FORMATO 5

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

LICENCIATURA EN DERECHO

TRABAJO POR ESCRITO QUE

PRESENTA:

EVA LOPEZ CRUZ

TEMA DEL TRABAJO:

"FRAUDE ELECTRÓNICO A TRAVÉS DE LA BANCA"

EN LA MODALIDAD DE "SEMINARIO DE TITULACIÓN COLECTIVA"

PARA OBTENER EL TÍTULO DE:
LICENCIADO EN DERECHO

FES Aragón

MÉXICO, ARAGÓN, MAYO DE 2008

Agradezco por ser parte de la UNAM, para mí es mas que una escuela ha sido mi segunda casa en ella me he formado como profesionista y persona.

Como testimonio de mi gratitud a mis profesores por su apoyo, aliento y estimulo mismos que posibilitaron la conquista de esta meta: Mi formación profesional con Admiración y Respeto

Como un testimonio de cariño y eterno agradecimiento por mi existencia, valores morales y formación profesional.
por que sin escatimar esfuerzo alguno, ha sacrificado gran parte de su vida y porque nunca podré pagar todos sus desvelos ni aun con las riquezas mas grandes del mundo. Por lo que soy y por todo el tiempo que les robe pensando en mi…
Gracias por ser mis Padres.

Con amor y respeto.

Rodolfo López Cruz ✝ he llegado al final de este camino hermanito y en mi han quedado marcadas huellas profundas de este recorrido. Tu aliento y tus consejos dieron resultados. Mi Novio con su paciencia, trabajo y esfuerzo. Mis amigos que me apoyaron y confiaron siempre en mí.
Gracias a todos

Con cariño

FRAUDE ELECTRÓNICO A TRAVÉS DE LA BANCA

PAG.

INTRODUCCIÓN

FRAUDE ELECTRÓNICO A TRAVÉS DE LA BANCA

Es menester mencionar que en la actualidad dependemos cada vez más de las redes electrónicas por lo que somos más vulnerables.

El uso de las computadoras y su interconexión ha dado lugar a un fenómeno de nuevas dimensiones; el delito instrumentado mediante el uso del computador, si bien no existe aún una medida exacta de la importancia de estas transgresiones, es probable que su incidencia se actúe con la expansión del uso de las computadoras y redes.

Por lo que respecta a México **el Fraude Electrónico** a través de la Banca ha suscitado una perdida considerable en donde los defraudadores se valen de diversos programas mismos que se abordaran en el Primer Capitulo como es la **Técnica de Salami**, que es robo automatizado de pequeñas cantidades de bienes (generalmente de dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace exactamente difícil su detección si de una cuenta de varios miles de pesos se roban unos centavos nadie va a darse cuenta de ello.

Su uso mas habitual es el sistema bancario, sin embargo como en una red con requerimientos de seguridad es posible que haya ordenadores dedicados a la contabilidad, facturación de un departamento o gestión de nominas del personal esto es una potencial amenaza al software encargado de estas tareas.

Por otro lado esta *phishing* (del ingles fishing- pescar) a la suplantación de identidad (en Internet, pero también por teléfono) que es el robo de identidad electrónico para tener acceso a los servicios privados y el *pharming,* (que se pronuncia como “farming”). Los pharmers constituye otra forma de fraude en línea, muy similar a su pariente, el *phishing,* utilizan los mismos sitios *Web* falsos y el robo de información confidencial para perpetrar estafas en línea, pero, en muchos sentidos, es mucho más difícil detectarlos

Por lo regular este tipo de delito son realizados por aquellas personas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es los sujetos activo tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible o bien son hábiles en el uso de los sistemas informáticos, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delito.

El Segundo Capitulo habla de las Legislación Nacional que ha adopta el Fraude Electrónico como lo contempla el Código Penal Federal en su Capitulo de Acceso Ilícito a Sistemas y Equipos de Informática en su articulo 211 Bis, el Código Penal para e Distrito Federal en su articulo 89 y 231 fracción XIV donde se establece el Fraude Electrónico y el Código Penal del Estado de Sinaloa que contempla en un capitulo los Delitos Informáticos.

El trabajo que se presenta consta de dos capítulos para su estudio y así poder llegar a una probable solución mediante el método inductivo y deductivo que se utilizara.

FRAUDE ELECTRÓNICO A TRAVÉS DE LA BANCA

CAPÍTULO PRIMERO

Marco Conceptual

1.1Legislacion Internacional que estipula el Fraude Electrónico

a) Alemania

"Este Estado sanciono en 1986 La Ley contra la Criminalidad Económica que contempla los siguientes delitos a) Espionaje de datos b) fraude informático c) Alteración de datos y d) Sabotaje informático",[9]

b) Austria

La Ley de reforma del Código Penal, promulgada el 22 de diciembre de 1987, en el artículo 148, sanciona aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de elaboración automática de datos a través de la confección del programa, por la introducción, cancelación, o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas.

c) Francia

En enero de 1998, este Estado promulgo la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multa de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique dato

Asimismo esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerado los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 262-4 también incluye este

---

[9] TÉLLEZ VALDEZ, Julio, Derecho Informático, segunda edición, Mc Graw, México, 1998. pag. 231

tipo penal una conducta intencional y a sabiendas de vulnerar los derechos de terceros, en forma directa o indirecta haya introducido datos en un sistema de procesamiento automatizado o haya suprimido modificado los datos que este contiene o sus modos de procesamiento o de transmisión.

d) España

El artículo 264-2, del Nuevo Código Penal de España, establece que se aplicará

La pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

e) Italia

En un Estado importante tradición criminalista, como es Italia donde se encuentran tipificados en su Código Penal los siguientes delitos:

Acceso abusivo, se configura exclusivamente en casos de sistemas informáticos y telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de *hardware)* que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso aquel sólo a personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años previniendo agraviantes.

1) Fraude Informático, cuando por medio de artificios o engaños, induciendo a otro error, alguien procura para sí o para otros un injusto beneficio, ocasionando daño a otro, también se entiende como tal la alteración del funcionamiento de sistemas informáticos o telemáticos o la intervención abusiva sobre datos, informaciones o programas en ellos, cuando se procure

una ventaja injusta, causando daño a otro. “La punibilidad de este tipo es de meses a tres años de prisión, más una multa considerable”.[10]

1.2 Fraude.

De acuerdo a Mariano Jiménez Huerta, “el delito de fraude es hoy lo mas frecuente y rutilante estrella de la constelación forjada por los defraudadores patrimoniales”. Sus primeras manifestaciones legislativas, hallándose de las disposiciones estatuidas por los pueblos antiguos para tutelar la honestidad de las relaciones comerciales y evitar en ellos las alteraciones de cantidades, pesas y medidas y la exigencia de un precio mayor del debido. El Código de Manú castigaba al que vendía grano malo por bueno, cosa vil por fragante cristal de roca colorada por piedra preciosa, hilo de algodón por hilo de seda, hierro por plata etc. El Código de Hamurabit sancionaba las falsificaciones de pesas y medidas; las leyes Hebraicas a los comerciantes ávidos de abusar de los compradores necesitados, y el Coran a los que se aprovechaban de las condiciones del comprador para venderle, o al vendedor, para comprarle, a precio respectivamente mayor o menor del justo valor de la cosa o hacia un uso de cualquier artificio dirigido o acrecentar el aparente valor de la mercancía, en el Derecho Romano para integrar algunos compendiosos y difusos crímenes como el furtum, falsum y stellionatus, el desarrollo factico de aquel delito de su completa estructuracion solo se alcanza cuando a partir de la mitad de siglo XIX, el comercio jurídico y el trafico mercantil se desarrollan intensamente en las relaciones humanas.

“Ahora bien la verdadera esencia antijurídica del delito de fraude, radica en los engaños, ardides, artificios y maquinaciones de que se vale el sujeto

---

[10] **CORREA M. Carlos, Derecho Informático, octava edición, Buenos Aires, Argentina, 1987. pag. 225**

activo para sumergir en un error a otro y determinarle a realizar un acto de disposición patrimonial".[11]

1.3 Fraude Informático

Son los actos fruto de intencionalidad realizados con la voluntad de obtener un beneficio propio y, si es posible, provocar un perjuicio a alguien. Así se puede hablar también de un tipo de fraude informático no intencionado, producto de un error humano al utilizar un sistema informático o por un defecto del hardware o del software. Este tipo de fraude es conocido como error informático puede no haber un beneficio directo para quien causa el funcionamiento erróneo del sistema informático, pero si un perjuicio a los otros usuarios a los propietarios del sistema.[12]

1.4. Presupuestos del Delito

"Manzini crea la doctrina del presupuesto del delito elementos jurídicos, positivos o negativos, anteriores a la ejecución del hecho y dependiendo de la existencia o inexistencia de estos condicionada la configuración del delito de que se trate. Se puede definir que los presupuestos del delito como aquellos antecedentes jurídicos necesarios para la realización de la conducta o hecho descrito por el tipo penal, cuya existencia depende el delito. [13]

1.4.2. Sujeto Activo

Los Códigos Clásicos decían que por medio de la intención de las circunstancias, agravantes y atenuantes, provenían a la determinación de la pena en función de la personalidad del delincuente. En este mismo sentido los positivistas establecieron que no hay delito sino delincuentes y no hay delincuentes sino hombres, por lo que la teoría del médico César Lombroso

---

[11] **JIMÉNEZ HUERTA, Mariano, Derecho Penal Mexicano, décima cuarta edición, Porrúa, México, 1984**

[12] **GONZÁLEZ DE LA VEGA, Francisco, Derecho Penal Mexicano, cuarta edición, México, 1996**

[13] **LÓPEZ BETANCOURT. Eduardo, Teoría del Delito, quinta edición, Porrúa. México, 1999**

quien en base a un estudio de investigación de internos en establecimientos penitenciarios estimo que había descubierto al “delincuente nato” el cual era un individuo con determinadas anomalías somáticas y psíquicas tendientes a convertirse en delincuentes aun en el caso de encontrarse en un medio favorable.

Ahora analizando y transportando todo esto a nuestro tema, el sujeto activo, que comete delitos informáticos, son aquellas que poseen ciertas características que aun no presenta el denominador común de los delincuentes en lo general son personas que no poseen antecedentes delictivos, por lo general son personas del sexo masculino, actúan de forma individual, que por su situación laboral se encuentran en lugares estratégicos, donde maneja información de carácter sensible, dentro de las organizaciones, las personas que cometen el delito de fraude han sido destacadas en su ámbito laboral como trabajadoras y motivadas.

1.4.3. Sujeto Pasivo

Es aquella persona que sufre directamente la acción, es sobre quien recae todos los actos materiales utilizados en la realización del ilícito el titular del derecho dañado o puesto en peligro y en caso del fraude electrónico por la técnica de salami, la victima es aquella persona que se esta dañando en su patrimonio.

1.4.4. Objeto Material

Este es la persona o cosa a quien le recae la ejecución del delito, axial puede ser sujeto activo o pasivo, puede definirse el objeto material como realidad corpórea e incorpórea susceptible de ser materia considerada como bien jurídico, como se menciono anteriormente sigue siendo el patrimonio.

1.4.5. Objeto Jurídico

Es el bien jurídico tutelado es decir, el bien o derecho que es protegido por las leyes penales el cual puede ser la vida, la integridad corporal, la libertad sexual, la posesión o ambas, se puede citar como ejemplo el objeto

material del fraude por la técnica de salami , es el patrimonio, la propiedad la posesión o ambas.

1.5. Elementos del Delito

Se hará referencia los elementos positivos que son aquellos elementos que describe a cada uno de los delitos

1.5.1. Conducta

Es el primer elemento positivo que se define como el comportamiento humano voluntario positivo o negativo encaminado a un propósito, lo que significa que solo los seres humanos pueden cometer conductas positivas o negativas. En el caso de la técnica de salami, la persona que realiza el redondeo hacia abajo, con la intención de trasferirla a otro cuenta apócrifa.

1.5.2. Tipicidad

Es el segundo elemento positivo que se define como la conducta que conlleva una acción u omisión que se ajusta a los presupuestos detalladamente establecidos como delito o falta dentro de un cuerpo legal. Esto quiere decir que, para que una conducta sea típica, debe constar específica y detalladamente como delito o falta dentro de un código. **Antijuridicidad**

Es tercer elemento positivo Se le define como aquel que posee un hecho típico que es contrario a las normas del Derecho en general, es decir, no sólo al ordenamiento penal.

La antijuridicidad supone que la conducta que se ha realizado está prohibida por el ordenamiento jurídico; en otras palabras, que dicho comportamiento es contrario a Derecho.

1.5.4. Imputabilidad

Es la capacidad de querer y entender, en el campo del derecho penal, querer es estar en condiciones de aceptar o realizar algo voluntariamente y

entender es la capacidad mental y edad biológica para desplegar esa decisión.

1.5.5. Culpabilidad

Es la desobediencia consiente y voluntaria y de la que una esta obligada a respondes a una ley, la cual podría ser de acuerdo a la ley el dolo o culpa

Dolo “es la producción del resultado típicamente antijurídico con la conciencia de que se esta quebrantando el deber, con conocimiento de las circunstancias de hecho y del curso esencial de la relación de causalidad existente entre las manifestaciones humanas y el cambio en el mundo exterior, con la voluntad de realizar la acción u con representación del resultado que se requiere”.[14]

Culpa. Es la voluntad omisión de diligencia en calcular las consecuencias posibles y previsibles del propio hecho. A esta teoría se le han formulado diversas criticas, lo que no implica que no se reconozca que el concepto de previsibilidad juega un papel de importancia en la culpa, sino tan solo que ese elemento no puede considerarse como suficiente para servirle de fundamento, dado que en otras razones, aun siendo previsible el resultado, puede no darse la culpa, si el sujeto ha actuado con la debida diligencia y prudencia.

1.5.6. Punibilidad

Es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran señaladas en nuestro Código Penal.
Cuello Calón, considera que la punibilidad no es más que un elemento de la

---

[14] **DE PINA VARA, Rafael, Diccionario de Derecho, octava edición, Porrúa, México, 1984**

tipicidad, pues el hecho de estar la acción conminada con una pena, constituye un elemento del tipo delictivo.

1.6. La Banca

Es el comercio del dinero, basado en la captación de capitales ajenos y su inversión en operaciones de crédito y en la creación y manejo de signos representativos de dinero, o sea el tráfico del dinero y el crédito. Se conceptúan operaciones pasivas de banca las de apertura y seguimiento de cuentas corrientes, cuentas de ahorro, custodia de valores, etc.; y activas, las crediticias, como el descuento de efectos de comercio, pagarés y la concesión de créditos y préstamos con garantía, anticipas con caución o garantía prendaría en metales preciosos, mercaderías, títulos mobiliarios, etc.

Las principales operaciones financieras de los bancos son la emisión de billetes y de obligaciones, cédulas y acciones; la compraventa de divisas, monedas, títulos mobiliarios y giros; el lanzamiento y colocación de empréstitos y emisiones; la fundación y financiación de empresas; la constitución de sindicatos financieros; los arbitrajes y las financiaciones en general.

Existe gran diversidad en la constitución y actividades de los bancos: unos son formados con capital privado, otros por acciones, otros en forma cooperativa, y otros con capital del Estado o de otra corporación pública y con capital privado; algunos se dedican a todas las operaciones ya enumeradas y otros solamente a ciertas especialidades. Existen bancos hipotecarios, de crédito agrícola, de formación de capitales, de construcción de viviendas, de colonización, de préstamos, bancos populares, de crédito cooperativo, etc.

1.7 Técnica de Salami. Se caracteriza “Por ser rodajas muy finas” se utiliza para desviar pequeñas cantidades de bienes generalmente dinero de una fuente una gran cantidad de los mismos: de la misma forma que en un salami se cortan pequeñas rodajas sin que en el total sufra una reducción

considerable, un programa salami roba pequeñas cantidades de dinero, de forma que su acción pasa inadvertida. Aunque su efecto es especialmente grave en entornos bancarios y no en sistemas habituales, existes diversos programas salami en donde ataca equipos Uníx dedicados a operaciones financieras, como la gestión de nominas de personal o la asignación de becas.

El principal problema de los programas salami es que son extremadamente difíciles de detectar, y sólo una compleja auditoria de cuentas puede sacar a la luz estos fraudes. Si un programador es lo suficientemente inteligible como para insertar *malware* de este tipo en los sistemas de un banco para el cual trabaja “si se trata de un atacante externo la posibilidad de ataque sería casi despreciable, seguramente conoce todo de dicho banco, de forma que no será difícil desviar fondos a cuentas que no son la suya, comprobar si se sobrepasa un cierto umbral en dichas cuentas”.

Umbral a partir el cual el banco se interesaría por el propietario de la cuenta o incluso a utilizar nombres falsos o cuentas externas a las que desviar dinero. Contra esto, una de las pocas soluciones consiste en vigilar de cerca las cuentas de los empleados y sus allegados , así como estar atentos a posibles cambios en su modo de vida: un coche de lujo de una persona con un sueldo normal, viajes caros, demasiados ostentaciones pueden ser signo de un fraude.

Un caso particular de programa de salami lo constituyen los programas de redondeo hacia abajo o round *down.* Este fraude consiste en aprovechar cálculos de los sistemas bancarios que obtienen cantidades de dinero mas pequeñas que la moneda de menor valor (en el caso de España cantidades de céntimos) por ejemplo que alguien tiene ingresadas 123.523 pesetas a un interés del 2`5 % los créditos le reditarán un total de 3088`075 pesetas que automáticamente para el banco se transformaran en 3088. si esos 7`5 céntimos se acumulan en otro cálculo con cantidades igual de despreciables,

se llegara tarde o temprano a un punto en el que la cantidad total de dinero sea lo suficientemente para un atacante dispuesto aprovechar la situación.[15]

1.8. Phishing

Se conoce como *Phishing* (del ingles fishing- pescar) a la suplantación de identidad (en Internet, pero también por teléfono) que persigue apropiarse de datos confidenciales de los usuarios. En la Red se utiliza el envió masivo de correos electrónicos que simulan proceder de Entidades de prestigio y apremian al ínter nauta a actualizar datos personales (nombres de usuario y contraseña de cuentas bancarias, números de tarjeta de crédito, etc.) a través de una pagina que imita a la original. Al introducir los datos en la página falsa, estos son pescados por los ciberdelincuentes para utilizarlos de forma fraudulenta.

Se trata de una forma de *spam (*correos electrónicos no deseados) especialmente perniciosa, pues no solo satura los buzones de basura, sino que pone en peligro la integridad de la información sensible del usuario con graves consecuencias. La proliferación de estos mensajes fraudulentos obliga a estar alerta y, de entrada, a tener presente que no se debe ofrecer datos personales que sean solicitados mediante el correo electrónico sin, al menos, realizar una comprobación telefónica. El mecanismo de este *timo on oline* el desarrollo es el siguiente:

El usuario recibe un email de un banco, entidad financiera o tienda de Internet en el que se le explica que motivos de seguridad, mantenimiento, mejora en el servicio, confirmación de identidad o cualquier otro, debe de actualizar los datos de su cuenta. El mensaje imita exactamente el diseño (logotipo, firma, etc.) utilizado por la entidad para comunicarse con sus clientes.

[En Línea]. Disponible:
[15] **htpp:/seguridadinternet2.ulsa.mx/congrsos/2003/cudi2/legislación-fullpdfgz. 06 de Noviembre de 2006 13:00 PM.**

El mensaje puede integrar un formulario para enviar los datos requeridos, aunque lo más habitual es que incluya un enlace a una página donde actualizar la información personal.

Esta pagina es exactamente igual que la legitima de la entidad algo sencillo copiando el código fuente (HTML) y su dirección (URL) es parecida e incluso puede ser idéntica gracias a un fallo de algunos navegadores.

Si se rellenan y se envían los datos de la página caerán directamente en manos del estafador, quien puede utilizar la identidad de la victima para operar en Internet (Ver imagen 1, 2, 3, 4, y 5).[16]

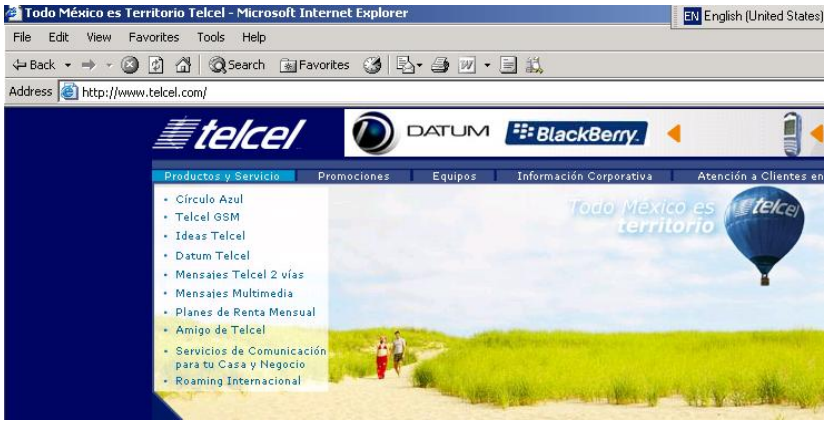
Un ejemplo claro es:

Imagen 1

[16] [En Linea.] Disponible: **htt//www.revista.unam.mx/vol3/num2/art3/ind.htm/#219. 23 de Febrero de 2007. 14:00PM.**

Página Oficial: http://www.telcel.com/

Imagen 2



Página Apócrifa http://www.recargatelcel.com/

Imagen 3

El robo de identidad bancaria se presenta en Nueva Recarga:

Imagen 4

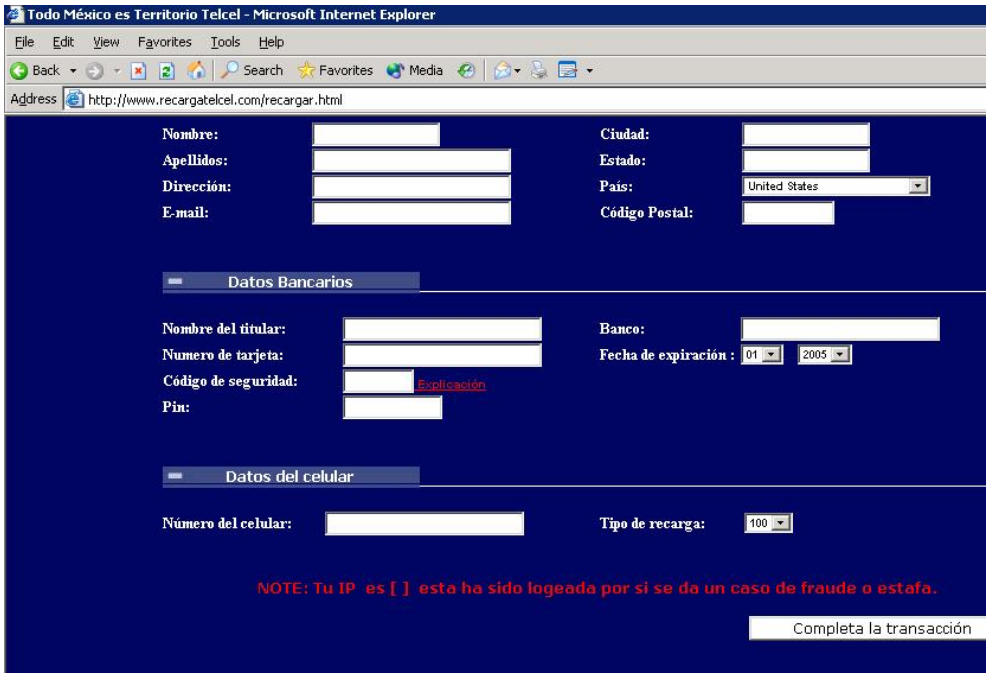


Imagen 5

1.9. El Pharming

El *pharming* (que se pronuncia como “farming”) constituye otra forma de fraude en línea, muy similar a su pariente, el phishing. Los pharmers (los autores de los fraudes basados en esta técnica del pharming) utilizan los mismos sitios Web falsos y el robo de información confidencial para perpetrar estafas en línea, pero, en muchos sentidos, es mucho más difícil detectarlos, ya que no necesitan que la víctima acepte un mensaje. En lugar de depender por completo de que los usuarios hagan clic en los vínculos engañosos que se incluyen en mensajes de correo electrónico falsos, el *pharming* redirige a sus víctimas al sitio Web falso, incluso si escriben correctamente la dirección Web de su banco o de otro servicio en línea en el explorador de Internet.

Para redirigir a sus víctimas, los *pharmers* utilizan varias estrategias. El primer método, que ha conferido a esta actividad el nombre de *pharming*, es en realidad un antiguo tipo de ataque denominado envenenamiento de la caché del DNS. El envenenamiento de la caché del DNS es un ataque dirigido al sistema de nombres de Internet que permite a los usuarios introducir nombres con un significado para los sitios Web

(www.mibanco.com), en lugar de series de números más difíciles de recordar (192.168.1.1). El sistema de nombres se basa en los servidores DNS para efectuar la conversión de los nombres de los sitios Web basados en letras, que son fáciles de recordar por parte de los usuarios, en dígitos comprensibles por los equipos para conducir a los usuarios al sitio Web de su elección. Cuando un *pharmer* logra lanzar un ataque de envenenamiento de la caché del DNS con éxito, lo que de hecho consigue es modificar las normas de circulación del tráfico en una sección completa de Internet. Las posibles y amplias repercusiones que conlleva el hecho de redirigir a una importante cantidad de víctimas desprevenidas a una serie de sitios Web falsos y hostiles ha dado el nombre de *pharmers* a esta categoría de estafadores. Los *phishing* lanzan un par de líneas al agua y esperan hasta ver quién pica el anzuelo. Los *pharmers* son criminales cibernéticos que intentan capturar a sus víctimas en Internet a una escala nunca vista.

Ejemplo de pharming

Uno de los primeros ataques de *pharming* de los que se tiene constancia se produjo a principios de 2005. En lugar de aprovecharse de una falla del software, parece ser que el atacante engañó al personal de una empresa proveedora de servidos de Internet para que transfiriera una ubicación de un lugar a otro. Una vez que la dirección original se hubo transferido a la nueva dirección, el atacante logró, de hecho, "secuestrar" el sitio Web e impedir el acceso al sitio auténtico, lo que puso a la empresa víctima en una situación complicada, con repercusiones negativas para su negocio. Semanas después, se produjo un ataque de *pharming* con consecuencias todavía más nefastas. Valiéndose de una falla del software, los *pharmers* consiguieron cambiar cientos de nombres de dominio legítimos por los de sitios Web hostiles y falsos. Se produjeron tres oleadas de ataques: en las dos primeras, se intentó cargar *spyware y adware* en los equipos atacados y, en la tercera, se intentó conducir a los usuarios a un sitio Web donde se podían

CAPITULO SEGUNDO

Planteamiento del problema, la propuesta y su desarrollo

Legislaciones que adopto los Delitos Informáticos

2.1. Código Penal para el Distrito Federal

Articulo 89 (Requisitos para la procedencia de la suspensión). El juez o el Tribunal, en su caso, al dictar sentencia condenatoria, suspenderán motivadamente la ejecución de las penas, a petición de parte o de oficio, si concurren los requisitos siguientes:
I. Que la duración de la pena impuesta no exceda de cinco años de prisión;

Artículo 230. Al que por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:

I. De veinticinco a setenta y cinco días multa, cuando el valor de lo defraudado no exceda de cincuenta veces el salario mínimo, o no sea posible determinar su valor;

II. Prisión de cuatro meses a dos años seis meses y de setenta y cinco a doscientos días multa, cuando el valor de lo defraudado exceda de cincuenta pero no de quinientas veces el salario mínimo;

III. Prisión de dos años seis meses a cuatro años y de doscientos a quinientos días multa, cuando el valor de lo defraudado exceda de quinientas pero no de cinco mil veces el salario mínimo;

IV. Prisión de cuatro a seis años y de quinientos a ochocientos días multa, cuando el valor de lo defraudado exceda de cinco mil pero no de diez mil veces el salario mínimo; y

V. Prisión de seis a once años y de ochocientos a mil doscientos días multa, cuando el valor de lo defraudado exceda de diez mil veces el salario mínimo.

Cuando el delito se cometa en contra de dos o más personas, se impondrá además las dos terceras partes de las penas previstas en las fracciones anteriores.

Artículo 231. Se impondrán las penas previstas en el artículo anterior, a quien:

XIV. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institución.

2.2 CODIGO PENAL FEDERAL

ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Artículo 400-bis. Se impondrá de cinco a quince años de prisión y de mil a cinco mil días multa al que por sí o por interpósita persona realice cualquiera de las siguientes conductas: adquiera, enajene, administre, custodie, cambie, deposite, dé en garantía, invierta, transporte o transfiera, dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, con conocimiento de que proceden o representan el producto de una actividad ilícita, con alguno de los siguientes propósitos: ocultar o pretender ocultar, encubrir o impedir conocer el origen, localización, destino o propiedad de dichos recursos, derechos o bienes o alentar alguna actividad ilícita.

La misma pena se aplicará a los empleados y funcionarios de las instituciones que integran el sistema financiero, que dolosamente presten ayuda o auxilien a otro para la comisión de las conductas previstas en el párrafo anterior, sin perjuicio de los procedimientos y sanciones que correspondan conforme a la legislación financiera vigente.

La pena prevista en el primer párrafo será aumentada en una mitad, cuando la conducta ilícita se cometa por servidores públicos encargados de prevenir, denunciar, investigar o juzgar la comisión de delitos. En este caso, se impondrá a dichos servidores públicos, además, inhabilitación para desempeñar empleo, cargo o comisión públicos hasta por un tiempo igual al de la pena de prisión impuesta.

En caso de conductas previstas en este artículo, 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 dicha Secretaría, en ejercicio de sus facultades de fiscalización, encuentre elementos que permitan presumir la comisión de los delitos referidos en el párrafo anterior, deberá ejercer respecto de los mismos las facultades de comprobación que le confieren las leyes y, en su caso, denunciar hechos que probablemente puedan constituir dicho ilícito.

Para efectos de este artículo se entiende que son producto de una actividad ilícita, los recursos, derechos o bienes de cualquier naturaleza, cuando existan indicios fundados o certeza de que provienen directa o indirectamente, o representan las ganancias derivadas de la comisión de algún delito y no pueda acreditarse su legitima procedencia.

Para los mismos efectos, el sistema financiero se encuentra integrado por las instituciones de crédito, de seguros y de fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondos de retiro y cualquier otro intermediario financiero o cambiario.

2.3. Código Penal para el Estado de Sinaloa

CAPÍTULO V

DELITO INFORMÁTICO

ARTÍCULO 217. Comete delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistema de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red.

Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

2.4. POSICIÓN PERSONAL

El Fraude Electrónico a través de la Banca es considerado un gran problema a nivel mundial, por que no se tienen las medidas de seguridad eficientes de la misma forma no hay una Legislación adecuada y por lo que respeta a México la tecnología es muy baja cuando tiene una medida de seguridad adecuada los ciberdelincuentes ya avanzaron a un 90% en la actualidad se ha presentado tres clases de fenómenos en la Banca como ya se hizo referencia por ejemplo la Técnica de Salami que consiste en por ser rodajas muy finas se utiliza para desviar pequeñas cantidades de dinero de una forma que pasa inadvertida de la misma forma que se corta un salami en pequeñas rodajas sin que el total sufra unas una reducción considerable se origina en entornos bancarios, existen diversos programas salami como la Gestión de Nominas del Personal, Asignación de Becas, Programas de Redondeo hacia Abajo.

Hay que considerar que en México no se tiene ningún antecedente de esta Técnica según la Lic. Conciliadora Imelda Jiménez Torres de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSET) misma que es el Organismo Descentralizado de la Secretaria de Hacienda, encargada de velar en forma integral por los intereses y derechos de los usuarios de servicios financieros facultada para orientarlos, asesorarlos y atender sus quejas, así como fomentar la cultura financiera.

Cabe mencionar que si bien no existe algún antecedente de la Técnica de Salami considero que lo vivimos a diario encuadrando todo esto al ejemplo antes citado, una referencia muy usual en México podría ser los centavos que se pierden en cado retiro que se hace en el cajero o las donaciones en las cuales se hace el redondeo hacia arriba mas sin embargo jamás se haría una denuncia ante la CONDUSET por unos centavos.

Ahora a mi parecer yo propondría que debería haber un capitulo de Delitos Informáticos en donde se establezca, todos los delitos que ocurren por medio de red ya se esta hablando una Asociación Delictuosa o la misma gente que labora en la Sucursales Bancarias, que si los bancos no cambian sus medidas de seguridad de nada sirve que exista una ley si nunca se va

encontrar a la personas que realiza este delito, una de las medidas de seguridad que el banco debería tener en caso de que se trate de un Fraude es la obligación de promocionar las cuentas donde se transfirió el dinero así como los datos de conexión con los que accedió al sistema (dirección IP fecha hora y usuario) que es difícil ya que cada persona que entra a la red tiene una dirección IP diferente, pero se podría hacer ya que con estos datos se conoce fácilmente el proveedor de Internet (Telmex, Cablevisión etc.) y este a su vez podría proporcionar las direcciones físicas de donde fue la conexión, también seria necesario el monitoreo diario de los DNS en búsqueda de registros que concuerden con los patrones de alerta, la búsqueda concordancias entre patrones de alerta y resultados del monitoreo en tiempo real, así como la búsqueda de concordancias en los textos de las paginas de inicio de los sitios de Internet, y así una infinidad de medios de seguridad, pero lo que considero conveniente que todos los usuarios que utilicen la red se les debería de dar una cultura para poder protegerse que si bien existen la CONDUSET no tiene una gran difusión para todos los ciudadanos que somos en México solo con este procedimiento podría desparecer poco a poco el Phishing y Pharming.

CONCLUSIONES

PRIMERA: Al analizar el fenómeno del Fraude Electrónico se pudo observar que no se tiene un capitulo especial de Los Delitos Informáticos en donde se establezca los delitos que se pueden cometer a través de la red.

SEGUNDA: Al observar que las medidas de seguridad que tiene los bancos considero que son ineficaces ya que cualquiera puede ser victima de este delito.

TERCERA: Es cierto que el personal bancario se pueda aprovechar de su situación laboral para poder manejar información interna y a si cometer este tipo de delito.

CUARTA: Es falso que el usuario sea el que comete el error ya que debería existir un medio de seguridad para que no puedan clonar las paginas oficiales, solo en el caso del pharming cuando se esta navegando en la red.

QUINTA: Es cierto que exista la CONDUSET quien promueve una cultura para los usuarios pero no existe una difusión apropiada para que todos los usuario bancarios se vean beneficiados.

.

FUENTES CONSULTADAS

1.- CORREA M. Carlos, Derecho Informático, octava edición, Buenos Aires, Argentina, 1987.

2.- GONZÁLEZ DE LA VEGA, Francisco, Derecho Penal Mexicano, cuarta edición, México, 1996

3.-. JIMÉNEZ HUERTA, Mariano, Derecho Penal Mexicano, décima cuarta edición, Porrúa, México, 1984

4.- DE PINA VARA, Rafael, Diccionario de Derecho, octava edición, Porrúa, México, 1984

5.-LÓPEZ BETANCOURT. Eduardo, Teoría del Delito, quinta edición, Porrúa. México, 1999

6.-SUÁREZ IÑIGUEZ, Enrique, Como hacer una Tesis, tercera edición, Trillas, México, 2000.

7.-TÉLLEZ VALDEZ, Julio, Derecho Informático, segunda edición, Mc Graw, México, 1998.

FUENTES ELECTRÓNICA

1.-htt//.es.tldp.org/Manuales-LUCAS/doc-unixsec/unixsec-htm/node8/.html/

2.-htpp:/seguridadinternet2.ulsa.mx/congrsos/2003/cudi2/legislación-fullpdf

3.-htt//www.revista.unam.mx/vol3/num2/art3/ind.htm/#219.

LEGISLACIONES

1.-Código Penal para el Distrito Federal

Agenda Penal del Distrito Federal, Edición Primera, ISEF, México, 2008.

2.-Código Penal Federal.

Agenda Penal del Distrito Federal, Edición Primera, ISEF, México, 2008.

3.-Código Penal para el Estado de Sinaloa.

Código Penal de Sinaloa, Edición Primera, Sista, México, 2008.