidad de crear un nuevo espacio, una nueva dimensión que puede ser tan grande como el universo mismo, en la cual podemos interactuar en ella de manera similar a como lo hacemos en la vida cotidiana utilizando los rasgos distintivos que nos identifican como persona, o bien podemos utilizarla de manera anónima, dependiendo de las actividades que se pretendan desarrollar en este sistema de transferencia de datos.

La identidad como derecho fundamental inherente a los atributos de la personalidad, es un aspecto en la individualización de las personas, pues hace referencia a un conjunto de características, datos o informaciones que permiten identificar de manera específica a un sujeto. Dichos atributos, son parte importante en las relaciones sociales, debido a que con estas se crean consecuencias de derecho, además existen signos personales distintivos como la firma, la huella dactilar, las contraseñas digitales, imagen institucional, etc. que son factores únicos e irremplazables mediante las cuales jurídicamente podemos obligarnos.

“En el mundo real nuestra identidad nos acompaña siempre; es lo que somos. En cambio, en el mundo virtual somos lo que decimos ser. Interactuar en el ciberespacio significa crear una representación de uno mismo de manera digital, misma que se va gene-

rando conforme a la interacción en dicho medio…[106]" y a la información personal que nosotros mismos proporcionamos con la necesidad de suscribirnos a las distintas actividades que ofrece este medio, que van desde las ociosas o sociales, hasta actividades de corte comercial.

Existe un inminente peligro por la gran aceleración en la tendencia que existe en el uso de los medios electrónicos, derivado de su rápida evolución y especialización existe una gran diferencia entre quien sabe utilizar dichas tecnologías de manera óptima o profesional, quienes la utilizan de forma básica o habitual y de aquellos que ni siquiera tienen acceso a este tipo de medios de comunicación, a este fenómeno se le ha denominado como "brecha digital". Por lo que en aspectos de seguridad informática el usuario común o regular de dichos medios tecnológicos se considera como el eslabón más débil de la cadena, pues por su inexperiencia o desinformación es más susceptible de ser víctima de diversos ataques cibernéticos, algunos de ellos referentes a la suplantación de identidad de personas físicas o jurídicas través de medios digitales que pueden conllevar a serias repercusiones económicas.

Derivado de lo anterior, han existido ciertos personajes que se han querido apoderar de aquellas características específicas que nos distinguen a un sujeto del otro, de esos elementos personalísimos que nos permiten identificarnos en el mundo digital y que pueden ser sustraídos por medio de técnicas especializadas implementadas por uno o diversos sujetos, suelen tener la finalidad de conseguir un aprovechamiento preponderantemente económico. El ardid es sumamente funcional, pues la finalidad es la de actuar en nombre del suplantado para la obtención de un beneficio o un lucro indebido sin comprometer la propia esfera jurídica de quien obra de mala fe. De tal manera que el hurto o robo de identidad consiste en el hecho de hacerse pasar por otro, con la previa apropiación indebida de la información de identificación que nos hace únicos, tales como el nombre, fecha de nacimiento, números de seguridad social, etc.

[106] Sanchis Crespo, Carolina Coord. *Et all,* Fraude Electrónico: Entidades Financieras y Usuarios de Banca, 1ª edición, Ed. [Thomson Reuters] Aranzadi, España 2011.

Como se ha podido apreciar a lo largo de este trabajo de investigación el ataque de phishing se construye por diversas fases o etapas, alguno de ellos es el referente a la suplantación de identidad que se presenta en dos momentos específicos y a sujetos diversos en cada uno de ellos; El primero, consiste en la suplantación de una página web perteneciente a una entidad financiera o a un grupo empresarial de reputación conocida que dentro de su giro comercial se dediquen usualmente a la venta de bienes u ofrezcan algún tipo de servicios por los cuales acepten diversos medios de pagos verbigracia, las transferencias electrónicas, o bien terceros que actúen como intermediarios en los cuales se puede utilizar el denominado "*e-cash*". Dicha imitación, servirá de anzuelo con el cuál se hará creer y generar confianza al usuario mediante diversos artilugios que se encuentra interactuando en el sitio real de la empresa o entidad suplantada, derivado de esto, ingresará sus datos de manera habitual sin ninguna preocupación, una vez capturados los datos de identificación en dicha interfaz falsa, estos serán recolectados por los delincuentes, para usarlos sin autorización del titular.

Explicado el paso anterior, el segundo momento se encuentra íntimamente ligado a lo establecido en el párrafo anterior, puesto que una vez que se obtienen los datos personales de identificación y autenticación del usuario de los servicios financieros por conducto del sitio web falso, tales como claves de acceso o firmas electrónicas, nip's de acceso, etc. se pueden disponer libremente de ellos, actuando en nombre y representación de su titular sin su consentimiento, con los que abiertamente pueden de manera anónima realizar transferencias de capitales, compra de bienes, o pago de servicios hasta por el monto total con el que cuente el saldo de la cuenta monetaria.

Es pertinente analizar estos dos supuestos con un poco más de detalle; En el primero de los casos la suplantación se encuentra enfocada a diseñar una página web que contenga los rasgos característicos de las entidades financieras reconocidas, tales como: tipografía, signos distintivos, logos, colores, etc. para lo cual no se necesita ser un gran experto en materia informática o en diseño de páginas web, en la red, existen centenares de manuales de instrucciones o videos tutoriales para el desarrollo de sitios en internet, inclusive se conocen de casos en que se ha identificado programas que se en-

cuentran a la venta en diversos portales de internet, los denominados “Kits de phishing”.

Además de la protección en cuestión de propiedad industrial la cual se ha estudiado en capítulos precedentes[107], la suplantación del sitio web de las entidades financieras presupone el medio ideal para la obtención de la información de carácter privado, pues con esta se le dé más credibilidad al ataque al suponer la víctima que realmente se encuentra en comunicación directa con la institución de preferencia por conducto del sitio fidedigno, cuando no es así.

En este apartado es relevante realizar un análisis respecto de quienes son los sujetos activos en este tipo de empresas u operaciones, pues si bien los ataques requieren de un conjunto de elementos que se encuentran adminiculados para producir sus frutos, no necesariamente todos los procedimientos son realizados por la misma persona, pues como he mencionado, es muy probable que el problema sea generado por una coalición de esfuerzos para conseguir el cometido, que conforme a las diferentes habilidades y virtudes que posee cada persona, serán aportadas para ser explotadas y obtener el máximo beneficio.

Es decir, en el caso específico una persona bien podría realizar o desarrollar el sitio web falso, con la única finalidad de comerciar con éste para diversos fines, o también podría auxiliar en todos el procesos técnicos, ejecutando diversos programas o virus informáticos, enlaces o programas emergentes, o con el envío masivo de correos electrónicos, así como el almacenamiento de los datos obtenidos en diversas bases de datos ocultas en servidores externos a efecto de que no puedan ser identificados o evitar ser detectados, entre otras gestiones.

Por lo anterior, sería pertinente aseverar que las prácticas relativas a los aspectos tecnológicos que sean utilizados para realizar phishing deberán ser atendidas a efecto de que exista una protección integral de la reputación de las entidades financieras, así como de los medios de promoción y vinculación de los servicios que ofrece a sus usua-

[107] Véase Capitulo II, sub tema 2.3.5., apartado Ley de Propiedad Industrial.

rios o clientes, además de lo referente a la protección de la información y los datos de los mismos. Como ejemplo de esto observemos una disposición contenida en la Ley número 1273, la cual modificó el Código Penal de la República de Colombia, agregando un Título denominado "De la protección de la información y los datos", en su artículo 269G, establece lo siguiente:

> ***"ARTÍCULO 269G**: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.*
>
> *En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco a otro sitio personal de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.*
>
> *La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito*[108]*."*

Además, el numeral subsecuente, enlista un conjunto de situaciones hipotéticas en las que podría agravarse el supuesto punitivo de la manera siguiente:

> *"**ARTICULO 269H:** CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:*

[108] Ley número 1273, en adición al Código Penal de la República de Colombia, Título denominado "De la protección de la información y los datos, visible en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2…

3…

4…

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales…[109]".

La disposición previamente citada, establece ciertos parámetros sobre la protección jurídica que se tiene respecto de las circunstancias descritas, sin embargo, se necesitan mecanismos suficientes a efecto de brindar mayor certeza a los usuarios con medidas preventivas, así como medidas de seguridad que deberán adoptar las entidades financieras para asegurar que los medios de comunicación y prestación de servicios financieros que se otorguen por medio de los sistemas automatizados sean seguro y eficientes.

Ahora bien, siguiendo el orden de ideas, como en párrafos previos se mencionó, existe un segundo momento en el que se presenta la suplantación por parte de los delincuentes cibernéticos y esta se materializa una vez que se han obtenido o "pescado" los datos financieros, de esta manera los "phishers" pueden utilizar libremente los datos recabados con diversos propósitos, actuando con la información personal o confidencial como si fuesen titular de la misma, atribuyéndose potestades de una manera ilegítima y además ilegal.

Como bien lo expresó el jurista Rodolfo Romero Flores, "las consecuencias de la atribución de la personalidad, permiten establecer a su vez consecuencias de una conducta para su autor"[110]. Es decir que quien reúna las características suficientes para osten-

[109] Ídem.

[110] Romero Flores, Rodolfo. El Robo o Usurpación de Identidad por Medios Informáticos o Telemáticos: Su Tratamiento Jurídico Penal, Instituto de Investigaciones Jurídicas UNAM, 2010: http://biblio.juridicas.unam.mx/libros/6/2958/20.pdf

tarse como propietario real de diversos datos personalísimos, aunque no lo sea, en primer término, creará consecuencias jurídicas y no jurídicas para aquel por quien se hizo pasar, pues al actuar en su nombre y representación, además de utilizar características únicas del sujeto, automáticamente se presumirá que los hechos o actos son propios, consentidos y voluntarios, mismos que serán generadores de obligaciones. Por otra parte, una vez analizada la situación, evaluando aspectos de forma y fondo, se podrá determinar la responsabilidad de las consecuencias de aquel que actuó en nombre y representación de otro sin su anuencia.

El mismo autor citando al organismo intergubernamental denominado "*Office Identity Fraud Steering Commite of United Kingdom*", señala que: "el robo o hurto de identidad consiste en la recogida de información relativa a la identidad de una persona con la finalidad de obtener un fraude identitario, prescindiendo del hecho de que la víctima sea una persona viva o fallecida"[111]. Es así, que no existen cuestiones específicas para determinar a quien se elegirá como víctima potencial, ejemplo de esto, es que las campañas masivas de correos electrónicos de phishing se envían a millones de destinatarios indistintamente, lo cual no implica ningún esfuerzo para el remitente, pues auxiliado de programas o virus informáticos (los llamados "*bots*[112]") tienen la capacidad de enviar de manera automatizada y en grandes proporciones los mensajes citados y basado únicamente en un aspecto de probabilidad, alguno o algunos de los destinatarios, por diversas circunstancias, cederán sus datos a causa del engaño.

En dicha circunstancia se hace notable que la usurpación por conducto de medios tecnológicos resulta cada vez más especializada e incógnita, pues no se requiere la presencia física directa para interactuar o intentar engañar a alguien, cualquier persona a través del uso de dichas tecnologías mantendrá cierta invisibilidad detrás de los ordenadores o medios electrónicos que faciliten su labor.

---

[111] Romero Flores, Rodolfo. El Robo o Usurpación de Identidad por Medios Informáticos o Telemáticos: Su Tratamiento Jurídico Penal, Instituto de Investigaciones Jurídicas UNAM, 2010: http://biblio.juridicas.unam.mx/libros/6/2958/20.pdf

[112] Los "bots", son programas informáticos que tienen la capacidad de imitar el comportamiento humano referente a la interacción con otros programas computacionales. Disponible en http:// www.identitytheft.org.uk

Para concluir este par de ideas relacionándolas directamente con la práctica del phishing, considerado como un fraude electrónico que tiene un grave impacto en las finanzas de la sociedad, que cometido con los diversos instrumentos tecnológicos los cuales brindan una protección a los delincuentes por el fácil acceso, otorgan confidencialidad o difícil detección de las actividades tendientes a suplantar o robar las identidades, que como pudimos observar, para el caso específico del phishing, se presentan en dos momentos específicos que me atrevo a clasificar de la manera siguiente:

1.-Suplantación de identidad institucional o empresarial online: se refiere a la elaboración apócrifa de una réplica de los sitios web de las instituciones o empresas de renombre, mediante la utilización de los signos distintivos tales como la imagen, el logotipo, el tipo de letra, los colores, así como de un dominio de internet, con la finalidad de engañar a los usuarios utilizando la confianza generada por la creencia de que se encuentran en presencia del sitio real, con el cual generan la obtención de información confidencial para realizar la estafa.

2.-Suplantación de identidad personal online: en este caso el robo de identidad se presenta respecto de la víctima una vez materializado el robo de información sensible, pues se utilizan en su nombre los datos obtenidos con la finalidad de transferir a terceros una cantidad de dinero, o bien, a la compra de bienes y/o servicios.

Es determinante para evitar este tipo de situaciones establecer medidas, procedimientos y actividades en materia legislativa, así como en los usos de las buenas prácticas bancarias y comerciales que permitan un adecuado uso de los medios informáticos, además de brindar certeza, en el caso de las instituciones financieras, que los medios de comunicación empleados con sus clientes o usuarios son seguros. Así mismo, crear conciencia en los internautas de los diversos peligros que conlleva el uso del internet per se, no solo hablando de phishing, o fraudes cometidos en medios electrónicos, sino en general de todo lo relativo a las diversas prácticas conocidas en el universo tecnológico las cuales conllevan una serie de situaciones perniciosas que se pueden presentar, ocasionando un riesgo patrimonial, de salud o hasta de vida, por no utilizar dicho medio de comunicación de manera adecuada y con las precauciones debidas.

3.2.- ACCESO A INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

El manejo, tratamiento, distribución y protección de la información y de los datos personales, ha sido una de las cuestiones que ha tenido mayor relevancia en los asuntos de discusión en los Estados dentro de sus estructuras internas, así como en el ámbito internacional, partiendo de los supuestos y de todas las medidas que se han venido implementando en los últimos años, se ha dado un especial énfasis en materia de derechos humanos, específicamente hablando de aquellos relativos a la protección de la intimidad y de la vida privada, mediante el tratamiento de acceso a la información y protección de datos personales.

Existe un derecho intrínseco que ha sido reconocido como parte de los derechos fundamentales, y es aquel de la protección a la vida privada. Derivado de la automatización y sistematización de las nuevas tecnologías, el tráfico de información personal se convierte en un riesgo efectivo para sus poseedores, por conducto de estas, se hace posible el procesamiento de millones de datos de cualquier índole, que al ser proporcionados por el mismo usuario, éstos pueden ser comparados entre sí de manera automática con cualquier otra base de datos que se encuentre cargada en la grandes autopistas informáticas que son de fácil acceso en el internet, misma que puede ser manipulada y/o utilizada de diversas formas, así como también por diversos sujetos.

He mencionado que en la actualidad el manejo de la información, -partiendo de la premisa que ha existido desde que el ser humano tiene conciencia propia de que el conocimiento se traduce en poder-, se ha convertido en un bien de apropiación comercial, pues la obtención de dichos datos se refleja en una ganancia pecuniaria para aquellos que la detentan, es decir, la información se ha convertido en un bien de consumo, que puede ser utilizada para diversos fines.

Es por ello, que con la modificación de diversas regulaciones, lo Estados han intentado brindar protección a las personas físicas sobre el tratamiento que se tiene sobre la información otorgada por diversas circunstancias, tanto a entidades públicas, como a

empresas de carácter privado, las relaciones que tienen el estado con las empresas, así como los diversos vínculos que pueden existir de los antes mencionados a nivel transnacional, sobre todo en aquellas que han sido implementadas por el desarrollo del comercio electrónico, pues el sin fin de transacciones monetarias que se dan en la red con el uso de medios electrónicos tales como compras, transferencias bancarias, trámites gubernamentales, etc., deriva en un intercambio masivo de datos e información.

Adecuado a las reglas y normas políticas de cada sistema jurídico específico, se han adoptado políticas de regulación respecto a la protección y privacidad de datos en la que existe una homologación entre lo que se encuentra estrictamente regulado por el gobierno y la auto regulación misma que realizan las empresas que responden eficientemente a las necesidades de protección de los ciudadanos y consumidores, mismas que en conjunto fomentan un equilibrio de protección de las distintas esferas jurídicas, conservando los intereses de las medianas y las grandes empresas, medidas que evitan la implementación de medidas arbitrarias y complejas por parte del Estado y que son altamente reforzadas con auxilio de las recomendaciones establecidas por los diversos organismos internacionales.

Ejemplo de esto, son los lineamientos y recomendaciones que ha establecido la OCDE (Organización para la Cooperación y Desarrollo Económicos) respecto al resguardo y privacidad de la información en aras de su protección, además de los cuidados o protecciones necesarias hacia el consumidor en la práctica del comercio electrónico, en el entendido de que dichas prácticas per se conllevan un riesgo entre sí, a efecto de llevar cualquier transacción por medio de las diversas tecnologías de comunicación, se requiere de una autenticación de información con la finalidad de conocer quien pretende llevar a cabo dicha acción y que realmente compruebe su identidad previamente definida por medio de diversas características, como lo puede ser un pre registro en algún sitio web o al carga de información previa a la operación, en una base de datos de con quien se pretenda entablar la relación comercial o de uso de algún servicio.

Las recomendaciones enlistadas por dicha entidad intergubernamental, refiriéndome específicamente a la "Recomendación del Consejo de la OCDE Relativa a los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico"[113] pretenden impulsar leyes políticas y prácticas relativas a limitar ciertas conductas comerciales o aparentemente comerciales, que pudiesen tener intenciones de carácter fraudulento, pues es indispensable para el crecimiento económico el impulso de las actividades que se realizan por medio de los diversos medios informáticos. Dichas protecciones son indispensables para generar confianza entre el oferente y el consumidor en aras de establecer transacciones comerciales más eficientes, económicas, veloces y seguras, protegiendo siempre los intereses del consumidor, con miras siempre a la debida diligencia y protección que debe de brindarse respecto del tratamiento de la información brindada por el cliente o usuarios, su resguardo y difusión.

Dentro de los lineamientos se hace hincapié en diferentes supuestos, que sirven de base para el mejor entendimiento de la protección de datos personales y su tratamiento en medios electrónicos, que puedan derivar en posibles actividades engañosas o fraudulentas, ejemplo de esto en el apartado II se menciona: "*Las empresas no deben realizar ninguna declaración, incurrir en alguna omisión, o comprometerse en alguna práctica que resulte falsa, engañosa, fraudulenta o desleal*[114]*."* Del tema en específico puede desprenderse que aquella acción u omisión que vaya en perjuicio de los consumidores será considerada como una práctica en perjuicio de los buenos usos comerciales, ejemplo de esto, podría ser la transmisión de información privada sin consentimiento del titular para utilizarla en diversos fines siendo estos legales o ilegales. Hablando específicamente del phishing, se sabe que la información necesaria para perfeccionar los ataques puede ser obtenida de cualquier sitio, desde ser extraída de las propias instituciones financieras, hasta de la basura.

Otra de las recomendaciones se encuentra enfocada a la difusión de publicidad u ofrecimiento de servicios en correos electrónicos, pues menciona que la decisión de recibirlos o no es únicamente del destinatario y ésta en caso de ser en sentido negativo debe

[113] https://www.oecd.org/sti/consumer/34023784.pdf Aprobadas el 9 de diciembre de 1999. (Consultado 18/09/2017)
[114] Ídem.

ser respetada. Así mismo, se debería implementar la práctica del olvido con tal negación a efecto de que la información de la dirección de correo electrónico no sea compartida con terceros debido al riesgo que podría generar su mala utilización, como pasa con el caso específico del phishing. En algunos países, los mensajes de información comercial no solicitada por correo electrónico se encuentran sujetos a leyes específicas o autorregulación de las mismas empresas.

Además, la OCDE recomienda que para el tratamiento de la información y a la privacidad en los medios electrónicos, se deben de tomar en cuenta y conducirse conforme a los principios de privacidad reconocidos y establecidos en los Lineamientos que regulan la Protección de la Privacidad y el Flujo Transfronterizo de datos personales de la misma OCDE de 1980, además de la Declaración Ministerial de la OCDE sobre Protección de la Privacidad en Redes Globales 1998[115].

Así como los instrumentos citados con anterioridad, existen diversidad de documentos internacionales que tienen la finalidad específica de contribuir a la mejor protección de los datos personales en las redes globales de comunicación, pues es importante destacar que su uso e implementación rebasa cualquier frontera y la privacidad personal puede estar en riesgo en cualquier parte del mundo por el uso de estos medios. Por ello, es importante que los países implementen y adopten las medidas legislativas pertinentes a efecto de brindar de cierta protección a los usuarios, así como de colaboración internacional para homologar y en su caso coadyuvar en un esquema internacional.

En México se han adoptado diversas medidas que son relativas al tema de la protección de los datos personales y acceso a la información, aspectos que han devenido de los distintos esfuerzos nacionales como internacionales, así como del inicio e implementación de la generación de los llamados derechos ARCO. Existe regulación específica para el tratamiento de la información descrita en este apartado, aplicable tanto para las entidades gubernamentales, así como para el cuidado y manejo de información de

[115] Se puede encontrar un resumen de este apartado en la siguiente liga: http://www.oecd.org/sti/ieconomy/15590267.pdf

carácter privado en posesión de los particulares. La filtración de información en su característica de bien comercial puede surgir de cualquier lado, por ello la importancia de regular su tratamiento en ambas esferas jurídicas, la de gobierno y la de particulares.

Para el caso en concreto de nuestro tema de estudio, que es la figura del phishing, se encuentra estrechamente adminiculada a la transmisión de datos e información personal, sobre todo de aquella que brinde al atacante las facilidades para crear una estrategia personalizada de campañas de pesca de información de usuarios. En esta tesitura, lo que busca el estafador, es encontrar perfiles adecuados y personalizados de las personas a quienes enviará el anzuelo, por lo regular esta acción, se realiza por conducto del correo electrónico. ¿Se dan cuenta? En este momento ya se obtuvo el primer dato personal, si, el correo electrónico de las posibles víctimas. Las preguntas en este momento son ¿Cómo y de donde los obtuvieron?

Sin tomar conciencia de ello, día con día inconscientemente al asistir a algún lugar, requerir un servicio, la creación de un perfil en internet, entre otros, se solicita de manera indistinta nuestra información dentro de la que se encuentra precisamente el correo electrónico. Si se piensa esta situación por un momento, es posible notar la cantidad innumerable de formularios o solicitudes que contienen esta información y se entregan voluntariamente por los usuarios o posibles clientes, bueno pues esa misma información se captura en bases de datos digitales, de las que probablemente se creen respaldos en servidores o nubes digitales. Ahora el cuestionamiento principal es ¿Cómo esta información que es entregada de manera voluntaria o inconsciente a un sujeto específico llega a manos de terceros?

Existen 3 supuestos. El primero de ellos, es acorde a un consentimiento expreso de su divulgación, pues en la mayoría de las veces existen cláusulas específicas contenidas en los formularios o en los contratos de adhesión en el que se permite la transferencia; El segundo es en el que aún sin el consentimiento, estos se transmiten de manera onerosa o gratuita a terceros con fines de promociones de productos, publicidad o bien obtener un lucro; El tercer supuesto es un poco más complejo, pues existen ciertas técnicas en las que se pueden intervenir sistemas digitales, con el propósito de sustraer in-

formación, que como bien se ha mencionado, repercute en un aprovechamiento para el sustractor.

Una vez obtenidas las direcciones electrónicas de destino de los falsos mensajes, se puede obtener información adicional con la finalidad de realizar ataques más personalizados, los cuales por ende tendrán mayor posibilidad de obtener los frutos deseados. Me explico, en el caso de los ataques enviados a los usuarios de las diversas entidades financieras, específicamente hablando de aquellas que otorgan el servicio de banca y crédito, para el atacante podría resultar de suma utilidad conocer cuáles son las instituciones específicas con las que mantiene un contrato de servicios el o los clientes, pues como se ha explicado con anterioridad, algunos de los ardides utilizados para dicha práctica, es la suplantación de la imagen corporativa de la entidad, situación que dará mayor credibilidad a la situación.

Ahora bien, hablando específicamente de lo descrito con anterioridad, los sujetos que poseen la información de carácter económica o crediticia de los clientes o usuarios de los servicios financieros, de origen, son las mismas instituciones financieras, que se limitan únicamente en su núcleo con sus propios usuarios o clientes. Por el otro lado existen las denominadas sociedades de Información crediticia o también conocidos como burós de crédito que son instituciones financieras, autorizadas por la SHCP, previa opinión del Banco de México y de la CNBV y son organizaciones que proporcionan servicios de recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales[116].

Su objetivo es contribuir al desarrollo económico del país ofreciendo servicios que promueven minimizar el riesgo crediticio, al proporcionar información que ayuda a conocer la experiencia de pago de empresas y personas físicas, lo que, a su vez, contribuye a

[116] Cfr. Información obtenida del portal de la Comisión Nacional Bancaria y de Valores, visible en: http://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/OTROS-SUPERVISADOS/Preguntas-Frecuentes/Paginas/Sociedades-de-Informaci%C3%B3n-Crediticia.aspx (Consultado 14/09/2017)

formar la cultura del crédito entre la población, al tiempo de promover un sano consumo interno[117].

Si bien la protección de la divulgación de la información debe ser protegida a nivel global, en nuestro país contamos con legislación específica que promueve o limita el uso de la información por parte de los diversos entes sociales, en caso de las Sociedades de Información Crediticia (SIC) en su ley específica, la denominada "Ley para regular las Sociedades de Información Crediticia" (LRSIC) en el artículo 28°, dispone el procedimiento específico mediante el cual los usuarios de los servicios que otorga la SIC, deberán obtener el consentimiento por parte de sus clientes a efecto de poder consultar su información conforme a los elementos siguientes:

> *"Las Sociedades sólo podrán proporcionar información a un Usuario, cuando éste cuente con la autorización expresa del Cliente, mediante su firma autógrafa, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que éste podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente[118]".*

Conforme a lo anterior, se entiende que la protección hacia la información crediticia de los usuarios de los servicios financieros siempre estará protegida herméticamente por las sociedades y que esta no podrá ser divulgada de manera alguna sin que antes medie un consentimiento expreso por parte de su titular, el plazo de consulta por los clientes únicamente es por un año, pudiéndose ampliar hasta dos cuando así haya sido autorizado. Cualquier contravención de lo anterior se entenderá como una violación a las disposiciones del Secreto Financiero tanto por parte de la Sociedad como de los funcionarios o empleados. En los casos en que realicen consultas sin autorización, divulguen información o proporcionen datos específicos con fines comerciales, incurrirán en

[117] Información obtenida del portal de la Comisión para la Protección y Defensa de los Usuarios de los Servicios Financieros (CONDUSEF), visible en: http://www.condusef.gob.mx/index.php/instituciones-financieras/sociedades-de-informacion-crediticia/624-sociedades-de-informacion-crediticia-que-son

[118] Extracto del artículo 28°, Ley para regular a las Sociedades de Información Crediticia. http://www.diputados.gob.mx/LeyesBiblio/pdf/237.pdf

el delito de revelación de secretos a que se refiere el artículo 210 del Código Penal Federal[119].

Como dato adicional la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en su artículo 2°, mantiene como supuesto de excepción de aplicabilidad de esta ley en su fracción I a las Sociedades de Información Crediticia, por lo que únicamente se tendrá por aplicable lo establecido por la LRSIC[120]. En ésta, se determina que deberán de adoptar las medidas de seguridad necesaria con la finalidad de evitar el manejo indebido de la información, misma que de ser trasgredida podría ocasionar severos daños patrimoniales, hay que tener en cuenta que la protección no debe ser únicamente interna, pues si bien los empleados o funcionarios podrían obtener una ventaja de su fácil acceso a la información en comento, existen otras maneras de obtener la información de manera remota, por lo que dichas Sociedades deberán de adoptar las medidas de seguridad tecnológicas a efecto de evitar el robo de información a las bases de datos en donde se contenga la información financiera de los usuarios de dichos servicios.

Derivado de lo anterior, se pretende establecer en este trabajo un parámetro que logre identificar el por qué la protección de datos personales como medida preventiva es de suma importancia, pues del flujo, tráfico y robo de información se traduce en un ventaja o aprovechamiento para aquellos que la detenten de manera ilegítima, auxilia de manera significativa a la proliferación de actividades ilícitas, tal como lo es en el caso del phishing, que otorga a aquellos estafadores las herramientas necesarias a efecto de hacer los ataques más especializados, pues al tener indicios tales como un enlace de comunicación como lo es el correo electrónico, nombres, identificación de las instituciones financieras en las que se realizan las principales transacciones, montos de saldos o capacidad crediticia, etc., propicia que los ardides sean más certeros y con mejores probabilidades de ocasionar un decremento económico tanto en el defraudado, como en la integridad del Sistema Financiero Mexicano, que puede conllevar a efectos negativos de carácter globales.

[119] Cfr. Ibidem. P. 17
[120] Cfr. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Puede consultarse en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf (Consultado 14/09/2017)

3.3.- SEGUROS DE PROTECCIÓN ANTI PHISHING.

Se han adoptado diversas medidas específicas por parte de las instituciones financieras para contrarrestar los efectos económicos negativos que produce la práctica del phishing, pues derivado de la escasez de medidas preventivas, de seguridad, legislación y procedimientos de prosecución e investigación referentes a este tipo de prácticas que día con día se hacen más comunes en México, se tienen que buscar alternativas que si bien no son para erradicar por completo estas actividades, sí lo son para intentar contrarrestar los efectos negativos en la economía de los usuarios de los servicios que normalmente se utilizan como medio de pago o ahorro, una alternativa que han encontrado e implementado la mayoría de las instituciones financieras, es la de proporcionar un seguro ya sea de manera onerosa o gratuita como servicio complementario, para la protección de los instrumentos de intercambio monetario en caso de ser víctima de cualquier tipo de práctica fraudulenta.

Un punto importante a considerar, es el gran incremento de estas actividades y el impacto que tienen en la liquidez de los bancos, los usuarios de las instituciones financieras y el Sistema Financiero en general, una vez sufrido y detectado el percance, las instituciones financieras tienen la obligación de realizar el reembolso automático de los fondos en cuestión, con la finalidad de no afectar la liquidez de los usuarios, como se ha mencionado, los afectados primarios y directos son los titulares de los medios de pagos, sobre todo de aquellos que sufren ataques en sus cuentas de débito, en el entendido de que estás se utilizan como medio de pago de nómina o ahorro, que aunque no representa la mayoría de los casos, si representa un porcentaje considerable y sobre todo un impacto directo a la economía de los cuentahabientes, que en comparación con las tarjetas de crédito los fondos sustraídos de estás son de la institución que respalda el plástico o cuenta de crédito.

Como una alternativa para sufragar la afectación tanto para los usuarios como para las instituciones de carácter financiero, se ha tomado la determinación de implementar el contrato de seguro como un soporte económico que permita a ambas partes tener una

protección adicional, pues su finalidad es la de prever un riesgo que de constituirse su realización permita controlar los perjuicios financieros, entendido a éste, como el contrato en virtud del cual una empresa aseguradora se obliga, mediante el pago de una prima, a resarcir el daño o pagar una suma de dinero al verificarse la eventualidad prevista en el contrato[121].

En palabras la profesora León Tovar, establece de manera terminante la importancia del contrato de seguro, brindándole una perspectiva íntimamente relacionada con el concepto de riesgo, mismo, que, al relacionarlo con el tema de estudio, la utilización del sistema financiero y sus múltiples instrumentos que conlleva éste y atinadamente lo expresa de la siguiente forma:

> *"La importancia del seguro se comprende en su esencia práctica cuando se pone en relación con el concepto de riesgo; esto es, con el hecho de que una persona esté expuesta a la eventualidad de un daño en su persona o en su patrimonio, debido a un siniestro y la posibilidad de transferir dicho riesgo a un tercero[122]".*

Este servicio, habitualmente es prestado por un intermediario financiero al que comúnmente se les denomina como Instituciones de seguros. El catedrático de la Fuente Rodríguez define a éstas como a continuación se transcribe:

> *"Las Instituciones de Seguros son aquellas sociedades anónimas de capital fijo o variable, autorizadas por la SHCP, para obligarse mediante el pago de una prima a resarcir un daño o a pagar una suma de dinero al verificarse la eventualidad prevista en el contrato[123]".*

---

[121] Definición adoptada y adecuada del artículo primero de la Ley sobre el Contrato de Seguro, publicada en el Diario Oficial de la Federación el 31 de agosto de 1935. Visible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/211.pdf Última reforma 04 de abril de 2013. (Consultado 14/09/2017)

[122] León Tovar, Soyla H., Contratos mercantiles, Editorial Oxford University Press, 1° edición, 10° reimpresión, México 2012, p. 593.

[123] De la Fuente Rodríguez, Jesús. Tratado de derecho bancario y bursátil, seguros, fianzas, organizaciones y actividades auxiliares del crédito, ahorro y crédito popular, grupos financieros. Sexta Edición, Tomo II, Editorial Porrúa, México 2010. Pp, 1039-1040.

En la actualidad con la nueva ley que regula el sector referente a las instituciones de seguros, la "Ley de Instituciones de seguros y fianzas" publicada en el Diario Oficial de la Federación el 4 de abril de 2013, en su artículo 11 menciona que la autorización para operar como institución aseguradora corresponde al Gobierno Federal por Conducto de la CNSF "Comisión Nacional de Seguros y Fianzas".

> *"ARTÍCULO 11.- Para organizarse y operar como Institución o Sociedad Mutualista se requiere autorización del Gobierno Federal, que compete otorgar discrecionalmente a la Comisión, previo acuerdo de su Junta de Gobierno. Por su naturaleza, estas autorizaciones serán intransmisibles[124]."*

Por otro lado, el docto en la materia en el mismo tratado brinda una definición sobre el contrato de seguro que para mejor entendimiento el cual me permito citar a continuación:

> *"Desde un punto de vista material, es el documento o póliza suscrito con una entidad de seguros, en el que se establecen las normas que han de regular la relación contractual de aseguramiento entre ambas partes (asegurador y asegurado), especificándose sus derechos y obligaciones respectivos[125]".*

Así mismo, el Doctor Vásquez del Mercado, en su obra "Contratos Mercantiles", menciona que es muy difícil o que se ha dudado que sea posible dar un concepto sobre el contrato de seguro que sea congruente con todas las operaciones, derivado a la gran diferencia que existe entre el seguro de daños y seguro de personas, no obstante, presenta el siguiente acercamiento:

> *"…se ha venido aceptando como concepto de contrato de seguro la relación jurídica en virtud de la cual la empresa aseguradora, contra el pago de una prima se*

[124]Ley de Instituciones de seguros y fianzas, última reforma publicada en el DOF 10 de enero de 2014. Puede consultarse en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LISF.pdf (Fecha de consulta 14/10/2017)
[125] Ibídem. P. 1062

obliga a relevar al asegurado en los términos convenidos de las consecuencias de un evento dañoso e incierto[126].

Conforme a las definiciones anteriores, se aprecia de manera muy general los diversos elementos personales (asegurador, asegurado y beneficiario), los elementos formales (respecto a la exteriorización del consentimiento y la validez ante la falta de forma), así como lo elementos reales (objetos o intereses asegurables, la póliza, la prima, el riesgo y los siniestros) mediante los cuales realizaré el análisis respectivo de los seguros que ofrecen las diversas instituciones financieras a sus clientes como medio de protección ante posibles fraudes hacia los medios de pago electrónicos que puede traducirse en su clonación, manipulación de sistemas de disposición de efectivo, robo de identidad, así como el robo de información y claves de acceso privadas que es el caso en específico de nuestro tema de estudio, el phishing.

Dicho lo anterior, las diversas empresas que brindan la facilidad a sus clientes de realizar pagos utilizando medios informáticos, electrónicos o magnéticos, primordialmente las instituciones de banca múltiple se han dado a la tarea de contrarrestar los efectos de las diversas prácticas fraudulentas con la contratación de seguros especiales que protejan de manera integral tanto a los clientes como a la misma institución. Como ya se mencionó algunos de éstos se otorgan de manera conjunta al producto ofertado por la institución y otros cuantos se pueden contratar de manera independiente por el usuario, sin embargo, debido al costo extra que genera esta prestación, muchos cuentahabientes omiten esta prestación adicional, pues las pocas personas que conocen acerca de los riesgos de esta ilícito consideran poco probable en convertirse en víctimas de este tipo de prácticas.

Aunque la finalidad de la contratación de esta gama de seguros especializados es la misma, es decir, la de intentar de manera preventiva disminuir los estragos de la consumación del probable riesgo, que en el caso específico del phishing sería la obtención de los recursos mediante el uso de los datos de identificación del cliente sin su consen-

[126] Vásquez del Mercado Cordero, Oscar. Contratos Mercantiles, 16° Edición, Primera reimpresión, Editorial Porrúa, México 2014. P. 269

timiento, las características del seguro serán variables dependiendo de quién es el sujeto contratante.

En el caso de aquellos seguros que se encuentran incluidos como prestación general en el contrato de crédito o de ahorro celebrado con la institución financiera, ésta será la contratante directo, es decir, el asegurado, quien en caso de producirse el siniestro, se encontrará con la posibilidad de resarcir el daño ocasionado al beneficiario que en este caso será el usuario afectado, mediante el abono del dinero que cubre la póliza contratada, previa investigación sobre los sobre los hechos ocurridos. Conforme a la Ley Para la Transparencia y Ordenamiento de los Servicios Financieros, en caso de presentarse alguna anomalía conforme a cargos no reconocidos o transacciones no aprobadas por los clientes las entidades que se vean reflejados en los estados de cuenta respectivos o en los medios electrónicos, ópticos o de cualquier otra índole que se hubieren pactado, deberán de aplicar el procedimiento que indica el artículo 23°, que procederá contra la solicitud de aclaración dentro del plazo de 90 días naturales a la fecha de corte o, en su caso, de la realización de la operación o del servicio[127].

Una vez realizada la investigación la entidad determinará con los elementos y evidencia suficiente, la procedencia o improcedencia de la reclamación, que en caso de ser procedente, el dictamen en el que se incluyan todos los elementos suficientes con pruebas indicativas de que se ha materializado la conducta, servirá como prueba documental para hacer efectivo el seguro ante la entidad aseguradora y los beneficios o resarcimiento se aplicará directamente a los fondos de la entidad financiera quien se encargará directamente de la gestión de la aplicación de las cláusulas de la póliza del seguro.

En caso de ser un servicio complementario que ofrezca la entidad financiera como una protección adicional a los instrumentos financieros, en la que sea opcional su contratación de manera independiente, el asegurado y a la vez beneficiario, será el titular de la

[127] Véase el artículo 23° de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, en el que se describe el procedimiento para presentar la reclamación a las entidades financieras o bien ante las unidades especializadas. Puede consultarse en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LTOSF.pdf última reforma publicada el 10 de enero de 2014.

cuenta, cabe mencionar que en ningún momento las entidades podrán condicionar la contratación de operaciones o servicios financieros a la contratación de otra operación o servicio, aunque para las entidades esta práctica sea la más común por las ganancias económicas que les genera, aunque como se mencionó con antelación, la población en general al tener el mínimo conocimientos sobre estas prácticas por su insuficiente difusión, omiten por completo los riesgos en los que se encuentran inmersos por el simple hecho de ser titulares de un instrumento de crédito.

Evidentemente, la triangulación que implica la contratación de un seguro especializado por parte de la aseguradora, la institución financiera y el beneficiario que es el cuentahabiente genera gastos extra para la institución e incremento en las gestiones necesarias para la solución de la contingencia suscitada, por lo que generalmente dichas entidades recurren a diversos argumentos que les permitan sustraerse de las obligaciones con sus clientes. Uno de los más recurrentes en casos de “Phishing”, es aquel en que las entidades indican a sus clientes, que la reclamación es improcedente en virtud de que ellos entregaron la información confidencial que permitió la disposición o utilización de los recursos de manera voluntaria, arguyendo que los usuarios están actuando de mala fe, pues a pesar de que estas prácticas lastimosas son bien conocidas por los integrantes del sector financiero, prefieren no ocuparse en primera instancia del asunto.

Derivado de lo anterior, los clientes deben de recurrir a otras instancias tanto administrativas como jurisdiccionales, ante la apatía de las instituciones bancarias de buscar una solución a la problemática ante los hechos concretos presentados, que les permitan solventar la afectación económica de la que han sido víctimas de este tipo de métodos de ingeniería social como lo es el “phishing”.

Actualmente en México cuenta con la Comisión Nacional para la Defensa de los Usuarios de los Servicios Financieros, autoridad que se encarga de atender las reclamaciones de los usuarios que han sido víctimas de actividades que pueden ser imputables a un posible delito de fraude o robo. Sus funciones son únicamente de carácter conciliatorio e intentan resolver la problemática entre el cliente y la institución de manera direc-

ta mediante un convenio o una transacción que se presenta derivado de las investigaciones y elementos presentados por la misma institución financiera. Dado el caso en el que no se pueda resolver por esta vía, la autoridad conciliatoria deja a salvo los derechos de los usuarios de los servicios financieros a efecto de que éstos hagan valer sus derechos ante la autoridad jurisdiccional correspondiente según sea el caso específico.

La CONDUSEF por conducto de diversos medios de comunicación tales como boletines, circulares, páginas web, etc. ha emitido una serie de recomendaciones preventivas tanto al público usuario de los servicios financieros a efecto de que procuren mantener buenas prácticas respecto a la protección de su información confidencial. Así mismo se han emitido recomendaciones a la Asociación Mexicana de Bancos de México (ABM) con la finalidad de tomar las medidas necesarias para proteger los intereses de los usuarios en la contratación y uso de productos o servicios financieros[128].

Conforme a las estadísticas semestrales publicadas por la misma CONDUSEF, informó que, durante el primer semestre de 2015, las posibles reclamaciones atendidas por dicho organismo por actividades relacionadas con un posible robo de identidad, que puede ser derivado de diversas prácticas de ingeniería social, una de ellas el phishing. La autoridad comenta que ha existido un incremento del 40% con respecto al mismo periodo del año 2014, de las quejas atendidas relacionadas con este supuesto, es decir, de 20 mil 168 quejas atendidas en 2014, en el primer semestre de 2015, han sido atendidas 28 mil 258 quejas[129], lo cual es un incremento considerable pues el impacto económico que tienen este tipo de prácticas ascienden a 118 millones de pesos, de los cual únicamente has sido abonados a las cuentas de los titulares 69 millones de pesos, menos del 60%, lo que implica una afectación directa a la economía del Estado mexicano, las Instituciones Financieras y sus usuarios.

Es por esto que las entidades financieras insisten con la contratación de seguros de protección bancarios, pues facilitarían de manera considerable los gastos de las ges-

[128] Información obtenida del portal web de la CONDUSEF, el cual puede consultarse en: http://www.gob.mx/condusef/prensa/aumentan-40-reclamaciones-imputable-a-posible-robo-de-identidad-en-primer-semestre-de-2015.
[129] Ídem.

tiones para atender este tipo de contingencias, además de que para éstas, en la mayoría de los casos, cuando son ellos que ofrecen este tipo de servicios se seguros, representan un ingreso extra de capital, pero, para los contratantes de estos productos representa un gasto constante con la incertidumbre de si se puede llegar a presentar la materialización del riesgo o no.

Los principales riesgos contemplados por los seguros contra fraudes en tarjetas de crédito y débito, que son los principales instrumentos afectados por estas prácticas son: Robo extravío o clonación; Protección por retiro de efectivo en ventanilla o cajeros automáticos; operaciones realizadas por internet, en este caso en específico entra en los supuestos que se encuadran dentro del phishing, pues si algún tercero utiliza sin autorización los NIP, claves bancarias, token o tarjetas de seguridad utilizadas en los diversos portales bancarios, el seguro cubre este tipo de incidentes; utilización forzada por terceros; robo con violencia; uso fraudulento de celular; asistencia por robo de identidad. En este caso en específico, algunos seguros otorgan a los clientes asistencia legal, así como auxilio con las autoridades a efecto de realizar las gestiones judiciales y extrajudiciales que permitan deslindar al titular del mal uso que pudiese llegar a darse de dichos instrumentos. Normalmente este tipo de coberturas únicamente cubre cierto número de eventos al año y un límite en los montos de protección.

Son diversas las medidas que se han implementado a efecto de frenar este tipo de actividades, aún queda mucho camino por recorrer, las nuevas prácticas se desarrollan con una rapidez exponencial, es por ello que deben de actualizar constantemente las acciones que permitan amortiguar los estragos económicos que derivan de estas actividades ilícitas, este trabajo deberá desarrollarse de manera conjunta con el Gobierno y sector financiero a efecto de generar conciencia en la sociedad del adecuado manejo que se le debe de dar a los instrumentos financieros utilizados como medios de pago, así como la generación de nuevas medidas de protección que vayan acordes a los productos y servicios que se ofrecen al público en general, que sirvan para aminorar los riesgos que conlleva su uso.

3.4.- FRAUDE.

Como se ha mencionado en reiteradas ocasiones el phishing tiene como fin primordial y último, obtener una serie de recursos de manera ilícita, lo que se traduce en un daño o afectación patrimonial para las víctimas lo que ha dado pie a una clasificación especial en la categorización de los delitos de carácter patrimonial que se cometen con la utilización de medios electrónicos. Existen algunas salvedades, pues las estructuras de la comisión de estos delitos deben delimitarse, pues tal como ha expresado el jurista Romeo Casabona:

> *"las nuevas tecnologías informáticas deben ser reducidas a sus justos términos. En efecto, no se debe entender que por el simple hecho de que en una conducta intervenga un elemento del ámbito informático o un medio electrónico, esté sea un delito informático[130]".*

En la última década, el índice de delitos patrimoniales que se han materializado mediante el uso de dispositivos electrónicos ha aumentado de manera considerable. En el caso del phishing es considerado por diversas legislaciones nacionales, así como internacionales, tal y como se ha explicado en capítulos precedentes, esta figura en muchas de ellas equiparable al Fraude, otras tantas lo categorizan en un apartado específico de delitos informáticos o de manipulación de los medios computacionales.

Para el caso genérico del fraude o estafa electrónica se considera que la práctica de aquellos que con ánimo de lucro y con el auxilio de alguna manipulación informática o artificio similar logren la transferencia o disposición de cualquier activo patrimonial en perjuicio de un tercero, para el caso en concreto de la figura en estudio, la manipulación no es realizada a los medios informáticos, sino que es por conducto de éstos, con los que se pretende engañar al poseedor legítimo de los recursos patrimoniales a efecto de sustraerlos mediante el artífice efectuado por las diversas prácticas de ingeniería social que han sido previamente planteadas.

---

[130] Romeo Casabona, C. M. Poder informático y seguridad jurídica, Fundesco, Madrid 1997, p. 41. Citado por Azola Calderón, Luis. Delitos Informáticos y Derecho Penal, Ubijus, México 2010, p. 51.

La facilidad que otorgan las diversas herramientas tecnológicas para perfeccionar los mecanismos de estafa en el phishing, como es el caso de la suplantación tanto de las páginas web de las instituciones financieras mediante programas de diseño y manufactura de páginas web, el envío masivo de mensajes engañosos o de correos electrónicos o servicios de mensajería instantánea y la capacidad de recolección de grandes fluidos de datos en servidores alrededor del mundo, que posteriormente servirán para realizar vía plataformas digitales bancarias, transferencias o disposición de fondos sin la necesidad de realizarlo físicamente, en nombre, representación y sin el consentimiento de aquellos que han sido víctimas de la trampa, y que sin intención han entregado sus datos confidenciales a un tercero, son el cúmulo de acciones relacionadas con el phishing que realiza o realizan los sujetos que intervienen en estas prácticas por dichos medios.

Es de suma importancia tener en consideración los diversos momentos y ambientes en los que se desarrolla de manera sucesiva y continúa el phishing, pues cualquiera de las prácticas previamente descritas pueden materializarse individualmente o ser desarrollada por diversos sujetos con diferentes fines al planteado en este tema, es necesario tener en consideración para la prevención y debido conocimiento para la regulación y su posterior aplicación al caso concreto, que para que se materialice completamente el phishing, deben de existir ciertos elementos específicos que son los siguientes:

1. La obtención por cualquier medio de ingeniería social a través de sistemas informáticos, de datos confidenciales o sensibles relacionados con la seguridad de las cuentas que representen activos económicos y;

2. La utilización de dichos datos cuando se traduzcan en la afectación económica o en el decremento patrimonial del sujeto engañado.

Es por lo anterior, que algunas legislaciones y doctrinas equiparan a la figura del phishing, como quedó explicado en el segundo capítulo de este trabajo pues abarca en

gran medida los elementos que conformas el tipo penal del fraude. El Código Penal Federal tipifica el delito de fraude de la siguiente manera:

> *"Artículo 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido."*

La legislación en comento contempla la figura del fraude, sin embargo, en todo el apartado destinado para su tipificación no se realiza ninguna distinción referente a su realización por conducto de medios o sistemas informáticos. Por lo anterior, estudiemos unas series definiciones doctrinarias a efecto de hacer una distinción del fraude común y su especialización por los medios de su comisión.

El jurista Camacho Losa propone la siguiente definición de fraude informático:

> *"toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito."*

El Doctor Santiago Acurio del Pino, se inspira en la definición del Código Español proponiendo la siguiente:

> *"El fraude informático consiste en la manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial de manera no consentida[131]."*

Por otro lado, el maestro Azola define al fraude informático como:

> *"…cualquier conducta y/o manipulación realizada a través o por medio de un sistema informático, con el objeto de obtener un beneficio ilegítimo ocasionando un perjuicio a una o varias personas[132]."*

---

[131] Acurio del Pino, Santiago. Delitos Informáticos: Generalidades. Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf , p.41

El autor Calderón Cerezo, hace explicita la función de los medios informáticos como la herramienta principal en la comisión de diversos ilícitos y nos expone algunos ejemplos de la siguiente manera:

> *"Defraudación en función de que el engaño constituya, en todo o en parte el medio comisivo: estafa, apropiación indebida, defraudación del fluido eléctrico y análogos e insolvencias punibles. Entre los delitos económicos se encuentran los siguientes: alteración de los precios en concursos y subastas públicas; relativos a la propiedad intelectual e industrial; relativos a los mercados y a los consumidores; sustracción de cosa propia a su utilidad social; delitos societarios, y receptación y otras conductas afines entre las que destacan las de blanqueo de capitales[133]."*

De la clasificación previamente expuesta podemos identificar algunos de los, supuestos que son propios del phishing, tal es el caso de los relacionados a la propiedad industrial, la receptación y el blanqueo de capitales, mismos que se han contemplado en este trabajo de investigación para su estudio. El conjunto de las diversas prácticas tiene como fin primordial la realización del fraude en sí, que en actividades concatenadas producirá el efecto deseado con mayor exactitud y eficiencia, situación que pone en jaque a las instituciones financieras, a sus usuarios y en gran medida a la estabilidad del Sistema Financiero Mexicano.

De esta manera, la doctrina hace una distinción sobre la clasificación del delito en orden a la afectación principal, que se dividen en delitos del orden patrimonial y delitos de carácter socioeconómico. A pesar de que en un primer término el phishing puede apreciarse como una afectación del orden patrimonial, pues el menoscabo deriva en el enriquecimiento ilícito de un tercero que actúa de mala fe, no se considera de esta manera, pues en el caso específico de los delitos informáticos se considera que el menoscabo es sobre el propio equipo informático o sobre la información contenida en él, por

---

[132] Azola Calderón, Luis. Delitos Informáticos y Derecho Penal, Ubijus, México 2010, p. 51.
[133] Calderón Cerezo, A., Choclan Montalvo, J.A., Derecho Penal. Parte especial, Tomo II, Editorial Bosch, Barcelona 2001, p. 222.

lo que esta práctica entonces deberá ser considerado dentro de aquellos clasificados como del orden socioeconómico, pues la estafa se deriva de la utilización de los equipos informáticos y de las herramientas que contienen los ordenadores para perfeccionar el engaño, que de producir sus efectos se traducirá en un decremento en el patrimonio del defraudado, una obligación para aquellos que deban realizar las investigaciones pertinentes para el esclarecimiento de los hechos y para el caso de que no se pueda resarcir el daño, ocasionará que la obligación tenga que ser cubierta por el Estado en aras de mantener el equilibrio en la sociedad.

Tiene cierta relevancia para este trabajo de investigación, delimitar de manera precisa los efectos y consecuencias jurídicas que emanan del phishing, si es práctico que se homologue con el delito del fraude con características especializadas o bien que se catalogue en otra serie de delitos dentro de las legislaciones pertinentes. En esencia nos referimos al fraude debido a que, a través del engaño o el desconocimiento que se causa el perjuicio económico al afectado directo, lo cual es la parte medular y el fin de esta artimaña social, sin embargo, no se puede dejar de lado todas las demás actividades que se realizan para conseguir dicho fin, pues en su realización trasgrede diversas esferas jurídicas que el derecho tiene como lógica procurar a efecto de mantener el orden social. Todas estas ideas serán materia de estudio en el capítulo subsecuente en el que intentaremos discernir cual es la mejor manera de prevenir, legislar, perseguir y aplicar diversos mecanismos la práctica del phishing que tanto afecta a la estabilidad del Sistema Financiero Mexicano y directamente al patrimonio de sus usuarios.

3.5.- LAVADO DE DINERO COMO CONSECUENCIA DEL PHISHING.

Dentro de las conductas afines a la práctica del phishing encontramos como el último eslabón de ésta el blanqueo de capitales, o como se le conoce coloquialmente “Lavado de dinero”. Una vez que se han obtenido los datos confidenciales, es decisión de aquel que tiene la posesión no consentida de que es lo que hará con estos, por supuesto todos derivan en obtener una ganancia ilícita, sin embargo, cuando los datos sean utilizados por los “phishers” o por terceros a quienes se los hayan cedido de manera onerosa, la pretensión será la de disponer de los fondos monetarios, lo cual puede reali-

zarse por medio de transferencias electrónicas hacia otras cuentas bancarias en cualquier parte del mundo, o bien mediante la adquisición de productos o servicios a los que se tenga acceso mediante el uso de los medios de pago que se encuentran disponibles en la red.

De esta manera también se procura por parte de los delincuentes, que la disposición de los recursos se realice de la manera más discreta y rápida posible, pues el tiempo que tienen antes de que los titulares de las cuentas afectadas se percaten del robo y mal uso de su información es muy corto, además a la par las instituciones financieras han desarrollado mecanismos para rastrear el destino de los recursos, siguiendo los movimientos realizados en la cuenta de sus clientes, situación que limita el campo de acción para los desarrolladores de phishing, pues los sistemas de las entidades permiten detectar movimientos inusuales, es decir de comportamientos o compras que no sean habituales en el historial del cliente en el uso del crédito, además los defraudadores corren el riesgo de ser descubiertos, pues todas las transacciones digitales son monitoreadas y dejan una huella que permite verificar la totalidad de las transferencias monetarias, que siempre y cuando estos recursos no salgan del sistema de pagos, pueden servir para identificar la ubicación del capital y dar con la identidad de los autores de la práctica en estudio.

Ahora bien, para que exista un mayor entendimiento del tema referente al blanqueo de capitales y su relación con el phishing, brevemente desarrollaré sus antecedentes, así como los principales conceptos elaborados por los principales organismos internacionales participes del tema, así como algunas definiciones doctrinarias, que finalmente será posible homologar y entender como estas prácticas en conjunto afectan en gran medida la economía global y debilitan el Sistema Financiero Mexicano.

La práctica del blanqueamiento de capitales o lavado de dinero comenzó a desarrollarse en Estados Unidos cerca de los años 20’s, derivado de las prohibiciones efectuadas a la compra, venta, transportación y distribución de bebidas alcohólicas. A raíz de esto, grandes grupos de personas vislumbraron una gran oportunidad de enriquecerse ilícitamente mediante el tráfico ilegal, pues a pesar de las prohibiciones, la demanda por la

preciada bebida era bastante alta, por lo que comenzó la proliferación de establecimientos clandestinos en los que producían, ofrecían y distribuían un sinfín de bebidas embriagantes a precios bastante elevados, por lo que representaba un gran ingreso para los contrabandistas. Aunado a esto, el tráfico de armas y extorsiones crecieron de manera desmedida como consecuencia de la lucha de poderes que se presentaba en aquel momento.

En ese entonces, como hasta ahora, es importante par a las organizaciones delictivas la ocultación del dinero proveniente de las actividades ilícitas y disfrazarlo a efecto de que se aparentare que éste ha sido obtenido de una fuente lícita. Derivado de lo anterior a un grupo de la mafia norteamericana le surgió una idea de ocultamiento que llevaron a cabo mediante la compra de una cadena de lavanderías, un negocio totalmente lícito que producía fructuosas ganancias y que les brindaba la oportunidad de mezclar las ganancias provenientes de los negocios del tráfico de alcohol y las actividades ilegales relacionadas con éste, con los ingresos obtenidos de las lavanderías a efecto de que pareciese que todos los ingresos provenían de éstas. De aquí, es de donde deriva el título de “Lavado de Dinero” o “Blanqueamiento de capitales”, que tanto la doctrina como diversos organismos internacionales se han dado a la tarea de definir esta práctica de manera clara[134].

Dentro de los diversos conceptos propuestos se presenta el siguiente:

> *“El lavado de dinero es el proceso mediante el cual se produce un cambio en la riqueza ilícitamente adquirida por bienes o activos financieros para darles la apariencia de que son de origen lícito; es el método de esconder y transformar el origen ilegal de los recursos. En otras palabras, son las actividades destinadas a conservar, transformar o movilizar recursos económicos en cualquiera de sus*

[134] Cfr. Córdova Gutiérrez, Alberto y Palencia Escalante, Carlos, El Lavado de Dinero: Distorsiones Económicas e Implicaciones Sociales, Instituto de Investigaciones Económicas y Sociales Lucas Alamán, A.C., México, 2001, pág. 3

formas y medios, cuando dicha riqueza ha tenido como origen el quebrantamiento de la ley[135].”

Por otra parte, el ACAMS (Asociación de Especialistas Certificados en Antilavado de Dinero) lo define de la siguiente manera:

“El lavado de dinero consiste en ocultar la fuente ilegal del producto de actividades delictivas con la expectativa de utilizarlo para realizar actividades legales e ilegales. Para decirlo de forma simple, el lavado de dinero es el proceso de hacer que el dinero sucio parezca limpio[136].”

El GAFI o FATF por sus siglas en inglés, es un organismo multinacional o intergubernamental creado en el año de 1989, por el grupo de los siete países industrializados (En aquel entonces conocido como el G-7) que tiene la finalidad de desarrollar acciones internacionales para prevenir y combatir el lavado de dinero. Este organismo da una perspectiva general del lavado de dinero en diversas actividades relacionadas con la delincuencia organizada, de la siguiente manera: “los delitos como la venta ilegal de armas, el tráfico de drogas, el contrabando, y otras actividades del crimen organizado, pueden producir grandes ganancias. El fraude, el abuso de información privilegiada, el soborno y las tretas de fraude electrónico también puede producir grandes ganancias creando un incentivo para ‘legitimar’ los fondos obtenidos ilícitamente con la práctica denominada lavado de dinero[137].”

También se ha señalado que el lavado de dinero debe manejarse desde dos nociones distintas, la general y la estricta. En el caso de la primera se alude genéricamente al proceso de legitimación de los bienes de procedencia ilegal, obtenidos al margen del control de administración tributaria; en cambio en su sentido estricto, lavado de bienes es referido exclusivamente al proceso de reconvención de bienes de origen delictivo.

---

[135] Gluyas, Millán Ricardo. “Inteligencia Financiera y Prevención de lavado de dinero”, *Iter Criminis, Revista de Ciencias Penales,* núm. 12, segunda época, México, INACIPE, México, 2005, pág. 59.
[136] Bryne, John J. y otros. Guía de Estudio para el Examen de Certificación CAMS, Quinta edición, Miami USA, 2011.
[137] Véase en: http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

"…el objetivo primordial del lavado de dinero es procesar las ganancias obtenidas de ganancias ilícitas, de manera tal que se transformen en lícitas, ya sea disfrazándolo, ocultándolo o mezclándolo de forma que se dificulte, evite u oculte su verdadera procedencia, a través de las diversas modalidades en las que se puede incurrir y que la propia legislación marca como tipos penales[138]."

Es por lo anterior que los ciberdelincuentes han encontrado diversas formas de poder disponer de los recursos sin ser descubiertos, además estos, tienen la intención de colocarlos en el sistema financiero aparentando con diversos medios que la mayoría de los ingresos obtenidos provienen de una fuente lícita, situación que les permite su uso, goce y disfrute. Esta práctica se traduce en una enorme afectación a la estabilidad económica del país, pues genera una falsa apreciación de la realidad económica adquisitiva, pues en el afán de convertir el dinero ilícito en lícito, se recurre a invertirlos en diversos tipos de activos que posteriormente vuelven a ser colocados en el mercado con una disminución importante en el valor normal, pues debido a la premura de obtener liquidez y de transformar los bienes patrimoniales en dinero justificable, éstos son enajenados en valores por debajo del mercado, lo que genera una competencia desleal dentro del comercio, que al final se traduce en cuestiones inflacionarias que desestabilizan y quebrantan al Sistema Financiero Mexicano.

Para el perfeccionamiento del lavado de dinero, existe un ciclo que deben de seguir los recursos de procedencia ilícita a efecto de que se materialice su legitimación, el cual consiste en tres etapas específicas. A la primera parte de este proceso se le conoce comúnmente como "introducción", que se refiere al proceso mediante el cual los sujetos activos del ilícito insertan de manera sistemática al sistema financiero los recursos provenientes de una actividad ilícita, esto usualmente se realiza mediante depósitos en efectivo fraccionados en diversas cuentas, o bien mediante la adquisición de diversos instrumentos financieros que sirven como medio de pago. Para el caso del Phishing existen diversas posibilidades que pueden seguirse en esta etapa, pues como se ha dicho a lo largo del presente trabajo de investigación, que una vez que han sido obteni-

[138] Gamboa Montejano, Claudia. "Lavado de Dinero" Estudio teórico conceptual, Derecho comparado, Tratados internacionales y de la nueva ley de la materia en México. Cámara de Diputados, Dirección de servicios de investigación, Subdirección de Análisis de Política Interior. Enero, 2013.

dos los recursos de manera ilícita, los “phishers” pueden disponer de éstos en formas distintas, que son realizadas en forma de transferencias, o bien por conducto de la adquisición de productos, bienes o servicios.

En caso de que el deseo del defraudador sea la disposición inmediata de los recursos, los ciberdelincuentes se valen de diversas herramientas para lograr su cometido, mediante la utilización de recursos tanto humanos como materiales, que derivan principalmente en la transferencia de los fondos. En el primero de los casos utilizan a un grupo de personas a los que se les conoce coloquialmente como “mulas”. Éstas tienen una única misión específica y deben de cumplir únicamente con un requisito sencillo que es el de proporcionar una cuenta activa en las que se le pueda realizar la transferencia de los recursos sustraídos de la cuenta del sujeto estafado, una vez transferidos, éstos deben de realizar el retiro del dinero y entregar o enviar por los medios previamente acordados la cantidad depositada menos una comisión por concepto de realización del servicio que se traduce en la ganancias de las llamadas “mulas”.

Por otro lado, existen maneras más elaboradas de realizar esta disposición de los recursos sin la necesidad de la utilización de terceros, pues con la recolección de la totalidad de los datos con el uso de esta técnica de ingeniería social, los estafadores pueden utilizarla para crear cuentas suplantadas en diversas instituciones financieras y disponer de los recursos de manera libre como si de ellos se tratara, lo que dificulta la identificación y detección de las transacciones involuntarias.

Para el caso de la obtención de bienes o servicios, éstos se venden en los diversos mercados comerciales sean lícitos a un precio muy por debajo de su costo normal, gracias a esto permite los delincuentes una obtención rápida de recursos que pueden destinar a otras actividades de su predilección.

Es importante hacer la precisión que en la mayoría de los casos donde se materializa el phishing las cifras obtenidas en un solo ataque no es suficiente para levantar sospecha alguna, pues los montos obtenidos, por lo común, suelen estar por debajo de los umbrales identificables, ya que normalmente los instrumentos de pago no poseen montos

de disponibilidad tan elevados, lo que representa un verdadero problema, pues se dificulta la prosecución de las miles de transacciones que se realizan en éstos y que en conjunto se traducen en pérdidas millonarias para las instituciones financieras.

El siguiente paso en el ciclo del lavado de dinero se le llama "ocultamiento", durante esta etapa se ha reunido una cantidad considerable de activos que se pretende invertir en fondos o colocarlos en múltiples cuentas alrededor del mundo. La finalidad del ocultamiento es la de realizar un sinfín de movimientos dentro del sistema financiero para intentar confundir a las autoridades de su origen, dichos movimientos regularmente son realizados dentro de aquellos países o jurisdicciones que tienen regímenes fiscales preferentes, o bien con aquellos que no se encuentran integrados a los acuerdos de cooperación para la prosecución de dichas prácticas. "La forma más común de disfrazar los movimientos es haciéndolos pasar por compras de bienes y servicios, que además les da una apariencia más legítima[139]."

Por último, se realiza el paso conocido como integración, que es la actividad con la que se pretende devolver los fondos al país de origen, es aquí cuando se ha perdido toda noción de su procedencia. Normalmente esto se realiza con la adquisición de bienes raíces, artículos de lujo o con la adquisición de acciones o negocios que permitan darles la apariencia legítima a los recursos procedentes de las actividades ilícitas.

Finalmente, es importante también precisar que el impacto que tienen este tipo de ilícitos afecta gravemente el desarrollo de los países, en especial de aquellos que tienen economías emergentes como lo es el caso de México, que aunque se ha trabajado de manera considerable en establecer un marco regulatorio tanto nacional como internacional, no se ha podido aplicar en su totalidad, además en aquellas jurisdicciones que no cuentan con instituciones financieras sólidas, que sus controles de acceso son nulos y su marco regulatorio es precario, propicia la vulnerabilidad de la estabilidad e integridad económica de estas. De manera paralela como causa colateral el flujo de capitales derivado de las inversiones que realizan otros países de manera directa o indirecta,

[139] Fernández Espejel, Gabriel. ¿Por qué legislar el combate al lavado de dinero? Acciones Frente al lavado de dinero. Centro de Estudios Sociales y de opinión Pública, México 2012. P.p. 19

provenientes de este tipo de ilícitos generan una alta volatilidad, al emigrar de un mercado a otro en el afán de intentar no ser detectados.

CAPITULO CUARTO.
AFECTACIÓN ECONÓMICA AL SISTEMA FINANCIERO MEXICANO COMO CONSECUENCIA DEL PHISHING.

El sistema financiero mexicano, siendo la base para el desarrollo y funcionamiento de la economía, requiere de medidas fuertes, específicas y especializadas que permitan su protección, pues existen diversas amenazas que ponen en riesgo de manera significativa su estabilidad. Es por esto, que existen esfuerzos conjuntos por parte de diversos organismos internacionales públicos y privados, dependencias gubernamentales a nivel interno como externo, así como de instituciones financieras convencionales y no convencionales a efecto de homologar los criterios y procedimientos que se deben de adoptar, con la finalidad de establecer mecanismos específicos efectivos que permitan proteger de manera integral la estabilidad de la economía global.

Las necesidades descritas en el párrafo anterior surgen a partir del flujo monetario que existe alrededor del mundo, pues con el crecimiento exponencial de los mercados, así como la oferta y demanda de productos, bienes y/o servicios que es cada día mayor, requiere de innovaciones, herramientas tecnológicas y medidas de distribución más eficientes, lo cual se describe como un proceso al cual se conoce de manera genérica como, globalización. A este proceso de interdependencia entre las partes que integran un todo en una red global de comunicación, ha sido posibilitada gracias a los enormes avances tecnológicos y a la cooperación de diversos entes que en su momento han tenido la necesidad, o bien el compromiso, de llevar empresas a un nivel más grande y estructurado. Estos avances si bien han permitido realizar procesos por demás complejos de manera más rápida y eficiente, también han abierto la puerta a realizar actividades que van en contra de las buenas intenciones con las que han sido creadas, ejemplo de esto lo encontramos con el Internet.

Si bien la red mundial denominada internet ha obsequiado un sinfín de ventajas y comodidades como herramienta tecnológica de comunicación para diversos fines como lo son: las comerciales, financieras, académicas, informativas, recreativas, entre otras.

También ha otorgado una serie de concesiones para aquellos que se dedican a realizar actividades mal intencionadas que ponen en grave riesgo la seguridad, el patrimonio, salud y hasta libertad de las personas que se encuentran en cierto grado de vulnerabilidad, acciones que tienen la tendencia de traducirse en un impacto económico, actividades que al ser ilícitas, repercuten gravemente en la estabilidad de las economías de los países, con un efecto en cadena que afectan de manera indirecta a la estabilidad global, siendo a través del sistema financiero el mecanismo primario utilizado como mecanismo de pagos y distribución de las riquezas.

El capítulo final del presente trabajo de investigación, tiene la pretensión de demostrar como una actividad, tal como el phishing, puede afectar de manera importante al sistema financiero mexicano, en una escala piramidal entre usuarios o clientes de los intermediarios financieros, a las mismas entidades de carácter financiero, a los órganos supervisores y reguladores del gobierno federal y finalmente con un impacto en la estabilidad económica global, si no se presta la debida atención a la proliferación de este tipo de actividades, mediante la creación y aplicación de mecanismos y procedimientos conjuntos, que permitan conocer, prevenir, regular y aplicar medidas coercitivas en caso de su materialización, se tendrán consecuencias como la disminución en el crecimiento económico sostenido y por ende un decremento en el bienestar de la población.

4.1.- REPERCUSIONES ECONÓMICAS DEL PHISHING.

En general, el incremento y la proliferación de ilícitos cometidos en la red, se ha convertido en una herramienta de fácil acceso que permite a los denominados ciberdelincuentes, una serie de prerrogativas tales como mantenerse en el anonimato, actuar de manera remota, dificultar la prosecución de las actividades que desarrollan, entre otras. Situación que genera un gran déficit en la estabilidad de la economía global, pues se estima que a nivel mundial, las pérdidas derivadas de este tipo de crímenes superan los 600 mil millones de dólares anuales[140], situación que es por demás alarmante, pues también existen estimaciones de empresas y consultoras especializadas en temas de

[140] Según datos referidos en un artículo del diario “Excélsior” consultado en la red con fecha 27 de febrero de 2017, disponible en la siguiente liga: http://www.excelsior.com.mx/nacional/2017/02/27/1148915

ciber seguridad, que este tipo de comportamientos se encuentran en un aumento exponencial, pues en el transcurso de los últimos tres años, la cantidad de delitos cometidos por este medio se ha triplicado hasta llegar a la cifra que conocemos hoy en día y seguirá en aumento, pues a medida que crecen las posibilidades del desarrollo de infraestructura que permitan suministrar a más personas acceso a internet a bajos costos, la cantidad de usuarios por ende, se incrementará, por lo que el campo de acción y de afectación a víctimas potenciales también irá en aumento.

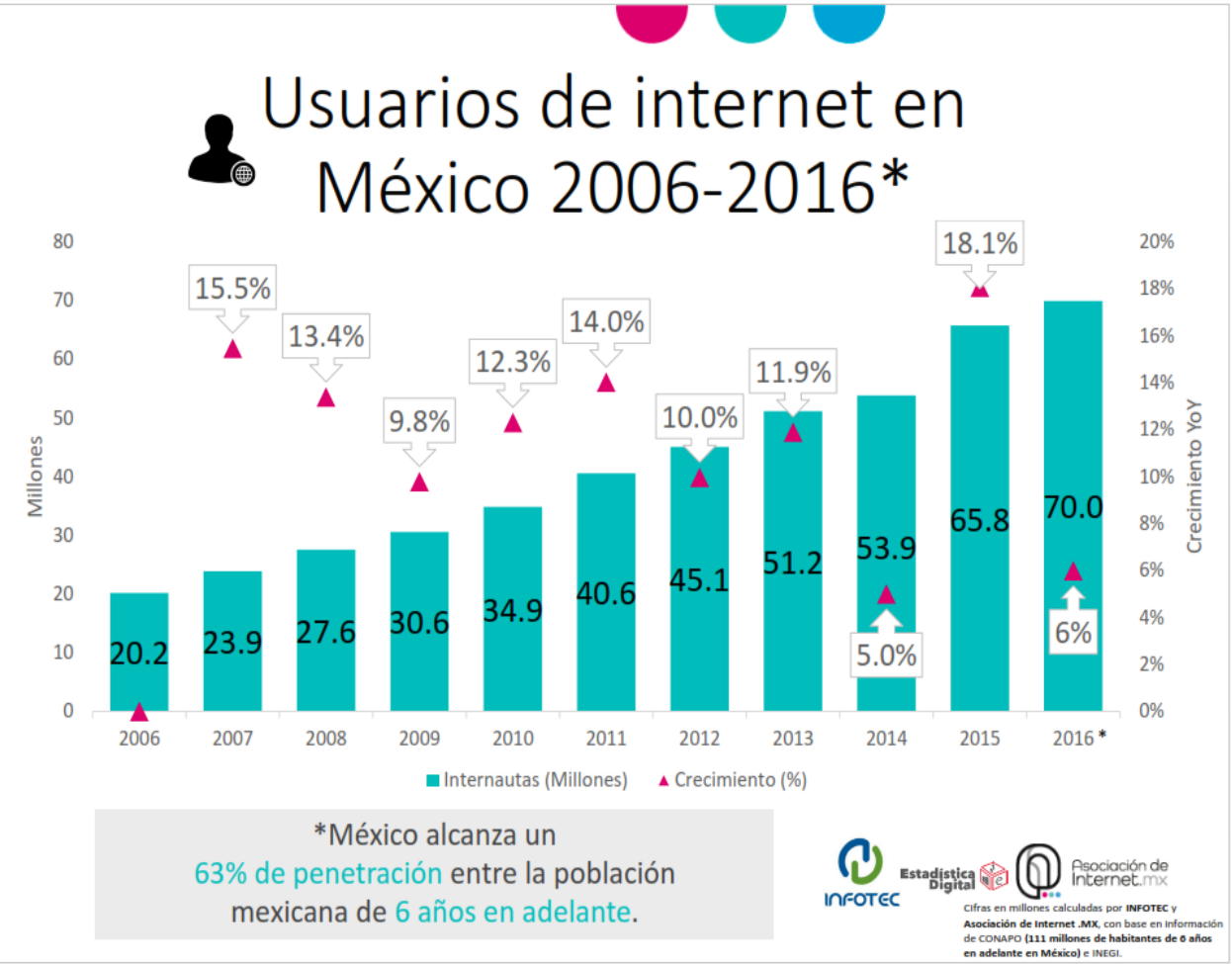
Lo anterior se traduce en una afectación patrimonial a la sociedad y por ende a la estabilidad económica que no debe limitarse solo de los territorios que albergan a las víctimas de este tipo de ilícitos, sino que, al ser un medio de comunicación global, puede afectar de manera directa la estabilidad de otros países, inclusive de regiones de gran extensión territorial, pues los ataques pueden ser perpetrados desde cualquier parte del mundo, la movilidad de los recursos obtenidos de manera no consentida se facilita enormemente gracias a las plataformas digitales que han desarrollado las instituciones financieras a efecto de mejorar y agilizar el sistema de pagos. Así mismo, las personas que se dedican a este tipo de prácticas tienen la preferencia de desarrollar los ataques cibernéticos en países o territorios poco desarrollados que tienen poca o nula regulación que permita su debida atención, prevención e investigación, pues no existe medio alguno por el cual puedan quedar al descubierto y ser sancionados.

En el caso específico de México, los datos no son por menos alarmantes, pues según informes de la unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República, expresaron que los delitos bancarios cuestan aproximadamente 3 mil millones de dólares al año, ubicando a México en el lugar número 17 del mundo en pérdidas económicas por estos crímenes[141], dentro de los cuales los principales se refieren a el robo de identidad, los fraudes, la extorsión y la pornografía infantil.

Para ponerlo en una mejor perspectiva sobre la evolución que han tenido este tipo de prácticas, hasta finales de diciembre de 2016, según datos del INEGI y de la Asocia-

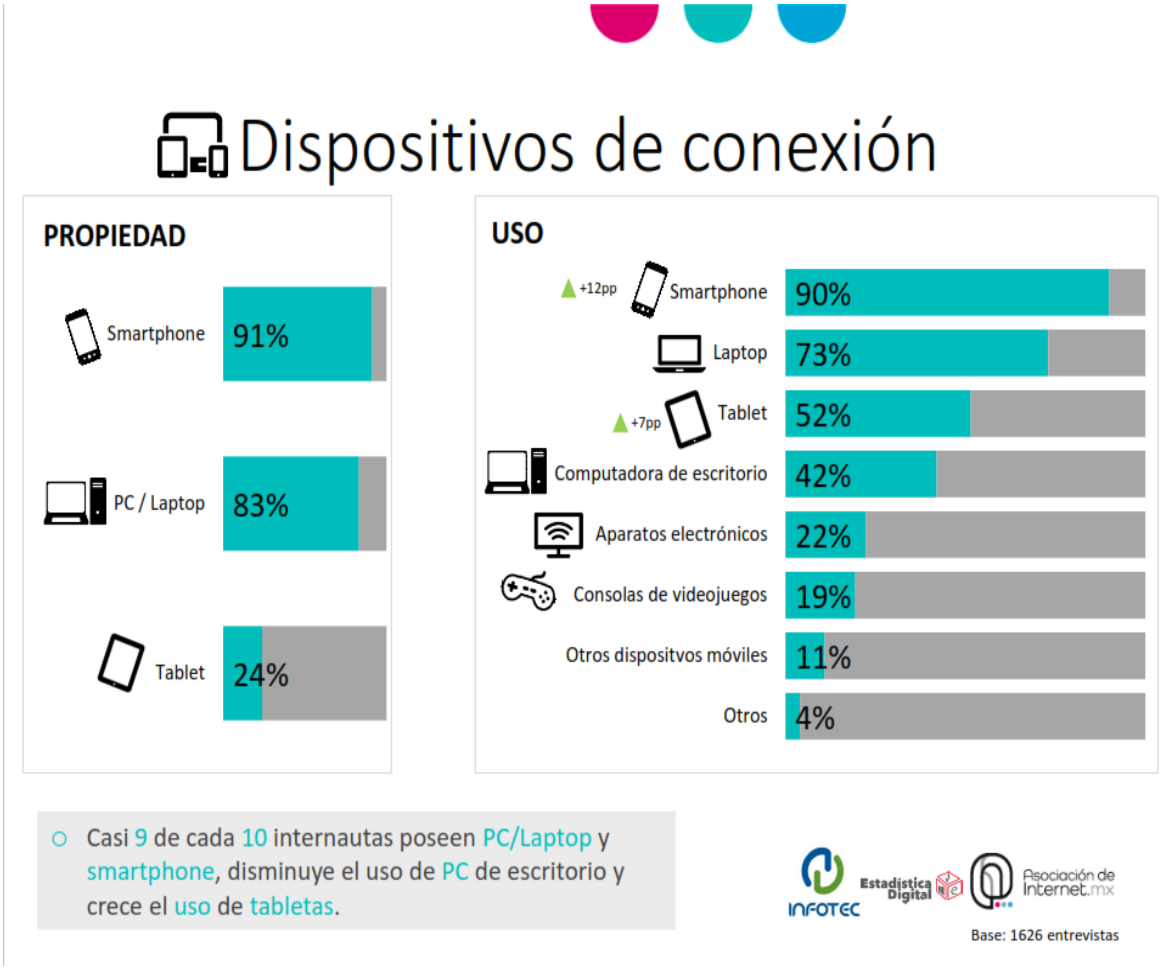
[141] Ibídem.

ción Mexicana de internet[142], alrededor del 60 por ciento de la población posee de alguna herramienta tecnológica que le permite el acceso a internet.



De las diversas herramientas tecnológicas que permiten el acceso a la red, encabezan la lista los siguientes dispositivos tales como: Smartphone, computadoras portátiles o de escritorio, tabletas electrónicas, consolas de videojuegos, electrodomésticos, entre otros.

[142] Los datos duros y los gráficos utilizados en el presente capítulo han sido descargados del sitio web de la Asociación Mexicana de Internet, con información del INEGI actualizada a 2016, los cuales pueden consultarse en la siguiente liga: https://www.asociaciondeinternet.mx/es/

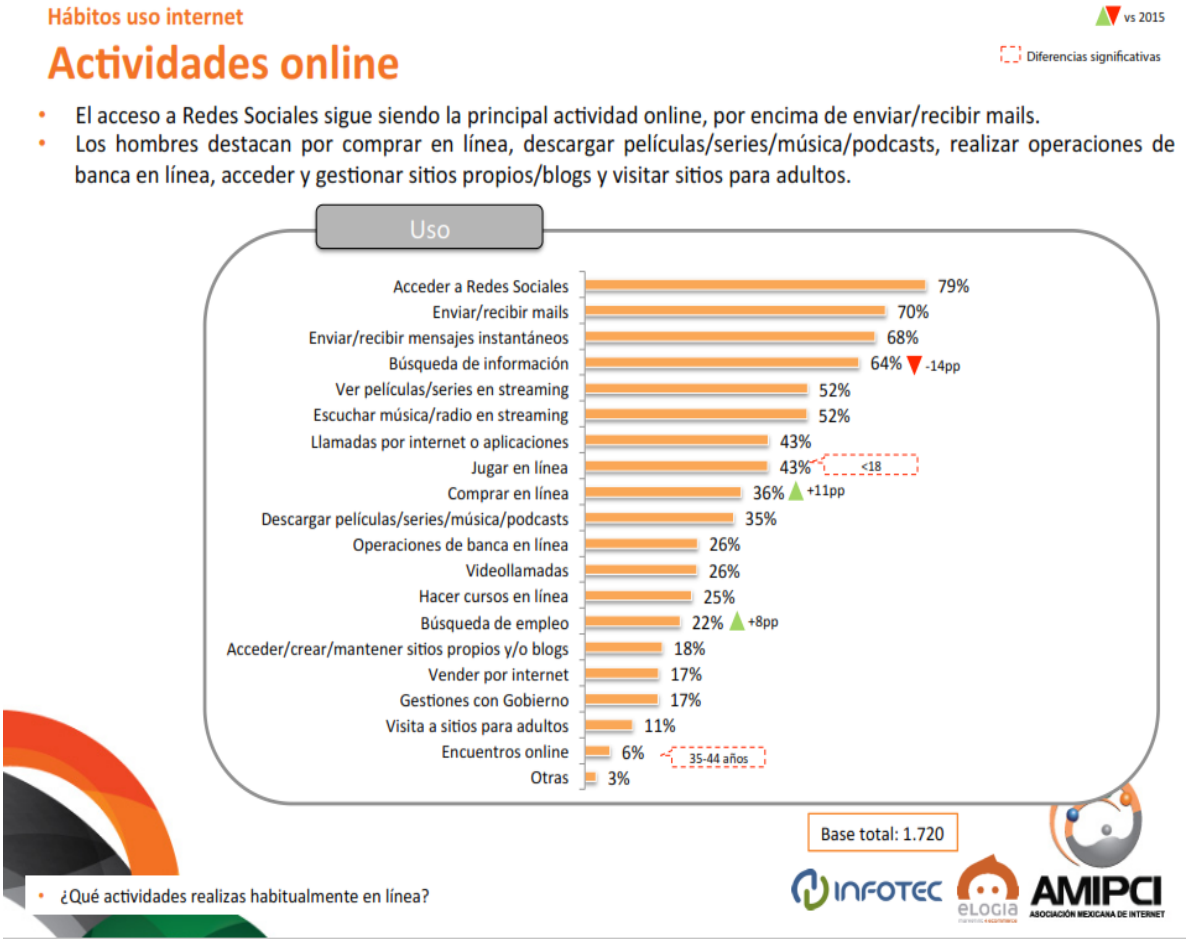


Dichos medios son utilizados para diversas actividades dentro de las que destacan: el acceso a redes sociales, envío y recepción de e-mails, utilización de servicios de mensajería instantánea, búsqueda de información, ocio y entretenimiento, operaciones de banca en línea, compra y venta de productos y servicios entre otras, situación que ha cambiado por demás el comportamiento de la sociedad gracias a las facilidades y beneficios que nos otorga esta valiosa herramienta.

El envío y recepción de emails son de las actividades que más realizan los usuarios activos en internet con un 78%, que es el medio por el cual se propagan este tipo de ataques en los que se envían mensajes a los usuarios en los que se indica por medio de un artífice que existe un problema con las cuentas bancarias de los clientes y que, para salvaguardar la integridad de los recursos, es necesario la actualización de los datos personales. En el mensaje se solicita al usuario que siga una liga y que proporcione

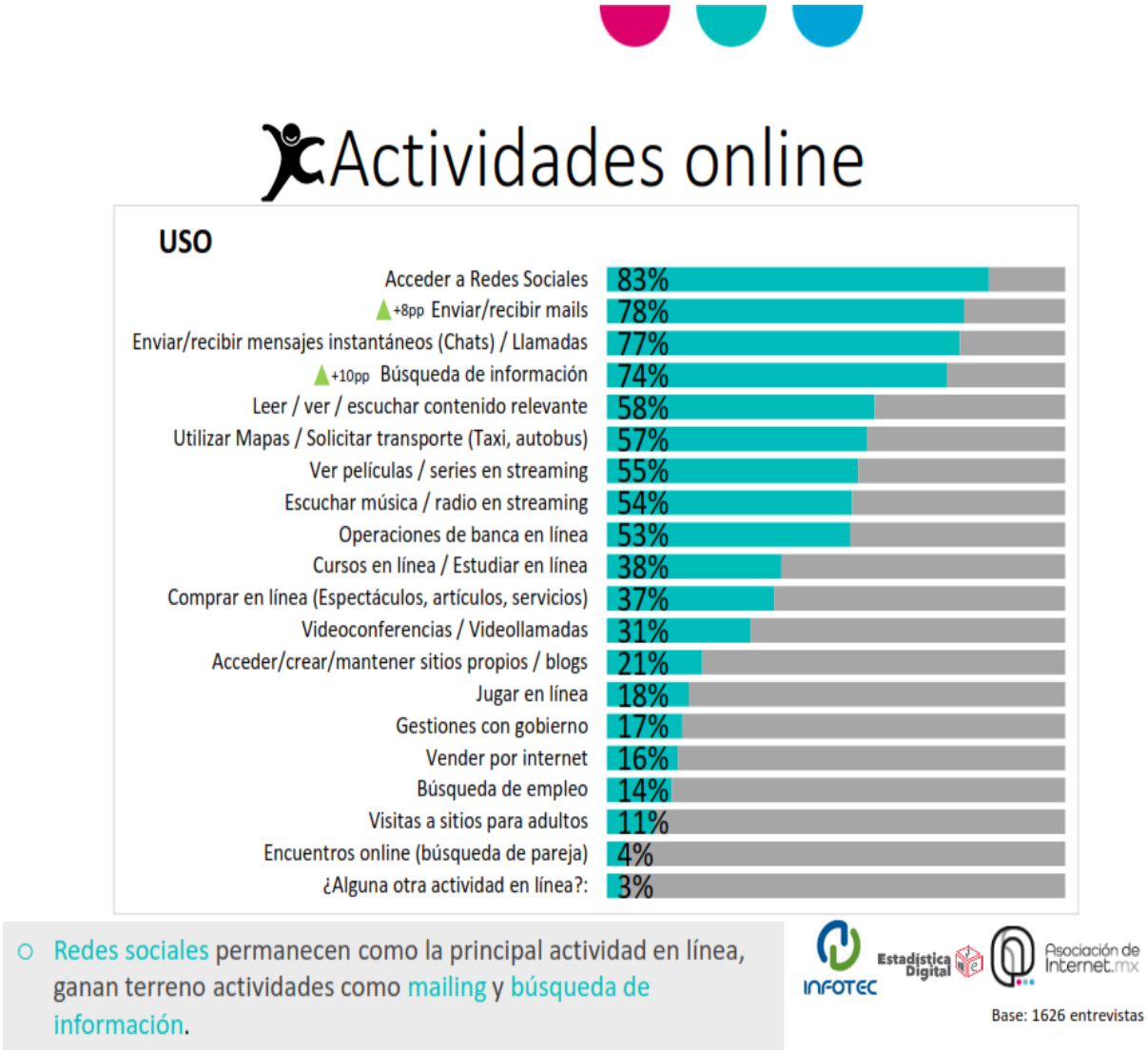
sus datos tales como usuario y contraseña, que al ser ingresados pueden ser utilizados libremente por aquel o aquellos que lanzaron el ataque para alguno de los diversos fines que hemos planteado.

Como se puede apreciar en los gráficos, en el 2015, un porcentaje considerable de la población, correspondientes al 36% y al 26% respectivamente, utiliza el servicio de internet para comprar en línea, o bien, realizar sus operaciones de banca mediante la infraestructura electrónica de las instituciones financieras.



En el 2016, existe un incremente bastante considerable respecto a las operaciones de banca en línea, pues comparado con el del año anterior aumentó del 36% a 53%, situación que permita hacer visible que las personas van generando más confianza en la utilización de dichos servicios, lo que representa una probabilidad más alta de que se

susciten en mayor medida la materialización de los riegos, como lo son ataques de phishing.



En el caso de las compras en línea, se necesita en la mayoría de los casos contar con un instrumento de pago que pueda ser validado y respaldado por una institución de carácter financiero. Por otra parte, en el caso de los servicios de banca electrónica es necesario proporcionar cierta información a efecto de poder consultar o realizar movimientos tales como depósitos, disposiciones, transferencias o retiros, la cual es protegida con la implementación de usuarios y contraseñas para mantener su confidencialidad y buen uso, que como se ha expuesto a lo largo de este trabajo de investigación es el

objetivo de aquellos que dedican sus esfuerzos a crear los ataques cibernéticos a los cuales conocemos ahora como “phishing”.

4.2.- AFECTACIÓN A TARJETAHABIENTES O CUENTAHABIENTES.

En México ha existido una evolución importante respecto al manejo en las finanzas de las personas, pues se han adoptado nuevas costumbres que han permitido que las transacciones monetarias se realicen de manera más rápida, cómoda y segura. Los avances tecnológicos y las necesidades del nuevo estilo de vida, ofrecen una gran variedad de servicios e instrumentos convencionales o tecnológicos mediante los cuales se ha transformado por completo el sistema de pagos monetarios a como lo concebíamos hace poco más de 60 años, cuando comenzaron a surgir diversos mecanismos como por ejemplo las tarjetas de crédito, las cuales han sido adoptadas por el comercio electrónico, pues al ser un instrumento el cual ha sufrido diversas variaciones en cuanto a seguridad y portabilidad, se han convertido en el medio de pago adecuado para dicho comercio.

Sin embargo, a pesar de los diversos estándares de seguridad que manejan las instituciones financieras y las diversas modificaciones que se la han realizado a los plásticos a efecto de evitar fraudes como la clonación de tarjetas, aún se cuenta con el error humano que ha permitido a diversas personas aprovecharse de la ingenuidad y del desconocimiento de lo sensible que puede llegar a ser el mal uso de los datos de carácter personal, más de aquellos que sirven como medio de protección para el resguardo de dinero, tales como usuarios y contraseñas.

La finalidad del presente trabajo de investigación es la de generar conciencia de los grandes estragos y del cambio en el cuidado y manejo de los recursos personales que han surgido debido a la implementación de nuevas tecnologías en la manera de actuar de las sociedades. La facilidad que nos otorgan las tarjetas de crédito y débito para la adquisición de bienes, productos o servicios, también representan un riesgo inminente que es necesario tener presente a efecto de crear mecanismos que permitan hacer ca-

da día más seguras las transacciones que se realicen con auxilio de los diversos instrumentos tecnológicos de carácter financiero.

El phishing es uno de estos riesgos que sin duda debe de ser atacado, pues en la actualidad, representa una de las más grandes pérdidas y afectaciones al sistema financiero, no solo de México (que es el segundo país en América Latina que más recibe ataques cibernéticos, únicamente después de Brasil[143]), si no que sus estragos son de carácter global, sin embargo, quienes reciben en un principio la afectación directa, son los titulares de alguna cuenta bancaria en la que puedan disponer de ciertos recursos monetarios que son respaldados por una entidad financiera, quienes son el primer eslabón para la ejecución de este tipo de ataques, que han recibido en más de una ocasión correos electrónicos apócrifos, con mensajes amenazantes o alarmantes, en los que se pretende robar la información sensible, mediante engaños.

Una vez materializado el engaño, el uso de dicha información sensible, supone una pérdida económica directa para el afectado, con este tipo de datos es muy fácil y recurrente realizar una serie de transferencias de fondos en plataformas de banca electrónica o móvil o bien, la adquisición de diversos bienes o servicios a través de las plataformas de comercio electrónico que podemos encontrar en la red, que pueden dejar en minutos vacías las cuentas que han sido suplantadas.

En el caso de que el robo de los datos personales sean propios de alguna tarjeta de débito o cuenta de ahorro, en las que los recursos son propios del cuentahabiente, se puede suponer una pérdida inmediata del esfuerzo del trabajo o bien de muchos años de administración y ahorro, ya que normalmente los titulares de dichas cuentas, prefieren dejar el dinero en sus cuentas como medida de seguridad, para no extraviarlo, o no cargar con grandes cantidades de dinero en efectivo y ser víctimas de los enormes índices delictivos que se sufren a lo largo del país. Así mismo, otra de las características de las tarjetas de débito es que, al ser instrumentos de pago mucho más básicos, nor-

[143] Cfr. http://www.eltiempo.com/tecnosfera/paises-latinoamericanos-en-ciberseguridad-129604 (Consultado 15/09/2017)

malmente las protecciones que otorga el banco son muy limitadas, tienen costos excesivos o son nulas.

En el caso de las tarjetas de crédito, la situación aún es un poco más sensible, como bien lo dice el nombre, con estos instrumentos las instituciones financieras otorgan una línea de crédito a sus tenedores para su uso y disfrute, lo cual conlleva una obligación directa de todas las transacciones que se realicen con ésta, se presumirá que han sido realizadas por el titular de dicho instrumento. Por otro lado, las líneas de crédito en su gran mayoría rebasan la capacidad real de pago de sus clientes y en caso de que dichos recursos sean sustraídos en su totalidad, los tenedores de las tarjetas de crédito serán los responsables de cubrir con dichas obligaciones, lo cual representa un menoscabo considerable a las finanzas de las finanzas de las familias mexicanas y un golpe grave a su estabilidad emocional.

Por otro lado, algunas de estas tarjetas que tienen el carácter de preferentes, mantienen activos algunas medidas de protección al usuario, como blindajes o seguros de protección y de seguimiento transaccional más estricto que permiten detectar a tiempo los movimientos realizados con dichos instrumentos, sin embargo, estos no son suficientes.

En ambos casos la afectación patrimonial se ha materializado, dejando en estado de insolvencia a los tarjetahabientes y con la incertidumbre de no saber qué es lo que ha ocurrido con su dinero y con la predisposición de tener que iniciar una serie de averiguaciones con el banco, trámites administrativos y hasta procedimientos de carácter judicial, que por supuesto implican un esfuerzo considerable, tiempo, paciencia y por supuesto más dinero para llevarlos a cabo, que no siempre resultan favorables para el cuentahabiente, pues así como éste intenta alegar la nula disposición de los fondos y que han sido suplantados sus datos personales y posteriormente utilizados en su nombre y representación, las instituciones financieras harán lo propio para no asumir el cargo respectivo por los montos consecuencia de estos artificios de ingeniería social, lo que requerirá de defensas mejor elaboradas, derivadas del conocimiento y experiencia, sin dejar de lado la capacidad económica de las partes

A su vez, el Estado cuenta con diversos mecanismos de protección a los usuarios que han sido de gran ayuda para resolver este tipo de controversias de manera conciliatoria, entre los clientes y la institución, sin necesidad de activar los mecanismos jurisdiccionales, sin embargo, no son suficientes, pues este tipo de actividades no debería de suceder y mucho menos seguir creciendo de la manera tan exorbitante en la que se ha podido apreciar en los últimos años. El principal aliado de este tipo de estafas es el desconocimiento por parte de los usuarios, derivado de la falta de información y de la puesta en marcha de programas que ayuden a mitigar este tipo de prácticas, así como la indiferencia en el buen cuidado de las finanzas personales.

4.3.- AFECTACIÓN A LAS INSTITUCIONES FINANCIERAS.

Los intermediarios financieros como también los conocemos, son las organizaciones empresariales que tienen la finalidad de ofrecer distintos servicios financieros a sus clientes, éstas principalmente, tienen como principal fin la acumulación de capitales y su transferencia por medio de préstamos con una tasa de interés previamente pactada, o bien para su inversión directa, servicios que se encuentran estrictamente regulados por el gobierno por conducto de diversos organismos que se encargan de procurar la estabilidad del sistema financiero Mexicano.

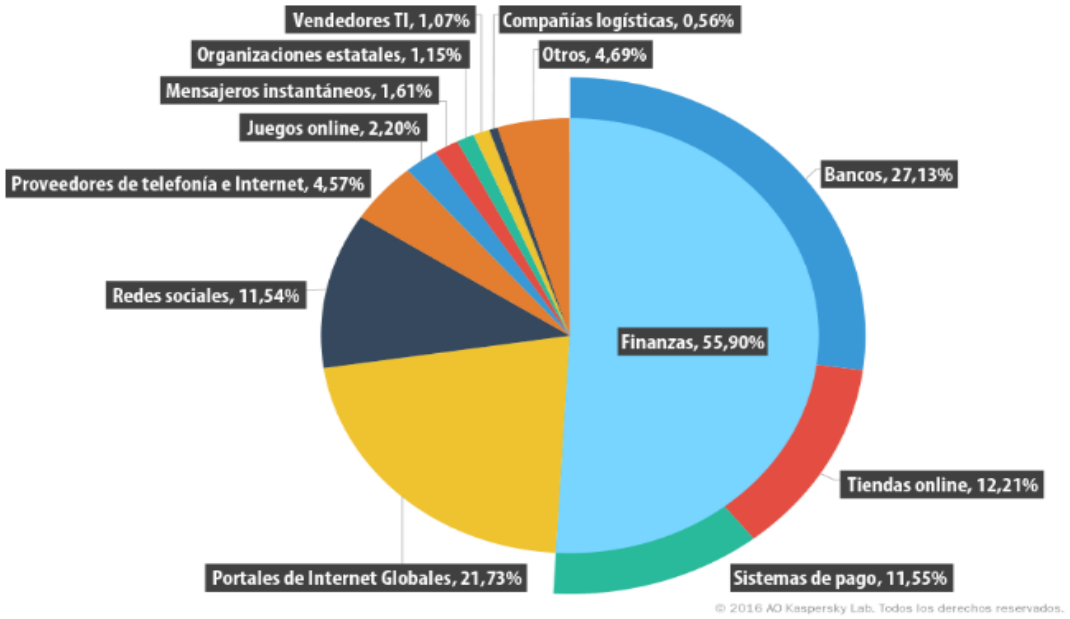
Existen diversos tipos de instituciones financieras dentro de las cuales encontramos a las instituciones de depósito, contractuales, de inversión y que las que únicamente ofrecen servicios como préstamos, pero no pude ofrecer depósitos a clientes. Sin duda, las más comunes son las instituciones bancarias que basan su funcionamiento y operaciones en la captación de ahorro y otorgamiento de créditos, tal como se hablaba en al capítulo precedente, las instituciones bancarias utilizan diversos instrumentos de pago mediante los cuales pueden llevar a cabo sus principales actividades ofreciendo diversos servicios de ahorro y préstamos a personas físicas y jurídicas, tales como cuentas de ahorro y líneas de crédito.

Sin duda, las instituciones financieras sufren una gran afectación derivada de los múltiples delitos que son cometidos con el uso de una plataforma digital, dichas afectaciones se traducen principalmente en pérdidas económicas multimillonarias derivadas de los grandes egresos que se tienen que sufragar por cuenta de gastos operacionales, implementación de tecnología, resarcimiento de daños, controversias jurisdiccionales, afectación a su nombre y buena reputación, entre otros.

Existen diversas empresas privadas y organizaciones no gubernamentales que se han dado a la tarea de recabar información relativa al comportamiento de los fraudes perpetrado en la red, algunos de estos estudios incluyen al phishing como una de las prácticas más utilizadas y con mayores frutos dentro del tipo de estafas cometidas a través de medios electrónicos. Estas empresas se valen de diversos mecanismos y plataformas que han diseñado a efecto de proteger a sus usuarios de este tipo de atraques, así mismo tienen la finalidad de recabar datos estadísticos respecto del comportamiento de este tipo de fenómenos en la red.

En un reporte trimestral que ha presentado la empresa de ciberseguridad “Kaspersky labs”, en su sitio web, se menciona que el porcentaje de los usuarios que han sido o han recibido este tipo de ataques durante el tercer trimestre del 2016, son aquellos relacionados con las entidades financieras, es decir, bancos, sistemas de pago, tiendas en línea, entre otras, pues este tipo de ataques representó más del cincuenta por ciento del total registrado en el periodo aludido, Señalando que por trimestre aproximadamente los ataques realizados a bancos aumentaron un 1.7%. ascendiendo a 27.13%; la categoría de “compras en línea” en un 2,82%, llegando al 12.21%; y referente al sistema de pago aumento en un 0.31%. quedando en 11.55%, para lo cual nos presentan la siguiente gráfica[144]:

[144] Información del tercer trimestre de 2016, obtenida de la siguiente página web: https://securelist.lat/analysis/informes-trimestrales-sobre-spam/84261/spam-and-phishing-in-q3-2016/



Distribución de las organizaciones atacadas por los phishers por categorías, tercer trimestre de 2016

En el caso específico del phishing la afectación comienza desde que los ciberdelincuentes tienen la pretensión de engañar a sus clientes haciéndose pasar por aquellas sociedades de gran renombre, suplantando los logos y páginas web para enviar una serie de mensajes intimidades en su nombre, con los que se pretende obtener diversa información sensible. Dichos actos, generan que las instituciones tengan que buscar implementar mecanismos eficientes de manera progresiva a fin de integrar elementos distintivos en sus sitios digitales para que su reproducción se dificulte, así mismo dar a conocer a sus usuarios de dichos cambios lo cual implica un que los esfuerzos monetarios sean bastante elevados, además los delincuentes trabajan día y noche a efecto de burlar las medidas de seguridad implementadas por los principales atacados, a efecto de hacer creer al usuario de que la página que se encuentra visitando es la legítima, lo que se traduce en una lucha constante por mantener el control.

De lo expuesto en el párrafo anterior, puede entenderse que una vez que logran el cometido de engañar a los usuarios y de esta manera obtener la información privada, el siguiente paso será el de utilizar dichos datos para la obtención de un beneficio económico, que al materializarse se verá reflejado en el decremento de las cuentas de los clientes que mantienen derivadas de una relación contractual con las instituciones fi-

nancieras, al darse cuenta de lo sucedido recurrirán a realizar las aclaraciones pertinentes con las instituciones que resguardan los fondos. En el caso específico de México se iniciará el procedimiento que indica el artículo 23°[145] de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, lo que implica que la institución financiera deberá de reembolsar la cantidad objetada en un periodo de tiempo que no podrá sobrepasar los cuatro días hábiles.

Lo anterior implica un estrago económico para las instituciones, pues deben de cubrir el monto por partida doble, pues por una parte, ya se pagó o transfirió a un tercero de manera no consentida una cierta cantidad y por el otro, deben de restituir casi de manera inmediata la cantidad objetada al usuario que ha recibido la afectación, insumos de los cuales no podrán disponer dichas instituciones hasta que no se determine mediante una investigación la procedencia o improcedencia de la reclamación, que si bien se coloca en perspectiva, las reclamaciones diarias realizadas por los clientes a este respecto, refleja que las instituciones ven mermado la disposición total de capital. Tan solo en 2016, el total de las reclamaciones relacionadas con fraudes imputables a un presunto fraude hacia los clientes de la banca según datos de la Condusef ascendió a 3 mil 72 millones 264 mil 732 pesos[146], considerando lo anteriormente dicho, la cifra se podría duplicar al tener que cubrir la afectación económica que ha sufrido el cliente, en tanto no se resuelva la investigación.

Este tipo de procedimientos también suponen una afectación económica adicional para las entidades, pues se requiere un equipo de trabajo integrado por investigadores, asistentes de atención telefónica, personal con conocimientos jurídicos, negociadores, desarrolladores de tecnología, entre otros, que permitan llevar a cabo la debida atención de los reclamos, a fin de evitar una posible controversia jurídica que por ende se verá reflejado en un gasto mayor derivado de la activación de los mecanismos jurisdiccionales que son demasiado costosos para ambas partes, por lo que siempre es conveniente llegar a un acuerdo conciliatorio en este tipo de situaciones, cuando se cuente

[145] Op, cit.: http://www.diputados.gob.mx/LeyesBiblio/pdf/LTOSF.pdf
[146] Información obtenida del Diario el Financiero con fecha 7 de julio de 2016: http://www.elfinanciero.com.mx/economia/aumentan-en-60-reclamos-por-fraudes-en-tarjetas.html

con los elementos suficientes para determinar que se ha sido víctima de un ilícito por conducto de los diversos medios tecnológicos.

Así mismo, los entes financieros tienen que dedicar una suma fuerte de dinero, en campañas publicitarias que auxilien en la prevención y conocimiento de los usuarios de este tipo de prácticas, las cuales tienen la finalidad de crear conciencia en la sociedad, para que no sea víctima de este tipo de fraudes. También se realizan erogaciones de importancia en el desarrollo de tecnología, de consultores y desarrolladores web, que permitan un uso más seguro de la red, así como detección oportuna de este tipo de ataques mediante programas y software antiphishing.

Las pérdidas económicas sufridas por las instituciones financieras afectan de manera importante la estabilidad del sistema financiero, por lo que el Estado debe de intervenir mediante la implementación de mecanismos que permitan que siga fluyendo su sano desarrollo, mediante la planeación de estrategias conjuntas que permitan mitigar los riesgos derivados de este tipo de prácticas.

4.4.- AFECTACIÓN ECONÓMICA AL ESTADO.

El estado ha desarrollado una estructura por demás compleja a efecto de procurar la estabilidad del sistema financiero mexicano, la cual se encuentra regulada por medio del Ejecutivo Federal por medio de la Secretaría de Hacienda y Crédito Público, que de manera directa o indirecta se encarga de velar por brindar la protección necesaria mediante las diversas comisiones creadas para este fin (Comisión Nacional Bancaria y de Valores, Comisión Nacional de Seguros y Fianzas, Comisión Nacional del Sistema de Ahorros para el Retiro) y el Banco Central (Banco de México). El estudio de la integración y funcionamiento del sistema financiero de manera complementaria en este trabajo, alejaría la idea del tema central debido a su complejidad operacional, por lo que únicamente se estudiará lo relacionado con nuestro tema de estudio, que es el estrechamente relacionado con el sistema bancario, los sistemas de pagos y aquellas actividades complementarias (o actividades paralelas) que utilizan o pueden utilizar medios

electrónicos como instrumentos monetarios y que pueden ser objetivos primordiales del phishing.

En el punto precedente se expusieron una serie de datos duros en los cuales se aprecian las diversas afectaciones económicas sufridas por las instituciones financieras, por las diversas prácticas cometidas en los medios electrónicos, sin embargo, la afectación se subsume a un tercer eslabón en el cual tenemos al Estado, que al ser el organismo rector de la procuración en la estabilidad del sistema financiero, pues al existir ciertas problemáticas relacionadas con éste, es éste quien debe asumir la implementación de las guías y propuestas de mejores prácticas que auxilien en el mejor desarrollo, impulsando actividades complementarias, así como en su caso aplicar los mecanismos monetarios suficientes de salvaguarda y protección, con la finalidad de que la economía sufra un menoscabo en su haber derivado de afectaciones inflacionarias, que debilitan la estructura de las finanzas mexicanas.

En el punto 3.3 de éste trabajo de investigación, se explicó que las entidades financieras y no financieras utilizan diversos mecanismos de protección a sus haberes como es el caso de los seguros y de los reaseguros, en otros casos utilizan las amortizaciones de deudas incobrables y ceden sus pasivos a carteras de cobranza, a efecto de recuperar algo de lo que ya se consideraba como totalmente perdido, dejando el esfuerzo de recuperación a otro tipo de empresas, sin embargo estas prácticas no son siempre posibles, debido a que las deudas o las perdidas contraídas por deudas incobrables o por ilícitos tales como el phishing y otras actividades, son muy difíciles de rastrear y recuperar, es por ello que existen otros mecanismos que en coordinación con las leyes fiscales, las instituciones pueden aplicar una serie de deducciones permitidas por las diversas regulaciones que se aplican a efecto de salvaguardar la estabilidad de dichas instituciones, pues estos recursos, son necesarios a efecto de poder seguir prestando los servicios profesionales operacionales a que se encuentran abocados.

Es por ello, que dentro de los mecanismos operacionales las entidades desarrollan estrategias contables específicas en sus estados de cuenta en las que de manera constante aparecerá un rubro denominado: “cuentas por cobrar”. Supuestos que devienen

principalmente de la prestación de servicios; enajenación de bienes; otorgamiento del uso o goce temporal de bienes, o en su caso del saldo insoluto de capitales otorgados en préstamo. En el caso específico del phishing al ser los recursos derivados de un contrato de crédito, se puede entender a grosso modo que este capital ha sido utilizado con tal finalidad, no obstante, la realidad es que la identidad del contratante ha sido suplantada y los recursos han sido transferidos para otros fines, considerado para tales efectos como un fraude, lo cual se traduce en una obligación de saldo insoluto, que dentro del momento en que se ha ejecutado la acción, queda a la deriva por no poder satisfacer de manera habitual la obligación.

Para esto, en términos generales los créditos otorgados a clientes se clasifican dependiendo de su disponibilidad, diseminándolas en cuentas por cobrar a corto, largo y mediano plazo, dentro que deberán de considerarse los intereses devengados, normales y moratorios, así como los costos y gastos incurrimos reembolsables, que deriven de las operaciones que dieron origen a las cuentas por cobrar, deben considerarse como parte de las mismas, por lo tanto, dichas reservas de cuentas incobrables se determinarán sobre el importe total de dichos conceptos. A efecto de que éstas se puedan considerar como carteras deducibles de crédito, se deben de cubrir ciertos requisitos que varían dependiendo de las cuentas por cobrar.[147]

Es así que el Estado otorga ciertas prerrogativas y cargas a las entidades que formas parte del Sistema Financiero, establecidas en diversas circulares emitidas por la Comisión Nacional Bancaria y de Valores, dentro de las cuales se deben de mantener como parte obligatoria, una reserva preventiva por riesgos crediticios, a efecto de que éstos sean menores y se pueda mantener una proyección estimada de los activos o pasivos a manejar, cuyo objetivo es determinar el porcentaje del crédito que será reconocido en los resultados de la entidad en forma anticipada.

Realizados lo cálculos anteriores, en término tributarios las deudas incobrables pueden ser susceptibles de aplicar deducciones por dos diversos supuestos, cuando se presenta la prescripción, o bien cuando existe una imposibilidad práctica de cobro, estas de-

[147] Cfr. http://www.eyboletin.com.mx/eysite2/pdf/comentarios_1617.pdf (Consultado 15/09/2017)

ducciones principalmente son aplicadas en tasas tributarias como a la relativa al impuesto sobre la renta (ISR), ya que es con éste que se puede compensar las erogaciones que se han realizado para la subsistencia de la empresa, los que quiere decir que el Estado es quien absorberá en parte importante aquellas deudas que se generen al realizar este tipo de prácticas, pues si no fuese de este modo, el capital de las instituciones financieras se vería gravemente mermado y no podrían continuar con la liquidez que les permite seguir llevando a cabo sus actividades de manera profesional.

Otra de las causas específicas del phishing, aunque en obviedad de repeticiones, es preciso dejar claro que es un proceso mecanizado, que utiliza diversos medios y estratificaciones complejas a efecto de que los ciberdelincuentes puedan aprovechar de manera final el producto del delito, llevándolo de un sitio a otro a efecto de que los recursos obtenidos sean difícilmente rastreables hasta sacarlos por completo del sistema financiero, esas pérdidas millonarias, repercuten directamente a la salud de las finanzas de los Estados a nivel global, acciones que de no tomar las medidas oportunas adecuadas, podrían desencadenar en graves crisis económicas que producirían a corto y mediano plazo hambruna y guerras, todo esto desencadenado de la sensibilidad y volatilidad de las economías globales.

El Estado en coordinación con todas sus partes integrantes realiza erogaciones muy importantes destinadas al óptimo desarrollo del sistema financiero, pues su mantenimiento es vital para un sano desarrollo de la nación. Estos costos sobrepasan de sobremanera la capacidad de pago de los Estados, pues las deudas contraídas son de tamaños inimaginables y una vez esta deuda debe de ser absorbida por el cúmulo de contribuyentes mediante aumentos en los productos de canasta básica, así como en el aumento en los precios de los bienes y productos de consumo, todo esto bajo la premisa de que quienes deben de tener la menor afectación, son aquellos organismos encargados de mover sus maquinarias operacionales que permiten el flujo monetario a lo largo y ancho del mundo, es decir que las instituciones financieras difícilmente van a perder su liquidez gracias al proteccionismo y auxilio de los diversos mecanismos que se han creado para salvaguardar su estabilidad, o bueno por lo menos no aquellas de carácter global con presencia en diversas partes del mundo que tienen la capacidad

para llevar a cabo estas acciones, por lo tal el Estado debe mantener un perfil de guardián ante las contingencias que puedan llegar a presentarse.

Dicho lo anterior, en el entendido de que el Estado hace frente a las pérdidas millonarias insubsanables por las entidades financieras, también éste debe desarrollar mecanismos preventivos, regulatorios, de investigación y una serie de logísticas operacionales con la finalidad de que las autoridades puedan detener este tipo de actividades, lo cual conlleva por supuesto un enorme gasto operacional en la implementación de tecnología, investigación, desarrollo y aplicación de leyes, divulgación, mecanismos jurisdiccionales, capacitación, éstas entre un sin fin de actividades que debe realizar el estado con la finalidad de mitigar este tipo de prácticas.

Una de las preguntas que genera este tipo de situaciones es definir que tanto intervencionismo debe de mantener el Estado en este tipo de relaciones, pues es evidente que existen ciertos intereses por parte de algunas clases políticas que pueden de alguna manera ser parte del mal que nos acomete, el Estado al tener un intervencionismo directo sobre éstas, su visión será la de enfocarse en otro tipo de prioridades que considere que son más necesarias para la atención de las diversas problemáticas que tienen en jaque al sistema financiero, o bien los intereses personales que se pueden derivar referentes a el manejo de los recursos o del otorgamiento de capital para proyectos personales.

Resulta trascendental el compromiso de los gobiernos de atender las recomendaciones y acuerdos internacionales a efecto de reducir las problemáticas derivadas del crecimiento exponencial del comercio electrónico, así como de las transacciones realizadas en la web, en mi punto de opinión es de suma importancia que se atienda esta problemática, pues sus características al ser una práctica que busca atacar sectores vulnerables, va migrando en las diversas esferas y regímenes sociales diversos, por lo que las experiencias previas en otras regiones que han sido víctimas de este tipo de prácticas nos pueden dar la pauta para poder implementar los mecanismos necesarios para erradicar este tipo de actividades, de la manera más acorde posible a nuestra propia idiosincrasia.

El esfuerzo operacional y económico que implica la implementación de este tipo de políticas es inimaginable, el primer paso que debiese darse a efecto de mitigar las prácticas es la de poner de conocimiento los rasgos que imperan en la utilización de los servicios electrónicos, es decir, medidas preventivas que permitan frenar mediante la oportuna detección de este tipo de ataques utilizando la web, para que de manera paulatina, puedan irse implementando los mecanismos de investigación que ayudaran a detectar este tipo organizaciones criminales, para que a su vez en caso de ser descubiertas puedan aplicarse todo tipo de medidas de reparación del daño, a efecto de aminorar los estragos ocasionados por el phishing y demás delitos cometidos en la internet, es decir que el Estado sea en todo caso aquel organismo rector que ponga las pautas necesarias para tener bajo control y resguardo los estragos derivados del prácticas tales como el phishing.

4.5.- PROPUESTAS SOBRE MEDIDAS DE SEGURIDAD PARA EVITAR EL PHISHING.

He hablado a lo largo de este trabajo de investigación, de la enorme importancia que conlleva conocer los diferentes fenómenos que día con día se presentan en nuestra sociedad, de lo trascendente que es conocer los avances tecnológicos y de las variaciones que se pueden presentar en estos. Una sociedad bien informada, es una sociedad fuerte, pues la transición del conocimiento nos hacer prevalecer ante las dificultades que se presentan día a día. Es consecuencia directa del desarrollo que en las sociedades exista por un lado abundancia y bienestar para aquellos que juegan un rol activo dentro de la maquinaria social, sin embargo, para aquellas que se desarrollan en un plano pasivo, no logran comprender y adecuarse al dinamismo de las nuevas eras, lo que también puede llegar a generar incertidumbre y cierta inestabilidad en las esferas más bajas de los estratos sociales, pues el desconocimiento y temor a lo nuevo, puede desencadenarse en una paranoia general, que bien puede ser aprovechada a efecto de crear daños con un gran impacto, esto en el entendido de que una sociedad desinteresada, poco informada y además temerosa, es blanco fácil debido a las vulnerabilidades que le rodean.

Para el Estado y las autoridades es de suma importancia mantener una esfera proteccionista en el territorio al que se encuentra concentrado su poder rector, por lo que es importante mantener un estricto control basado en la legalidad que abarque y proteja los aspectos más vulnerables de las sociedades, más de aquellos territorios con economías emergentes que aún mantienen estándares muy bajos en su calidad de vida, tal como pasa en México. Por ello, los Estados deben de desarrollar estrategias proteccionistas basadas en todos los mecanismos posibles de que puedan allegarse, los cuales siempre deberán tener como cimiento fundamental el de la prevención.

Para poder aplicar de manera adecuada estos mecanismos, primero se debe de tener conocimiento de qué o cuáles son las problemáticas a las que nos enfrentamos, cuál es impacto ocasionado, tanto en aspectos económicos como sociales, así como los costos operacionales de la implementación de políticas que atiendan al caso concreto, situación que está por demás decir se traduce en egresos que muy difícilmente pueden ser satisfechos debido a los diversos problemas que subsisten en nuestro país.

Hoy día uno de los grandes retos que enfrenta las regulaciones económicas, es el dinamismo y la rapidez con la que se generan nuevos métodos con los que se mueve el dinero, por lo que los Estados que por conducto de sus autoridades reguladoras deben de mantener una estricta coordinación con sus supervisados, que en el caso concreto hablamos de las instituciones financieras a efecto de generar medidas que auxilien a la prevención o detección de delitos que puedan llegar a cometerse a través de medios electrónicos como es en el caso del phishing. La organización debe de establecerse de manera piramidal, teniendo al Estado como principal rector de la creación e implementación de medidas de seguridad, pero su aplicación debe de ejecutarse de manera horizontal por los tres de entes que conforman la pirámide, siendo la base se está los clientes o usuarios de los servicios financieros, las instituciones financieras y el Estado como protector del sano desarrollo de la Economía en su territorio.

4.5.1. ESTADO.

Una vez que se han expuesto los estragos económicos que produce la figura del phishing en apartados precedentes, es el momento apropiado para tocar el tema referente a las medidas de seguridad que ha implementado o debería a mi humilde consideración el Estado en su carácter de rector y protector del sano desarrollo del Sistema Financiero Mexicano, así como aquellas que deberían de adoptarse de manera inmediata en atención a las recomendaciones emitidas por los diversos organismos y organizaciones internacionales doctas en la materia, al entendimiento de las diversas problemáticas con las que viene aparejado el crecimiento y aplicabilidad de nuevas tecnologías, así como la adopción de nuevos mecanismos que permitan en caso de que se materialicen este tipo de prácticas, tales como el phishing, establecer mecanismos adecuados de investigación y sanción basados en las ventajas que nos ofrecen las herramientas de la era moderna, insumos tecnológicos.

Conocimiento: Una de las grandes problemáticas que allegan a los Estados, o en algunos de estos, sobre todo en aquellos en el que el desarrollo es limitado, que es el desconocimiento de las nuevas tendencias o prácticas que se van desarrollando a cada segundo a lo largo y ancho de la faz de la tierra, en especial en cuestiones tecnológicas. El estado por medio de sus diversos mecanismos debe de encontrarse atento a los acontecimientos relevantes así como a todas aquellas conductas perniciosas que pueden llegar afectar de alguna manera ya sea directa o indirecta la territorio que circunscribe su gobierno, es decir debe de adelantarse a los hechos conocidos de otros territorios y crear políticas preventivas antes de que los fenómenos ocurran en su territorio, que si bien es posible que no detenerse de manera inmediata y completa, sería un importante mitigante que ayude a prevenir y reducir considerablemente los estragos económicos que producen este tipo de casos como lo es el phishing.

Capacitación: Para que pueda desarrollarse correctamente el punto anterior, es importante que las instituciones encargadas de velar por la seguridad, sobre el Estado surjan constantemente programas de educación y actualización, a efecto de que los integrantes de los organismos puedan llevar a cabo una labor más completa y que en general los mecanismos de protección que posee el estado tanto materiales, regulatorios y humanos , éstos, se encuentren siempre óptimos para enfrentar y resolver las situaciones

que se presenten. En este aspecto la constancia es uno de los aspectos más importantes a desarrollar, pues el dinamismo de la sociedad en general, alienta a que el entendimiento de las conductas se vuelva por demás complejo y laborioso, pues este cambio se presenta de una manera tan rápida y cada vez más elaborada, que es difícil seguir el ritmo de todos los cambios que surgen, por lo que se sugiere tomar ejemplos de casos que se presenten al rededor del mundo y que por sus características puedan materializarse en nuestro territorio, de esta manera tendríamos la infraestructura necesaria que auxiliaría en la disminución de diversos factores riesgosos elaborando planes de acción en contra de ataques que puedan generar daños patrimoniales o económicos que afecten de manera grave a nuestro sistema financiero.

Por lo que las diversas instituciones que tienen la enmienda de velar por la estabilidad del sistema financiero, así como todos aquellos organismos que tienen las facultades de investigación, deben de ocuparse en que su personal cuente con las capacidades técnicas y cognoscitivas de todas aquellas conductas que se vayan presentando, lo que propiciará a que exista un mejor manejo ante los diversos riesgos que se producen a través del mundo de la tecnología, sobre todo, de los medios de comunicación incluidos los medios electrónicos, tales como las transacciones monetarias por internet.

Así mismo, esto conlleva a la profesionalización de las instituciones en nuevas áreas de conocimiento en donde no se tiene el desarrollo necesario para crear e implementar los diversos mecanismos que permitan combatir adecuadamente las conductas que se presentan en los medios electrónicos, tales como el phishing.

Legislación: Las autoridades mediante sus diversos organismos necesitan de mecanismos que le permitan llevar a cabo las gestiones necesarias a fin de combatir actividades tales como el phishing, sin embargo, para que estas puedan llevarse a cabo de manera adecuada, deben de encontrarse en todo momento avaladas por una ley que les permita su correcto ejercicio, atendiendo a una serie de criterios y procedimientos que previamente deben de encontrarse establecidos en las leyes pertinentes.

Es por ello que lo mencionado en el punto anterior es su suma importancia, pues se requiere de personal altamente capacitado, con la convicción de desempeñar un excelente rol legislativo, a efecto de que puedan establecerse mecanismos eficaces en las normas, que para poder combatir efectivamente estas técnicas de ingeniería social tales como el phishing, pues requieren de una gran técnica legislativa y conocimientos precisos sobre las diversas conductas que puedan presentarse de manera paralela en este tipo de estafas, en el entendido de que los diversos artífices que se producen a efecto de obtener beneficios económicos de manera ilegal, son tan dinámicos como la sociedad misma, es por ello que la regulación deben intentar abarcar la totalidad de las posibilidades que se pueden presentar, a efecto de otorgar un gran margen de acción a las autoridades. Pues cuando se dé el momento oportuno a efecto de encender la maquinaria legislativa en torno a estos temas, será una única oportunidad que deberá ser aprovechada al máximo, pues sabemos lo tedios y difícil que temas así sean considerados de relevancia en nuestro país.

Además de esto, las leyes que se apruebe al respecto no solo servirán a efecto de prevenir e investigar este tipo de ilícitos, sino también serán el eje rector regulatorio del sector financiero, es decir, será la directriz mediante la cual el Estado proponga los estándares y medidas de seguridad mimas que deberán de adoptar e implementar las instituciones financieras a efecto de que conjuntamente se tengan controles adecuados que permitan mitigar este tipo de conductas que producen pérdidas multimillonarias a los participantes activos de nuestro sistema financiero.

Cooperación: El Estado, a través de sus diversos mecanismos, debe de proponer las directrices mediante las cuales los gobernados, hablando de personas físicas, así como de entes jurídicos, sobre todo de aquellos que forman parte del sistema financiero, las cuales deberán de ser adoptadas puntualmente por estos, a efecto de que el conocimiento de aquellas conductas tan perniciosas para el equilibrio económico de nuestra nación, tales como el Phishing, ocurran de manera inmediata, lo que brindará un mayor margen de acción, pues el rápido conocimiento de este tipo de actividades permite su pronta difusión, para con ello evitar que un gran número de personas sucumba ante este tipo de artífices de ingeniería social, la dificultad de esto radica en un principio en

que el ataque es realizado a los usuarios de los servicios financieros, este no tiene siquiera conocimiento de este tipo de prácticas que pueden ocurrir en decremento de su patrimonio, por lo que el desconocimiento y/o ignorancia permite que sean pocas las quejas presentadas ante las instituciones financieras y aquellas que son atendidas son tratadas con un sin fin de escrúpulos a fin de imputar la responsabilidad a los propios clientes.

Es así que el Estado debe de proporcionar los medios idóneos y facilitar el flujo de información, mediante la cual los integrantes del sistema financiero, deberán de allegar los reportes de todas aquellas conductas, así como las nuevas prácticas que se detecten por éstos, que puedan significar pérdidas patrimoniales por fraudes tales como el phishing, lo anterior en aras de desarrollar procedimientos, programas de reconocimiento inmediato y la correcta difusión de los nuevos medios comisivos, así como las medidas de acción que habrán de seguirse a efecto de procurar evitar que el mal se siga propagando.

Por otro lado, el Estado en conjunto a sus diversos organismos, deberá de proponer los lineamientos que deberán de seguirse a efecto de proporcionar la información a las autoridades que auxilie al conocimiento de las diversas conductas que puedan llegar a presentarse, para aplicar las medidas de seguridad pertinentes previamente establecidas y que estás se cumplan al pie de la letra los diversos mecanismos homogéneos establecidos para tal fin. Para que esto pueda ser aplicado con la debida diligencia por todos aquellos que se encuentren en los supuestos de vulnerabilidad, específicamente hablado de los entes financieros, deberán de proponerse medios coercitivos que incluyan medidas de apremio a efecto de que éstas sean aplicadas con todo el rigor de la ley en caso de la no cooperación, por la desatención a los requerimientos de las autoridades, por permitir la proliferación de dichos ataques en decremento del sistema financiero mexicano y de las personas que mantienen su patrimonio resguardado en éste.

4.5.2. INSTITUCIONES FINANCIERAS.

La mayoría del flujo de operaciones monetarias, cada vez es más frecuente que se realicen habitualmente en los diversos instrumentos financieros digitales que ofrecen instituciones del sector, debido a las facilidad con la que pueden ser realizadas y por la seguridad que implica no estar disponiendo de cantidades considerables de dinero en efectivo, con el temor de ser atacados, siendo víctimas de robos y asaltos violentos, es por ello que es imperante para el sector financiero realizar las acciones necesarias con la finalidad de que este tipo de transacciones sigan siendo consideradas ágiles y seguras, estableciendo estas premisas como su base de negocio.

Sin embargo, se encuentran ante un grande reto, pues la automatización de estos servicios, conlleva de manera paralela, nuevas formas de intentar obtener aprovechamientos, valiéndose de las herramientas tecnológicas de manera que gracias a sus benevolencias pueden obtener ingresos de manera ilegal, por lo que se vuelve necesaria la intervención y anticipación que permitan que los servicios financieros sigan siendo considerados seguros, es decir deberán de llevar a cabo las estrategias necesarias que permitan que sus clientes tengan la seguridad y confianza de mantener resguardado su patrimonio en estas. Para lograr lo anterior, deberán de implementar como mínimo las siguientes acciones:

Conocimiento: Para las instituciones financieras es de relevante importancia encontrarse en constante actualización de la misma forma y a la velocidad como lo realizan los ciberdelincuentes al encontrar nuevas formas de realizar nuevas conductas en los medios electrónicos o computacionales, a lo que comúnmente denominamos como tipologías.

El tema de la actualización y del conocimiento debe de tener la característica imprescindible que es la que debe de ser de manera permanente, pues el dinamismo de estas conductas y la velocidad con la que se propagan muchas veces dificulta su debida identificación derivando en un menoscabo patrimonial. Es por lo anterior que el área responsable en las instituciones de identificar este tipo de riesgos, debe de tener un conocimiento inmediato respecto de aquellas conductas que puedan llegar a presentar una amenaza latente tanto para la institución, como para sus clientes, es por ello que

deben de implementar medidas de detección oportunas, que auxilien a frenar a todos aquellos que pretenden realizar acciones que vulneren el sistema financiero, con el propósito de obtener ciertos beneficios de en perjuicio de terceros.

Implementación de Tecnología y seguridad: Por lo anterior, las instituciones deberán de implementar por conducto de sus estructuras organizacionales, un centro de inteligencia integrado por personal altamente capacitado, que se encuentre de manera permanente al pendiente de posibles ataques cibernéticos, de la posible sustracción de información, de la suplantación o robo de sus principales medios de comunicación, tales como sus páginas más de internet. También deberán de encontrarse al tanto de aquellas actividades sospechosas, así como del monitoreo transaccional de sus clientes, con el propósito de identificar alguna práctica fraudulenta o bien inusual.

Se deberá implementar un programa de acción, en el que la vigilancia sea constante, reforzando las medidas de seguridad, proponiendo mecanismos adecuados que permitan el debido cuidado y manejo de la información tanto de la propia institución como de sus clientes.

Con lo anterior, se pretende dar un gran margen de acción a las instituciones, a efecto de que se pueda actuar con prontitud ante este tipo de imprevistos y evitar que el quebranto económico hacia las instituciones y el sistema financiero no tenga un impacto grave, así mismo deberán de implementarse programas de colaboración que permitan la difusión de las distintas prácticas o medios comisivos de los que pudieron percatarse las instituciones, por lo que deberá de recabarse y conservarse la información que tenga las características de relevante a efecto de que pueda ser diseminada y divulgada a efecto de implementar planes de acción que permitan mitigar los riesgos generados por estas prácticas.

Capacitación: Para que lo anterior tenga un funcionamiento ideal, es necesario que las entidades financieras apuesten por el perfeccionamiento del conocimiento que posean sus empleados. Es necesario que se implementen programas de capacitación constante respecto a los nuevos riesgos que puedan surgir, a las medidas de seguridad y los

lineamientos mínimos que deben seguir los empleados a efecto de poder detectar posibles riesgos, así como brindar la atención pertinente a clientes que tengan duda respecto a la posibilidad de haber sido perjudicados por este tipo de artífices como el phishing.

Además, su labor deberá estar encaminada a resolver las problemáticas que conlleva el phishing, por lo que tendrán que estar sumamente preparados para recabar diversa información que auxilie en la labor de investigación, que de tal manera servirá para la integración del expediente que sustentara la investigación respectiva, que al caso concreto deberá justificar el resarcimiento de los daños y en su caso iniciar las acciones legales pertinentes a efecto de recuperar los activos perdidos.

Cooperación: Así mismo, deben de implementarse mecanismos coordinados que permitan a las instituciones financieras perseguir conjuntamente la prácticas que tienden a vulnerar el sistema financiero tales como el phishing, pues permitirán conocer en mayor medida de las experiencias negativas que se han tenido al respecto, lo que de cierta manera ayuda a mitigar el riesgo, pues se crea una conciencia específica sobre casos que pueden llegar a presentarse y derivado de estas experiencias, tomar las determinaciones necesarias para evitar el perjuicio económico.

Es por ello que se expresó en el punto precedente, que es importante que las instituciones conserven en sus registros todas aquellas operaciones de relevancia informática, a efecto de que quedé perpetrado el conocimiento y se tenga una noción de las prácticas que pueden repetirse en un espacio de tiempo determinado, aunque sobre el particular, dichos registros únicamente le servirían a la propia institución, por ser información confidencial, por lo que sería ideal que se establecieran ciertos mecanismos por los cuales las diversas instituciones se permitieran el intercambio de ésta, a efecto de contar con un mayor conocimiento sobre las diversas tipologías relacionadas para realizar ataques de phishing u otras conductas relacionadas con sistemas informáticos.

Así mismo, al Estado debe de incumbirle el intercambio de este tipo de información, y permitir, así como incentivar este tipo de alianzas, es a través de sus autoridades regu-

ladoras, así como sus unidades de inteligencia financiera y agencias de investigación ministeriales, tendrían la capacidad no sólo de conocer el desarrollo y evolución de las prácticas tales como el Phishing de manera directa, sino también de ser el medio idóneo a efecto de servir como enlace entre las instituciones, para si buscar como fin común, evitar la proliferación de este tipo de conductas. Además, bajo su autoridad se impulsaría que este intercambio se realizará de manera segura, confidencial e inmediata. Para la implementación de este tipo de comunicaciones se necesita de infraestructura tecnológica adecuada, lo que puede llevar años y millones de recursos invertidos en su funcionamiento.

Por lo que se debe actuar en un ambiente de permanente cooperación entre pares (hablando de las Instituciones financieras), teniendo como nexo al Estado ejerciendo los diversos mecanismos con que se cuente, con la permanente supervisión de las autoridades que se designen para el caso concreto.

Difusión: Una vez que se tenga conocimiento puntual sobre un posible ataque de phishing, las entidades en sus diversos medios de comunicación deberán hacer del conocimiento inmediato a sus clientes sobre el ataque del que pueden llegar a ser víctima, indicando en dichos mensajes de manera puntual, las acciones que se habrán de tomar en caso de recibir ese tipo de mensajes, o en caso de ya ser víctima de ellos.

Por otra parte, deberán de llevar a cabo campañas permanentes a efecto de concientizar a sus clientes, respecto a los riesgos latentes que existen al utilizar parte de sus servicios, respecto de la importancia de la confidencialidad de la información personal y las acciones tendientes a su protección, creando suma conciencia de que las claves de seguridad, Nip’s, usuarios, contraseñas, claves dinámicas, números de tarjetas, son datos sensibles y personales, por lo que deberán de tener un manejo especial.

Además, deberán de hacer extensiva la información que se obtenga por parte de las autoridades, aplicando de manera pronta las guías y propuestas de mejores prácticas de seguridad que sean publicadas en los medios pertinentes por la autoridad responsable, promoviendo de manera constante la capacitación entre sus empleados para

poder atender las contingencias que se presentes por prácticas cometidas con el abuso de medios electrónicos, tales como el phishing.

4.5.3. CUENTAHABIENTES.

Los titulares de los diversos productos financieros que ofrecen las entidades, en realidad son quienes se ven más afectados por este tipo de prácticas de ingeniería social tales como el phishing, pues la afectación económica recae directamente sobre su patrimonio, tal y como ha dicho a lo largo de este trabajo de investigación, por lo que en este apartado describiremos algunas acciones tendientes a efecto de evitar ser víctima de esta y cualquier otra práctica fraudulenta que pueda comprometer la confidencialidad de su información y la integridad de sus bienes.

En primer lugar, aquellas personas interesadas en obtener algún servicio o producto de la diversidad que ofrecen las entidades financieras, es de vital importancia que se informen respecto de los diversos beneficios, cargas, penalidades y sobre todo de los riesgos que puede conllevar la adquisición de cualquiera de estos productos, esto con la finalidad de tener en mente que es lo que puede llegar a ocurrir en dadas circunstancias y así prevenir cualquier anomalía que pueda llegar a presentarse en el manejo de sus cuentas, para ello deben de acercarse con los especialistas o bien consultar la información que brindan las entidades en sus diversos medios de comunicación, una herramienta de consulta bastante práctica y accesible es visitar la de los sitios de internet de las instituciones, en estas, se encuentra un gran cúmulo de información importante.

Otro método a efecto de tener información es buscar o apoyarse directamente en páginas de los diversos organismos gubernamentales que tienen como prioridad el regular dichas actividades, o bien cuidar los intereses de los usuarios, tales como la realiza la CONDUSEF.

Así mismo, es importante que los clientes, se creen una buena costumbre y tener interés por adquirir una nutrida cultura financiera, para ello es importante que tomen en cuenta todas las recomendaciones e información que de manera directa les son reali-

zadas por las entidades por conducto de sus diversos canales de comunicación, siendo los más usuales los desplegados en sus páginas de internet, mediante el envío de mensajes en los estados de cuenta, los desplegados en las pantallas de los cajeros automáticos, así como anuncios publicitarios en medios de comunicación masiva como redes sociales, televisión, radio y anuncios publicitarios.

No obstante, estas medidas deberán de ser mínimas, pues la obligación de mantener un control y otorgar la confianza de la realización de las transacciones monetarias mediante la utilización de sistemas informáticos debe de incumbir primordialmente a las instituciones financieras y estará en sus manos implementar los mecanismos necesarios que brinden seguridad integral a sus clientes. Así mismo, el Estado deberá regular de manera inmediata las actividades que permitan estas circunstancias y en mayor medida les brinden la protección suficiente a los cuentahabientes.

CONCLUSIONES.

PRIMERA: A grandes rasgos el “Phishing” es una especie de fraude electrónico especializado basado en la implementación de medios tecnológicos, en la cual, quien la realiza, tiene el cometido de obtener información detallada, personal y confidencial. Específicamente aquella información relacionada con claves de seguridad para acceso a servicios financieros, bancarios, sitios de compraventa de productos y servicios en línea, etc., con la finalidad de utilizarlos en su beneficio de manera lucrativa.

SEGUNDA: Dentro de sus modos de operación el “phishing” se realiza enviando un correo electrónico a sus víctimas o usuarios, en los que imitan casi a la perfección el lenguaje, formato e imagen de los portales web de entidades bancarias o financieras, así como en algunos casos de empresas que ofrecen productos o servicios de reconocido prestigio, solicitando a los usuarios o prestatarios de los servicios la confirmación de determinados datos personales íntimamente relacionados con transacciones bancarias, a efecto de la verificación de los mismos, argumentando distintos motivos que suponen un riesgo para el usuario tales como: medida de seguridad, actualización, cambio en las políticas de privacidad, prevenir algún tipo de fraude, problemas técnicos, en fin cualquier tipo de excusa por la cual los clientes de dichas empresas sientan la imperiosa necesidad de proporcionarlos, y una vez que han sido engañados envían la información confidencial al estafador, y una vez que ha pescado las contraseñas, puede disponer libremente de los recursos, sustrayendo el dinero, realizando transferencias electrónicas a otras cuentas o bien realizando compras o pago de servicios.

TERCERA: La notable evolución en la manera en que se realizan transacciones económicas en la actualidad, además de facilitar enormemente el flujo monetario transnacional, otorga un gran nivel de confianza a los usuarios debido a que gracias en los sistemas informáticos y computacionales se tiene siempre conocimiento del origen y des-

tino de los recursos. No obstante lo anterior, gran parte de la población aún se encuentra temerosa de su implementación, debido a que no comprenden del todo su funcionamiento, el desconocimiento y la poca información que poseen los usuarios de los diversos servicios financieros provoca que prácticas como el phishing tengan éxito, no por ello quiere decir que el usuario tenga la carga de la culpa ante estas acontecimientos, sino todo lo contrario, el Estado y los integrantes del sistema financiero deben encontrarse al tanto en todo momento a efecto de afrontar las diversas eventualidades que puedan llegar a presentarse al utilizar los servicios de transacciones económicas electrónicas y ante todo brindar la protección necesaria a los usuarios en aras de mantener la estabilidad del sistema financiero.

CUARTA: Es imprescindible tener en mente que, así como el "phishing" que se encuentra basado en un simple engaño utilizando la suplantación con métodos de ingeniería social, pueden surgir en cualquier momento nuevas prácticas que tiendan a perjudicar a las personas que día con día utilizan los servicios de internet, por lo que es necesario que la comunicación e intercambio de información de las diversas tipologías que puedan llegar a detectarse, sea de manera inmediata. Por lo que en le caso de México la participación en foros internacionales y la suscripción o ratificación de acuerdos internacionales, según sea el caso, en materia de seguridad informática, en general sea de manera constante e inmediata. Lo anterior auxilia en la pronta detección, la mitigación de riesgos y la detención en la proliferación de conductas perniciosas para la sociedad, sobre todo de aquellas tan sensibles como las patrimoniales.

QUINTA: A través del estudio jurídico de la figura del phishing es posible apreciar el gran dinamismo y amplitud que nos permite conocer la ciencia jurídica y la relevancia empírica que puede llegar a tener en su aplicación. Existe un hecho negativo muy importante íntimamente relacionado con las nuevas tecnologías y la informática relativo a los hechos que ocurren en ella y éste es que en México es casi nulo el estudio del derecho en dichas áreas, aquel al estar relacionado prácticamente con todo lo que nos rodea, también debe de estarlo con la informática que se ha vuelto indispensable en la vida cotidiana de la mayor parte del mundo, incluidas las transacciones financieras.

SEXTA: El derecho informático debe de ser ampliamente estudiado, de ser incluido en los planes de desarrollo vocacional de las universidades, en atención a los nuevos requerimientos y competencias que son necesarias para el desarrollo en el nuevo mundo, el mundo tecnológico. Por lo que es de suma relevancia que todos aquellos que tengan relación directa con las leyes y el Derecho, adquieran conciencia respecto de que hoy en día la mayoría de las actividades del ser humano se realizan con auxilio de las nuevas tecnologías y con base en ello pueden existir consecuencias de derecho que deben de ser específicamente reguladas, con la finalidad de mantener el buen control y estabilidad de la sociedad.

SÉPTIMA: Así mismo, es de destacar la relación que tiene el derecho informático con las múltiples transacciones económicas que se encuentran íntimamente relacionadas con el derecho mercantil debido a que en una gran parte los actos de comercio ahora son realizados con el auxilio de los medios informáticos, es por ello que también por estos medios han aparecido sujetos que han querido aprovechar las vulnerabilidad de éstos para obtener beneficios económicos de manera ilegal, mediante el desarrollo de prácticas como el “phishing”, prácticas que afectan de manera importante la estabilidad de las economías de los países y del sistema financiero.

OCTAVA: El phishing afecta gravemente la estabilidad de las economías del mundo perjudicando principalmente al sector bancario atacando los puntos débiles que precisamente es a través de sus usuarios, se mencionó que aproximadamente en el 2015, la empresa “Karsperky labs” (especialista en programas antivirus) informó que conforme a sus estudios, en sus bases de datos se detectaron aproximadamente 50 millones de ataques de phishing, como actualización para 2016, la cifra aumentó a 398 millones, de los cuales el 47% han sido perpetuados en contra del sector bancario. Es por ello que existe la insistencia en que tanto el estado como las partes del sistema financiero optimicen sus medios de defensa con medidas preventivas, que permitan la mitigación de riesgos de ataques que utilicen como medio de comisión los sistemas electrónicos o informáticos y así evitar las pérdidas millonarias que sufren año con año las instituciones financieras y por ende, el sistema financiero, no obstante, para esto es necesario

contar con los mecanismos legales adecuados que permitan formar el plan o planes de acciones que combatan estas prácticas.

NOVENA: No obstante, lo anterior los mecanismos legales con los que cuenta México son ineficientes e insuficientes no solo para el caso específico del phishing, sino de todos los ilícitos que puedan llegar a cometerse con el uso de sistemas informáticos. En primer término, la aplicación de las pocas leyes que existen se vuelve prácticamente imposible, en el caso de las penales no existe ningún tipo penal que pueda adecuarse al caso concreto específico, el phishing al estar compuesto por diversas etapas que tienen diversas variantes, como es el caso del robo de información, la suplantación de identidad, la falsificación o secuestro de sitios web, el lavado de dinero, etc. conlleva una gran labor poder identificar y homologar cada uno de los elementos.

DÉCIMA: Sería prudente elaborar un manual de acción a efecto de evitar y sancionar éste tipo de prácticas en los diversos ámbitos de competencia por materia, es decir, si cualquiera de las autoridades administrativas de investigación detecta alguna caso en particular de phishing, deberá de investigarlo y hacer del conocimiento a las demás autoridades a efecto de seguir con la investigación y posible aplicación las sanciones tanto penales, civiles y administrativas, según sea el caso concreto y en el ámbito de sus respectivas competencias. Sin embargo, para que lo anterior pueda acontecer primero se requeriría que las leyes específicas de cada materia contemplaran el supuesto, esto es, que cuente con los mecanismos legales adecuados y con una capacitación integral que permita el buen desempeño de sus funciones.

Para que esto sea posible se necesitaría una reforma estructural y complementaría respecto a los temas de seguridad informática, como se ha mencionado es necesario la adopción de los diversos tratados internacionales y su inmediata ratificación para que con ello se active la maquinaria legislativa y dar la suficiencia de mecanismos tanto a autoridades como a particulares, aunque se sabe que esto podría tardar demasiado debido a la politización de los procesos creadores de normas, aquí es en donde radica la insuficiencia.

DÉCIMA PRIMERA: Dentro de las particularidades de la figura del phishing es que transgrede diversas esferas jurídicas tal como se expuso en el capítulo tercero, tales como la suplantación de identidad, el robo de datos personales mediante la defraudación, la copia ilegal o secuestro de sitios web, el lavado de dinero, etc., sin embargo, quien es más vulnerable y afectado es el sistema financiero en sus múltiples niveles hablando específicamente y en orden ascendente son los usuarios del sistema financiero, las entidades y por último el Estado como máximo rector del sistema financiero mexicano. La finalidad de hablar del tema es principalmente poner sobre la mesa un asunto del que pocos hablan y muchos desconocen, exponer de manera breve pero concisa cuál es el avance que tenemos hasta ahora y cuáles son las posibles medidas que podrían adoptarse apoyado en las diversas experiencias de otros países, hacer hincapié en la pronta adopción y aplicación de los tratados internacionales.

DÉCIMA SEGUNDA: En éste momento se encuentra el ante proyecto de la denominada “Ley Fintech de México” encargada de regular a las empresas de servicios e instituciones de tecnología financiera, que básicamente se encargan de realizar operaciones con activos virtuales, por ejemplo las denominadas “criptomonedas”, es un pequeño gran paso, pues es importante regular su funcionamiento ya que su importancia uso y valor adquisitivo cada día son más importantes, sin embargo, no me cansaré de repetirlo, también hay que pensar en las consecuencias y posibles peligros que pudiesen acontecer y trabajar en ello adecuando en lo posible nuestro marco normativo y forma de entender y crecer con la propia evolución tecnológica de que somos parte.

FUENTES DE INVESTIGACIÓN.

BIBLIOGRAFÍA.

• Acosta Romero, Miguel, Nuevo Derecho Bancario Panorama del Sistema Financiero Mexicano, 9ª Edición, Editorial Porrúa, México 2003.

• Acosta Romero, Miguel, Derecho de la Defensa de los Servicios Financieros Mexicanos, 1ª Edición, Editorial Porrúa, México 2002.

• Azaola Calderón, Luis, Delitos Informáticos y Derecho Penal, 1ª Edición, Editorial Ubijus, México 2010.

• Barrera Graf, Jorge, Instituciones de Derecho Mercantil, 2ª Edición, Editorial Porrúa, México 2014.

• Bryne, John J. y otros. Guía de Estudio para el Examen de Certificación CAMS, Quinta edición, Miami USA, 2011.

• Calderón Cerezo, A., Choclan Montalvo, J.A., Derecho Penal. Parte especial, Tomo II, Editorial Bosch, Barcelona 2001.

• Calderón Martínez, Alfredo; Garzón Galván, Jonathan Gabriel; Gómez Treviño Joél A.; Guerra Valdivia, Alicia Rubí; Ibarra Sánchez, Ernesto; Nava Garcés, Alberto Enrique (Coord.), et al, El Derecho en la Era Digital, 1ª Edición, Editorial Porrúa, México 2013.

• Carvallo Yañes, Erick, Nuevo Derecho Bancario y Bursátil Mexicano, 8ª Edición, Editorial Porrúa, México 2010.

• Cervantes Andrade, Raúl, "Robo de Identidad. Urgencia de su Regulación en México", en Roque Díaz, José Rodrigo, Delitos de Cuello Blanco, INACIPE, México 2011.

• . Córdova Gutiérrez, Alberto y Palencia Escalante, Carlos, El Lavado de Dinero: Distorsiones Económicas e Implicaciones Sociales, Instituto de Investigaciones Económicas y Sociales Lucas Alamán, A.C., México, 2001

• Corco y Bidasolo, M. y Joshi Hubert, U., Delitos contra el patrimonio cometidos por medios informáticos, Revista Jurídica de Cataluña, Núm III, Barcelona, 1988.

• Choclan Montalvo, J.A. "Fraude informático y estafa por computación", en internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid 2001.
• De la Fuente Rodríguez, Jesús. Tratado de derecho bancario y bursátil, seguros, fianzas, organizaciones y actividades auxiliares del crédito, ahorro y crédito popular, grupos financieros. Sexta Edición, Tomo II, Editorial Porrúa, México 2010.
• De la Fuente Rodríguez, Jesús, Delitos Financieros, Teoría y Casos Prácticos (Bancarios, Bursátiles, Seguros, Fianzas, organizaciones Auxiliares del Crédito y de Ahorro y Crédito Popular), 2ª Edición, Editorial Porrúa, México 2010.
• Fernández Espejel, Gabriel. ¿Por qué legislar el combate al lavado de dinero? Acciones Frente al lavado de dinero. Centro de Estudios Sociales y de opinión Pública, México 2012.
• Fuentes Sánchez, Damian, Fraudes en la Red, en s/a, Cibercriminalidad, INACIPE, México 2006.
• Galindo Sifuentes, Ernesto, Derecho Mercantil, Comerciantes, Comercio Electrónico, Contratos Mercantiles y Sociedades Mercantiles, 2ª Edición, Editorial Porrúa, México 2007.
• Gamboa Montejano, Claudia. "Lavado de Dinero" Estudio teórico conceptual, Derecho comparado, Tratados internacionales y de la nueva ley de la materia en México. Cámara de Diputados, Dirección de servicios de investigación, Subdirección de Análisis de Política Interior. Enero, 2013.
• Gluyas, Millán Ricardo. "Inteligencia Financiera y Prevención de lavado de dinero", *Iter Criminis, Revista de Ciencias Penales,* núm. 12, segunda época, México, INACIPE, México, 2005
• Gómez Granillo, Moisés, Breve Historia de las Doctrinas Económicas, 23ª Edición, Editorial Esfinge, México 2001.
• Guerrero, Diego, Fraude en la red. Aprenda a protegerse contra el fraude en Internet, Editorial Ra-Ma, 2010.
• Gutiérrez Zarza, Ángeles (Coord.) Nuevas Tecnologías Protección de Datos Personales y Derecho Penal, 1ª Edición, Editorial Wolters Kluwer, España 2012.

•León Tovar, Soyla H., Contratos mercantiles, Editorial Oxford University Press, 1° edición, 10° reimpresión, México 2012, p. 593

•Márquez Piñeiro, Rafaél, Delitos Bancarios, 6ª Edición actualizada, Editorial Porrúa, México 2010.

•Mora, José Luis y Enzo Molino, Introducción a la Informática, Editorial Trillas, México 1973.

•Muñoz Torres, Ivonne, Delitos Informáticos Diez Años Después, 1ª Edición, Editorial Ubijus, México 2009.

•Nava Garcés, Alberto E., Análisis de los Delitos Informáticos, 1ª Edición, Editorial Porrúa, México 2005.

•Narvaez Bonnet, Jorge Eduardo, El Contrato de Seguro en el Sector Financiero, 2ª Edición, Editorial Ediciones Librería del profesional, España 2004.

•Quintana Adriano, Elvia Arcelia, Ciencia del Derecho Mercantil, Teoría Doctrina e Instituciones, 2ª edición, Editorial Porrúa, México 2004.

•Rios Estavillo, Juan José, Derecho e Informática en México, 1ª Edición, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México 1997.

•Romeo Casabona, C. M. Poder informático y seguridad jurídica, Fundesco, Madrid 1997, p. 41. Citado por Azola Calderón, Luis. Delitos Informáticos y Derecho Penal, Ubijus, México 2010.

•Romero Flores, Rodolfo. El Robo o Usurpación de Identidad por Medios Informáticos o Telemáticos: Su Tratamiento Jurídico Penal, Instituto de Investigaciones Jurídicas UNAM, 2010.

•Romo, Jorge L. Prevención del Lavado de Dinero y Delincuencia Organizada, 1ª Edición, Editorial UBIJUS, México 2012.

•Sanchis Crespo, Carolina Coord. *Et all,* Fraude Electrónico: Entidades Financieras y Usuarios de Banca, 1ª edición, Ed. [Thomson Reuters] Aranzadi, España 2011.

• Téllez Valdés, Julio, Derecho Informático, 4ª Edición, Editorial Mc Graw Hill, México 2009.

•Vásquez del Mercado Cordero, Oscar. Contratos Mercantiles, 16° Edición, Primera reimpresión, Editorial Porrúa, México 2014

FUENTES ELECTRÓNICAS.

- http://docplayer.es/5876513-Ol-clphishing-y-pharming-una-aproximacion-desde-el-cibercrimen.html
- http://www3.diputados.gob.mx/camara/005_comunicacion/a_boletines/2012_2012/003_marzo/28_28/4943_adecuan_el_codigo_penal_federal_para_castigar_delitos_informaticos
- http://www.antipishing.org
- http://www.antiphishing.org/about-APWG/
- http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf
- https://www.asociaciondeinternet.mx/es/
- https://www.banamex.com/es/personas/servicios/seguridad/ejemplos_phishing/demo_ejemplos_phishing.htm
- https://www.bbva.com/es/skimming-la-estafa-la-clonacion-tarjetas/
- http://bcn.cl/1m196
- http://biblio.juridicas.unam.mx
- http://biblio.juridicas.unam.mx/libros/6/2958/20.pdf
- http://blog.segu-info.com.ar/2011/02/phishing-tipo-penal-en-argentina-y-sus.html
- http://www.brighthub.com/internet/security-privacy/articles/82116.aspx
- http://www.bsecure.com.mx/enlinea/espia-de-llamadas-voip/
- https://www.boe.es/diario_boe/txt.php?id=BOE-A-1995-25444
- http://www.cnnexpansion.com/mi-dinero/2015/05/20/mexicanos-desconfian-de-la-ciberseguridad-de-sus-bancos_(Consultado
- http://www.cnnexpansion.com/tecnologia/2015/06/03/rompase-en-caso-de-phishing-que-hacer-antes-y-despues
- https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf
- http://www.gob.mx/condusef/prensa/aumentan-40-reclamaciones-imputable-a-posible-robo-de-identidad-en-primer-semestre-de-2015.

- http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/667-clonacion-de-tarjetas
- http://www.cnbv.gob.mx/SECTORES-SUPERVISADOS/OTROS-SUPERVISADOS/Preguntas-Frecuentes/Paginas/Sociedades-de-Informaci%C3%B3n-Crediticia.aspx
- http://www.condusef.gob.mx/index.php/instituciones-financieras/sociedades-de-informacion-crediticia/624-sociedades-de-informacion-crediticia-que-son
- https://www.congress.gov/bill/109th-congress/senate-bill/472/text
- http://www.consumer.es/web/es/tecnologia/internet/2013/11/05/218429.php
- http://www.delitosinformaticos.com/06/2008/noticias/la-incorporacion-de-los-delitos-informaticos-al-codigo-penal-argentino#
- http://www.diputados.gob.mx/LeyesBiblio/pdf/43_170616.pdf
- http://dof.gob.mx/nota_detalle.php?codigo=4948419&fecha=17/05/1999
- http://www.elfinanciero.com.mx/economia/aumentan-en-60-reclamos-por-fraudes-en-tarjetas.html
- http://www.eltiempo.com/tecnosfera/paises-latinoamericanos-en-ciberseguridad-129604
- http://www.excelsior.com.mx/hacker/2016/12/07/1132670
- http://www.excelsior.com.mx/nacional/2017/02/27/1148915
- http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223
- http://www.gytcontinental.com.gt/portal/portal/productos.asp?Option=4&idProd=FAQ&Category=Article&SubCategory=seguridad&idQ=21&State=1
- https://hechoencu.wordpress.com/2008/04/07/phreaking-hacking-o-cracking-telefonico-delitos-informaticos/
- http://www.elfinanciero.com.mx/sociedad/mexico-suscribe-convenio-iberoamericano-contra-la-ciberdelincuencia.html
- http://www.eyboletin.com.mx/eysite2/pdf/comentarios_1617.pdf
- http://www.hsbc.com.mx/1/2/es/pie-pagina/seguridad/phishing
- http://www.infospyware.com/articulos
- http://www.jornada.unam.mx/ultimas/2015/09/14/fraudes-financieros-crecieron-14-este-ano-condusef-164.html

- https://www.juridicas.unam.mx/legislacion/ordenamiento/codigo-federal-de-procedimientos-penales#7496
- http://www.lawyerpress.com/news/2013_07/3107_13_005.html
- http://www.malware.unam.mx/es/content/un-vistazo-la-situaci%C3%B3n-de-phishing-y-malware-en-m%C3%A9xico-abril-%E2%80%93-junio-2015.
- https://malware.unam.mx/es/content/steam-plataforma-de-videojuegos-objetivo-de-phishing-y-malware
- http://www.mcgraw-hill.es/bcv/guide/capitulo/8448171330.pdf
- http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
- http://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx
- https://mx.norton.com/cybercrime-phishing
- http://www.oas.org/dil/esp/Codigo_Penal_de_la_Republica_Argentina.pdf
- ttp://www.oas.org/juridico/PDFs/arg_ley26388.pdf
- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- https://www.oecd.org/sti/consumer/34023784.pdf
- http://www.oecd.org/sti/ieconomy/15590267.pdf
- http://www.onguardonline.gov/phishing
- http://www.osimga.org/export/sites/osimga/gl/documentos/d/ogsi/doc_ext/ambito_estatal/estudio_sobre_usuarios_afectados_por_phishing_2007.pdf
- http://pages.ebay.es/aboutebay/thecompany/companyoverview.html
- http://www.pdichile.cl/jenadec/cibercrimen/index.htm
- http://perezmacedo.com/artículos-de-interés/delitos-graves-en-el-codigo-nacional-de-procedimientos-penales/
- https://proyectophishing.wordpress.com/2006/08/10/phishing-%C2%BFque-es-su-historia-y-modo-de-operar/
- http://www.quo.es/tecnologia/un-grupo-de-hackers-roba-900-millones-de-euros-a-100-bancos
- https://securelist.lat/analysis/informes-trimestrales-sobre-spam/84261/spam-and-phishing-in-q3-2016/
- . https://seguinfo.wordpress.com/2006/11/14/el-numero-de-ataques-de-phishing-se-duplica-en-estados-unidos-3/

- https://seguinfo.wordpress.com/category/ingenieria-social/page/11/
- http://transparencia.senado.gob.mx/historico_respuestas/content/2005/1-abril/F601.pdf
- http://www.tsi.com.pe/historia9.htm
- http://www.victormiranda.com.mx/vmwp/sabes-que-es-phishing/
- http://www.washingtonpost.com/wp-dyn/articles/A63749-2005Mar1.html

LEGISLACIÓN CONSULTADA.

- Código Penal Colombiano, publicada el 24 de julio del 2000, última modificación 2 de febrero de 2016.
- Código Penal del Estado de Guanajuato, publicado el 2 de noviembre del 2001, última reforma 14 de julio de 2017.
- Código Penal del Estado de Yucatán, publicado el 30 de marzo del 2000, última reforma 18 de julio de 2017.
- Código Penal Para el Distrito Federal, publicado en la Gaceta Oficial del Distrito Federal el 16 de Julio de 2002, última reforma 16 de junio de 2016.
- Código Penal Para el Estado de Colima, publicado en el Periódico Oficial "El Estado de Colima", 11 de octubre de 2014, última reforma 11 de junio de 2016.
- Código Penal para el Estado de Chiapas, publicado en la Tercera Sección del Periódico Oficial del Estado de Chiapas, el miércoles 14 de marzo de 2007, última reforma 7 de marzo de 2012.
- Código Penal para el Estado de Hidalgo, publicado el 9 de junio de 1990, última reforma 15 de agosto de 2016.
- Código Penal para el Estado de México, publicado 3 de septiembre de 1999, última reforma 8 de septiembre de 2017.
- Código Penal para el Estado de Michoacán de Ocampo, publicado el 17 de diciembre de 2014, última reforma 25 de septiembre de 2015.
- Código Penal para el Estado de Nuevo León, publicado el 26 de marzo de 1990, última reforma 3 de julio de 2017.
- Código Penal para el Estado de Querétaro, publicado el 23 de julio de 1987, última reforma 01 de septiembre de 2017.
- Código Penal para el Estado de Sinaloa, publicado el 28 de octubre de 1992, última reforma 28 de diciembre de 2016.
- Código Penal para el Estado libre y soberano de Puebla, publicado el 23 de diciembre de 1986, última reforma 31 de marzo de 2017.
- Código Penal Federal, publicado en Diario Oficial de la Federación el 14 de agosto de 1931, última reforma 26 de junio de 2017.

• Código Penal para el Estado libre y soberano de Baja California Sur, publicado el 30 de noviembre de 2014, última reforma 17 de julio de 2017.
• Código Penal para el Estado libre y soberano de Quintana Roo, publicado el 11 de julio de 1979, última reforma 19 de julio de 2017.
• Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 5 de febrero de 1917, última reforma 15 de septiembre de 2017.
• Convenio Sobre la Ciberdelincuencia, Consejo Europeo, 23 de noviembre de 2001, Budapest.
• Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia, 28 de mayo de 2014.
• Legislación Penal para el Estado de Aguascalientes, publicada en el Periódico Oficial del Estado el 21 de julio de 2003, última reforma 25 de marzo de 2013.
• Ley 26.388, modificación al Código Penal Argentino, publicada 24 de junio de 2008.
• Ley 19223, Ministerio de Justicia Chileno, publicada el 7 de junio de 1993, versión única.
• Ley 20009, Ministerio de Justicia Chileno, publicada el 1 de abril de 2005, versión única.
• Ley de Instituciones de Crédito, publicada el 18 de julio de 1990, última reforma 10 de enero de 2014.
• Ley de Instituciones de seguros y fianzas, publicada el 4 de abril de 201, última reforma 10 de enero de 2014.
• Ley de la Propiedad Industrial, publicada en el Diario Oficial de la Federación el 27 de junio de 1991, última reforma 01 de junio de 2016.
• Ley Federal contra la Delincuencia Organizada, publicada el 7 de noviembre de 2011, última reforma 7 de abril de 2017.
• Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010.
• Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, publicada en el Diario Oficial de la Federación el 17 de octubre de 2012.

• Ley General de Títulos y Operaciones de Crédito, publicada en Diario Oficial de la Federación el 27 de agosto de 1932, última reforma 13 de junio de 2014.
• Ley Orgánica 10/1995, 23 de noviembre, del Código Penal (España), última reforma 3 de noviembre de 2016.
• Ley para la Transparencia y Ordenamiento de los Servicios Financieros.
• Ley para regular las Sociedades de Información Crediticia, publicada en el DOF el 15 de enero de 2002, última reforma 10 de enero de 2014.