INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO

GERENCIA DE CAPITAL HUMANO

POSGRADOS

"SOLUCIÓN DE ESTRATEGIA EMPRESARIAL

DOMINIOS DE NIVEL SUPERIOR PARA MITIGAR EL FRAUDE ELECTRÓNICO (PHISHING) EN LA BANCA ELECTRÓNICA POR INTERNET"

SOLUCIÓN ESTRATEGICA EMPRESARIAL

Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

Presenta:

Miguel Ángel Camacho Castillo

Asesor:

Dr. Alberto Nava Garcés

Ciudad de México, agosto, 2016.

INFOTEC
POSGRADOS

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 16 de Agosto de 2016

La Gerencia de Capital Humano/Gerencia de Investigación hacen constar que el proyecto terminal titulado:

Solución De Estrategia Empresarial Dominios De Nivel Superior Para Mitigar El Fraude Electrónico (Phishing) En La Banca Electrónica Por Internet

Desarrollada por el alumno

Miguel Ángel

Camacho

Castillo

Desarrollado bajo la asesoría de:

Dr. Alberto Nava Garcés

Ha sido revisada y aprobada por los profesores investigadores:

Dr. Federico César Lefranc Weegan

Dra. Olivia Andrea Mendoza Enríquez

Mtra. Evelyn Téllez Carvajal

Quienes han depositado en estas gerencias en su oportunidad sus reflexiones y comentarios que han sido atendidos e integrados en su totalidad por el alumno a la nueva versión escrita del proyecto integrado revisado; siendo corroborados por los mismos revisores, quienes emitieron sus votos aprobatorios por separado que obran en el expediente de investigación correspondiente.

Por lo cual, se expide la presente autorización para la impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Patricia Ávila Muñoz
Encargada del Despacho de la Gerencia de Capital Humano

Dra. Olivia Andrea Mendoza
Coordinador del posgrado en Derecho de las Tecnologías de la Información y Comunicación

*** Anexar la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.**

A mi esposa Adriana, la que con paciencia y amor apoya todos mis proyectos, te amo cielo.

A mis hijos Vannia y Miguel Ángel, a quiénes les he quitado tiempo, pero quiero que sepan que son la razón de mi vida.

A María del Carmen, mi mamá quien me dio la vida y siempre está atenta y celebra mis logros, uno más para que te sientas orgullosa.

A la memoria de Genaro Camacho, mi papá que se sentía orgulloso al saber que inicie este proyecto, pero Dios lo llevó a su lado. Te quiero mucho.

Tabla de contenido

Resumen

El presente estudio busca poner de manifiesto el aprovechamiento de la tecnología para realizar el delito de fraude, particularmente a través de Internet, precisando el comportamiento de los defraudares que utilizan medios electrónicos con los usuarios de la red que realizan operaciones financieras a través de los servicios de banca electrónica. El presente análisis pretende concientizar a los usuarios de banca electrónica por Internet para que tomen en consideración elementos técnicos del portal del banco que les presta servicios de banca, así como hacer una propuesta a las instituciones financieras para que inviertan en la adquisición de un nombre de dominio de nivel superior, con el objeto de que lo usen como una medida más de seguridad en sus portales financieros para ofrecer los servicios de banca electrónica.

Capítulo I.

Phishing.

Capítulo I. *Phishing*

1. Origen y definición del término

Los avances de las tecnologías no sólo han facilitado las actividades cotidianas, también se han utilizado para realizar actos ilícitos que se aprovechan de la falta de información, del desconocimiento y de la buena fe de los usuarios de Internet, tanto de migrantes como de nativos digitales[1], que por su poca experiencia en esta red llegan a ser víctimas de la actividad conocida como *phishing*.

En relación con el origen de este concepto,

> se dice que el término "*phishing*" es la contracción de *"**p**assword **h**arvesting f**ishing**"* (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo, dado que el dígrafo *'ph'* es comúnmente utilizado por los *hackers* para sustituir la 'f', como raíz de la antigua forma de hacking telefónico conocida como *phreaking*. El término *phishing* apareció por primera vez en enero de1996, en el grupo de noticias de hackers *alt.2600*, aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias *hacker 2600 Magazine*. El término '*phishing*' fue adoptado por quienes intentaban "pescar" cuentas de miembros de América Online (AOL).[2]

Por su parte, la revista de *DelitosInformáticos.com* señala que "el origen de este delito data de la década de los noventa, y su operativa se centraba en el

---

[1] **Nativo Digital**: Los universitarios de hoy constituyen la primera generación formada en los nuevos avances tecnológicos, a los que se han acostumbrado por inmersión al encontrarse, desde siempre, rodeados de ordenadores, vídeos y videojuegos, música digital, telefonía móvil y otros entretenimientos y herramientas afines
(In)Migrante Digital: hemos de hacer constar que, al igual que cualquier inmigrante, aprendemos –cada uno a su ritmo- a adaptarnos al entorno y al ambiente, pero conservando siempre una cierta conexión (a la que denomino "acento") con el pasado.

Nativos e inmigrantes digitales [http://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf], consultada el 15 de abril de 2016.

[2] *EcuRed*, voz '*phishing'* [http://www.ecured.cu/index.php/Phishing], consultada el 8 de marzo de 2014. Negritas en original.

envío de correos electrónicos fraudulentos a los clientes de entidades financieras. En un principio estos mensajes estaban mal redactados, con una burda traducción al español y con errores ortográficos, sin embargo, en la actualidad, su redacción es mucho más perfeccionada, por lo que consiguen conferir mayor credibilidad al mensaje".[3] También indica que "el término *phishing* proviene de la palabra inglesa '*fishing*' (pesca), hace alusión al intento de hacer que los usuarios 'piquen en el anzuelo' y se conviertan en víctimas. A la persona que pone en práctica este delito se le conoce como *phisher*",[4] quien se aprovecha de la falta de conocimientos por parte de los usuarios de banca electrónica de cierto tipo de medidas se seguridad en los portales financieros en Internet, razón por la que caen en los engaños de estos delincuentes que han obtenido las técnicas para engañarlos y consecuentemente defraudarlos.

Por otro lado, el *phishing* es definido por el Equipo de Respuesta a Incidencias de Seguridad Informática de la UNAM de la siguiente forma: "su nombre completo es *Phishing Scam*. Es un conjunto de técnicas y mecanismos empleados por los intrusos o *hackers* con el propósito de robar información personal de un usuario y así poder suplantar su identidad. Generalmente los intrusos buscan información financiera como números de tarjeta, claves usuario, etc.".[5] En este concepto podemos destacar que el *phishing* requiere la utilización de técnicas y mecanismos en Internet para gestar el robo de información. Sobre esto último, más adelante establecemos ejemplos reales de la forma en la cual los delincuentes informáticos han perfeccionado su comunicación utilizando las marcas, logotipos, comunicación institucional, frases y otros elementos que las

[3] "Información sobre *Phishing*, ofertas de trabajo falsas y blanqueo de capitales", revista *Delitos Informáticos.com*, [http://www.delitosinformaticos.com/03/2012//fraudes/informacion-sobre-phishing-ofertas-de-trabajo-falsas-y-blanqueo-de-capitales#.UxyN2fl5MxM.], consultado el 8 de marzo de 2014.

[4] *Ídem*.

[5] Voz '*Phishing*', [http://www.seguridad.unam.mx/usuariocasero/diccionario/?txtbusq=phishin], consultado el 22 de noviembre de 2013.

instituciones de crédito usan en su comunicación o publicidad para sus clientes, elementos estos con los que los *phisher* se comunican de manera convincente con los usuarios de banca electrónica por Internet.

En cuanto a la definición de esta actividad, Microsoft señala que el *phishing "*es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas *web* que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio)".[6] En términos coloquiales, podemos entender que el *phishing* es una actividad que busca la *pesca* de información o datos de identificación y autenticación de los usuarios de servicios financieros en Internet.

El *phishing*, como ya se indicó, es utilizado por los defraudadores informáticos quienes, a través del engaño y aprovechándose de la escasa experiencia de los usuarios de la banca electrónica o banca por Internet, han llegado a ellos para obtener sus claves y contraseñas con el objeto de hacerse de recursos; una vez que el cliente ha sido engañado y consecuentemente defraudado, este es el principal promotor de señalar que los medios electrónicos son inseguros, pero no es así, sino que las propias personas son vulnerables por su falta de conocimiento.

El *phishing*, como técnica de engaño mediante el uso de medios electrónicos para defraudar a las personas a través de páginas electrónicas apócrifas, es un fraude considerado como una *"*conducta activa, [pues] el sujeto

[6] "¿Qué es el *phishing?*", [http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=125], consultado el 25 de febrero de 2014.

activo no tiene que desplazarse hacia la cosa, porque la obtuvo como resultado del engaño en que hizo caer a su víctima; su verbo rector es 'engañar*': hacerse de* una cosa mediante el engaño o aprovechándose del error en que otro se halle".[7] La conducta activa se realiza cuando el sujeto lleva a cabo los actos necesarios para lograr el engaño en el usuario de banca electrónica para obtener las claves y contraseñas; en este caso, podemos considerar que la conducta activa se actualiza en el momento en que utiliza las claves y contraseñas en una plataforma electrónica de servicios financieros para transferir recursos de manera ilícita.

Una vez que hemos descrito la historia y el significado del *phishing*, podemos ofrecer una definición de la siguiente forma: se trata de una conducta activa que utiliza técnicas y mecanismos para engañar a los usuarios de servicios financieros por Internet o por cualquier medio electrónico, con el objeto de obtener claves y contraseñas mediante las cuales se adquieren de manera ilícita recursos monetarios en los portales financieros de las instituciones de crédito.

2. Estudio de caso (incidencia del *phishing*)

En el año 2014, los incidentes de *phishing* aumentaron 406%;[8] este dato nos indica que dicho incidente sigue utilizándose para engañar a las personas con el objeto de que proporcionen sus llaves de acceso a los servicios de banca electrónica y así realizar el fraude.

En cada incidente de *phishing*, habitualmente se envían hasta millones de correos electrónicos a direcciones que han podido ser obtenidas de diferentes

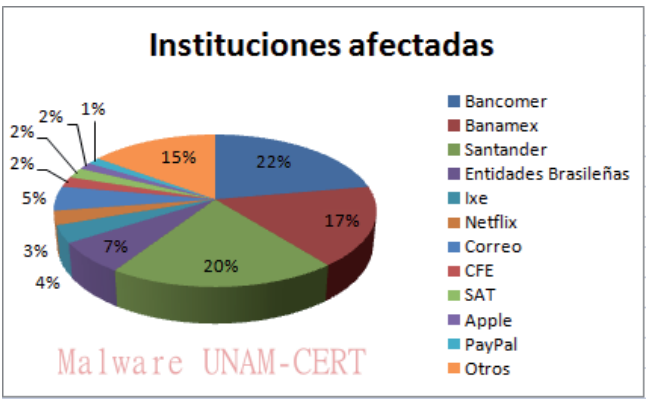
[7] Sara Pérez Kasparian, *Manual de delitos en particular,* 2ª ed., México, Porrúa, 2014, pp. 171 y 172.

[8] Symantec, *Tendencias de seguridad cibernética en América Latina y el Caribe*, Washington, Symantec, 2014, p. 68.

maneras, por lo que *no es un ataque dirigido.* La probabilidad de recibir un correo de *phishing* es igual a la probabilidad de que tu dirección de correo electrónico haya sido capturada en algún foro, cadena de correos, *web* u ordenador infectado, al descargar una aplicación móvil, al permitir el acceso a los contactos de un dispositivo móvil, etc.; en esta primera parte, el *phisher* desconoce si las personas titulares de las cuentas de correo electrónico tienen una cuenta bancaria y si poseen un servicio de banca electrónica.

Los blancos más comunes de los ataques de *phishing* son las instituciones bancarias, porque en total representan el 69%, de éstas, el 66% se encuentra en México (Bancomer, Banamex, Santander, Scotiabank, IXE, Banorte y HSBC) y el 3% en Brasil (Banco do Brasil, Bradesco, Caixa e Itau) (ver figura 1).[9] Cabe precisar que quienes reciben el ataque son los usuarios de servicios financieros, ya que son los que reciben la comunicación de los defraudadores que analizaremos más adelante.

Figura 1



Fuente: CERT UNAM

[9] *Proyecto Malware,* "Un vistazo a la situación de *phishing* y *malware* en México (Abril-Junio 2015)" [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 el 15 de septiembre de 2015.

El gráfico anterior (figura 1) nos indica claramente qué instituciones financieras en México son las más utilizadas para atacar a los cuentahabientes, ya que son las que tienen mayor cuota de mercado y, en consecuencia, un mayor porcentaje de incidencia.

El *phishing* está dirigido principalmente a los usuarios del sector financiero; como se ha señalado, los *phisher* utilizan el envío masivo de correos electrónicos fraudulentos, en ellos se solicita ingresar a una página que solicita claves, contraseñas y números de identificación como pueden ser los números de servicios (ID), *password* y claves dinámicas, con el argumento de que existen problemas técnicos, procesos de actualización, sincronización y revisión de datos, lo que aprovecha el desconocimiento o la poca experiencia en Internet de los usuarios de servicios de banca electrónica. Dichos mensajes, en algunos casos, también solicitan otro tipo de información como el nombre completo, fecha de nacimiento, empresa donde se labora etc., y usualmente aparentan provenir de administradores de los servidores de correo legítimos que se refirieren a alguno de los siguientes temas:

a) Actualización de la base de datos con la amenaza de cancelar la cuenta.
b) Solicitud de datos personales para verificar que el usuario se encuentre activo.
c) Sincronizar dispositivos electrónicos para su correcto funcionamiento.

Como ejemplo de lo que se ha señalado, actualmente circulan correos que remiten a páginas en Internet para hacer *phishing*, mediante los cuales muchos usuarios de diversos bancos han sido objeto de fraudes a través de este mecanismo; cabe resaltar que el defraudador (*phisher*) que realiza esta actividad utiliza imágenes y textos convincentes para los usuarios de la banca electrónica, lo que permite obtener datos, incluyendo claves y contraseñas.

A continuación citamos una serie de ejemplos de Bancomer y Banamex sobre la forma en la cual los *phisher* se comunican con los usuarios de banca electrónica para poder engancharlos y llevar a cabo su actividad fraudulenta (figuras 2 a 5), las imágenes son ejemplo de como el *phisher* utiliza comunicación muy parecida a la de las instituciones de crédito, para hacer creer a los clientes que son comunicado reales que su banco les envía.

Figura 2. Bancomer

Fuente: Correo electrónico apócrifo.

Al igual que la figura anterior, la figura 3 es otro ejemplo de una comunicación apócrifa que el phisher utiliza para poder enganchar a los clientes, podemos resaltar que el problema no es privativo de una sola institución de crédito y que aqueja a varias de ellas.

Figura 3. Banamex

FUENTE: Correo electrónico apócrifo.

En la figura 4, se observa una comunicación vía correo electrónico que simula ser una comunicación oficial de la institución de crédito misma que contiene elementos en sus textos con los que induce y engaña el *phisher* a los clientes.

Figura 4. Correo electrónico (Bancomer)

------- Mensaje reenviado ----------
De: **Bancomer.com** <envio@re.bancomercorreo.com>
Fecha: 30 de junio de 2014, 13:53
Asunto: Activación Plataforma - Segundo Aviso

ESTIMADO CLIENTE

En Bancomer estamos comprometidos con tu seguridad. Por eso te informamos que en Junio del 2014, tendrás que actualizar tus claves de acceso.

Click aquí para actualizar tus claves

Estamos seguros de que siguiendo estas sencillas medidas de seguridad podrás aprovechar todos los beneficios de tu Banca en Línea de manera segura.

Recomendaciones

- Cambia periódicamente tus datos de acceso.

*No aplica con otras promociones o descuentos, vigencia del 15 de mayo al 15 de julio. Para conocer tiendas participantes consulta vidabancomerdescuentos.com Ingresa a www.bancomer.com/vidabancomer para consultar todos los comercios en los que puedes comprar gratis con tus Puntos y los Términos y Condiciones del Programa.

IPAB Producto garantizado por el IPAB hasta por el equivalente a cuatrocientas mil UDIS por persona.

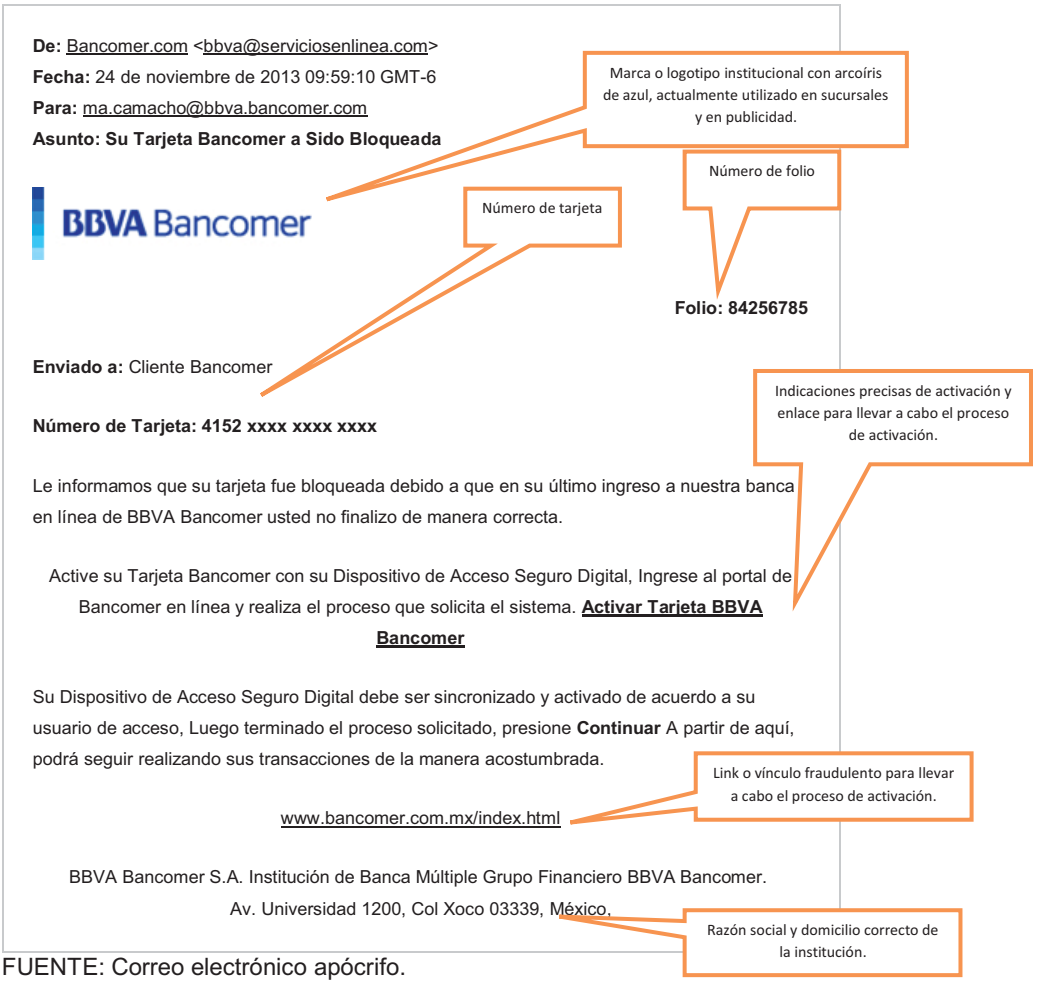
BBVA Bancomer, S.A. Institución de Banca Múltiple, Grupo Financiero BBVA Bancomer. Av. Universidad 1200, Col. Xoco 03339, México, D.F

Este correo electrónico es un mensaje comercial de BBVA Bancomer, Ciudad de México. Si no quiere recibir más correos electrónicos en el futuro, puede eliminar su registro en: desuscripciones@re.bancomercorreo.com

FUENTE: Correo electrónico apócrifo

Nombre de la cuenta de correo que parece que es una cuenta institucional.

Figura 5. Correo electrónico (Bancomer)



FUENTE: Correo electrónico apócrifo.

Los ejemplos anteriores (figuras 2 a 5) nos permiten visualizar cómo el delincuente informático que trata de defraudar utiliza elementos que inducen al

engaño a los usuarios de banca electrónica mediante el uso de características de instituciones bancarias, el cual le da confianza al usuario por el desconocimiento de este tipo de mecanismos.

El usuario que cae en el engaño accede a la página *web* falsa del intruso e introduce sus datos personales. La información que los intrusos intentan obtener comúnmente a través de un ataque de *phishing* es el *nombre de usuario* (conocido como *login*) y la *contraseña* para acceder a un servicio, así como los *números de su tarjeta de crédito* y *claves de acceso* a su banca electrónica, los *números de seguro social* y cualquier otra información que les permita tener acceso a servicios privados del usuario con el fin de obtener un beneficio propio como, por ejemplo, realizar un fraude a través de la banca electrónica.[10] Dicha información se guarda para poder realizar el ilícito antes mencionado. Generalmente, los datos que se solicitan son los relacionados con los accesos a la banca electrónica, pero también es posible que se pida el número de la tarjeta de crédito, la fecha de caducidad y el código CVV contenido al reverso de la tarjeta, para, de esta forma, realizar compras en Internet (comercio electrónico).

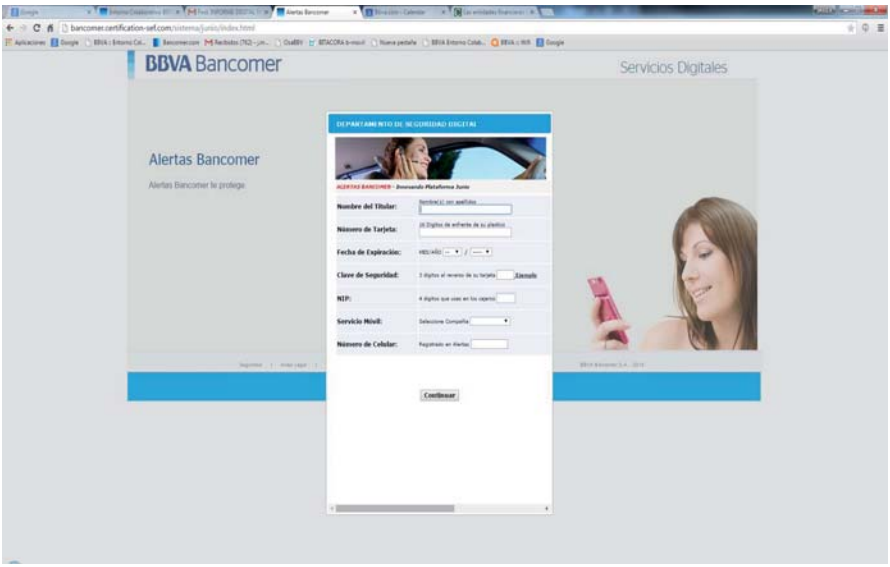
De este punto podemos señalar que el *phishing* consiste en el envío de mensajes (anzuelos) a una base de datos de correos electrónicos que recurre a un método de engaño para suplantar a una institución bancaria con el objetivo de persuadir (engañar) a su víctima para que proporcione sus claves y contraseñas financieras. Una vez obtenida, esta información es utilizada para realizar operaciones monetarias como transferencias de fondos que afectan económicamente a la víctima y reputacionalmente a la institución de crédito.

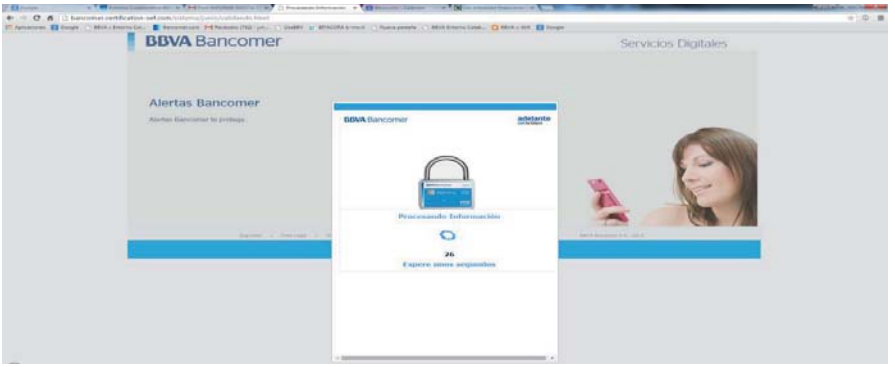
---

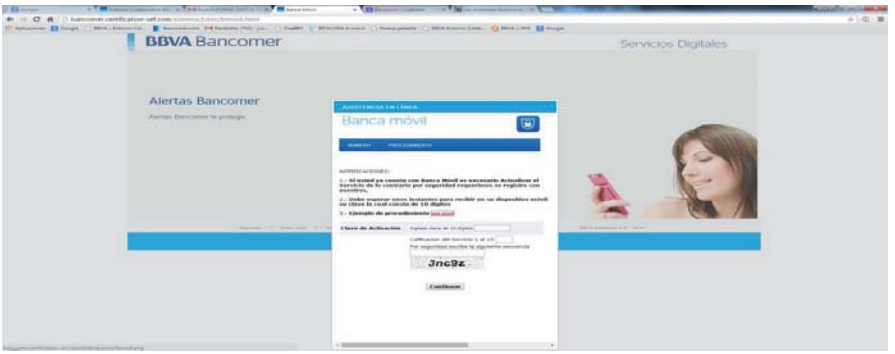
[10] *Véase* *Phishing* Scam, [http://www.seguridad.unam.mx/usuariocasero/eduteca/main.dsc?id=166#queEs], consultado el 7 de marzo de 2014.

Una vez que el *phisher* envió los correos electrónicos, solo basta esperar a que los usuarios de servicios de banca electrónica accedan a los enlaces (*links*) de los sitios en Internet falsos que ha enviado en el cuerpo del mensaje del correo y con ello pueda obtener claves y contraseñas. A continuación presentamos algunas imágenes que los usuarios de servicios financieros ven y en que confían, ya que aparentemente su banco les está solicitando sus claves y contraseñas para efectos de sincronizar o actualizar sus datos. Se trata de una secuencia de formularios que los usuarios de servicios financieros requisitan, en los que proporcionan datos personales, así como claves y contraseñas, con las cuales se el defraudador tiene acceso a los servicios de banca electrónica (figura 6).

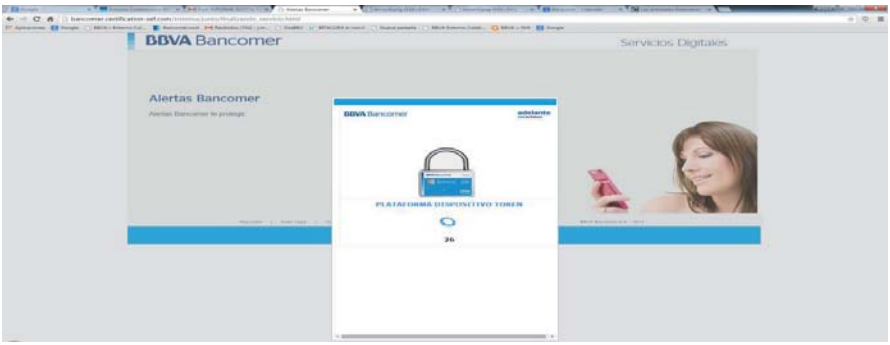
Figura 6. Secuencia de formulario Bancomer



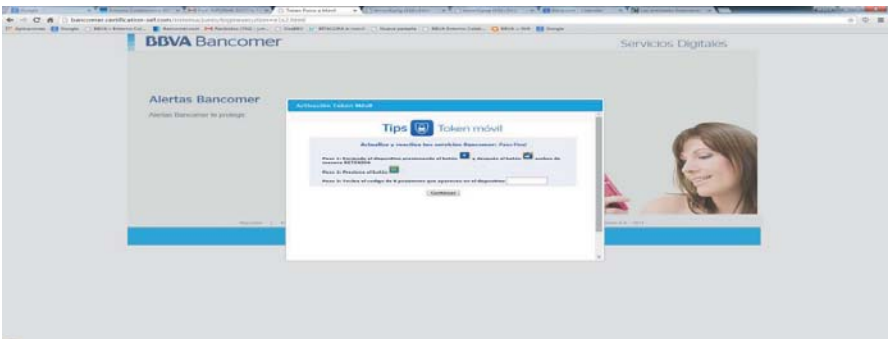

BBVA Bancomer
Servicios Digitales
Alertas Bancomer
Procesando Información
26
Espere unos segundos


BBVA Bancomer
Servicios Digitales
Alertas Bancomer
Banca móvil
Jnc9z
Continuar


BBVA
13:12
¡Felicidades! activaste Bancomer movil exitosamente. Cualquier duda llama al 01 800-262663/52262663
13:12
Tu clave de activacion a Bancomer movil es: 7864307423
NOTA
Los siguiente msgs deben llegar a su dispositivo móvil


BBVA Bancomer
Servicios Digitales
Alertas Bancomer
Alertas Bancomer te protege
BBVA Bancomer
PLATAFORMA DISPOSITIVO TOKEN
26


BBVA Bancomer
Servicios Digitales
Alertas Bancomer
Alertas Bancomer te protege
Activación Token Móvil
Para Continuar Selecciona tu Dispositivo Digital de Bancomer


BBVA Bancomer
Servicios Digitales
Alertas Bancomer
Alertas Bancomer te protege
Activación Token Móvil
Tips
Token móvil

FUENTE: página fraudulenta *phishing*

Dentro de esta secuencia (figura 6) el *phisher* realiza lo siguiente: *i)* duplica una página *web* una vez que el intruso tiene implementado el sitio *web* falso en Internet, *ii)* comienza a realizar el envío masivo de correos electrónicos que en su tema y cuerpo del mensaje hacen referencia a que el usuario debe acceder al sitio de Internet de la institución financiera y realizar cambios a su información personal; estos correos electrónicos contienen la dirección electrónica en la que el usuario debe acceder para realizar los cambios que se le solicitan.

Como hemos visto, un ataque de *phishing* es bastante sencillo de ejecutar, pero a la vez, muy fácil de detectar, puesto que hay que desconfiar de cualquier petición de entrega de nuestras claves de acceso a cualquier sitio *web*, venga la petición por correo electrónico, SMS, o incluso si alguien nos llama por teléfono solicitando las mismas.[11]

[11] Protege tu información, Banca *online* [http://www.protegetuinformacion.com/docs/11/banca_online_2_phising.pdf], consultado el 8 de marzo de 2014.

Estos mensajes de correo electrónico como mensajes de datos,[12] siempre incluyen enlaces que conducen aparentemente a las páginas *web* oficiales de las citadas entidades financieras pero que, en realidad, remiten a páginas electrónicas apócrifas alojadas generalmente en servidores totalmente normales, pero que, por algún fallo de seguridad, han sido comprometidos, y los estafadores han podido alojar dichas páginas falsas en servidores personales, de empresas o, incluso, de organismos oficiales.

3. Alerta del *phishing* por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financiaros (Condusef) ha emitido alertas de correos fraudulentos (citados más adelante, en las figuras 7), con las cuales informa a los cuentahabientes de instituciones financieras de la existencia estos correos falsos que están circulando. En dichas alertas realiza recomendaciones, sin embargo, sus esquemas carecen de difusión en medios de manera masiva, ya que actualmente solo se puede conocer sobre los mismos en la página www.condusef.com, y esporádicamente en *spots* de radio.

[12] En el artículo 89 del Código de Comercio se define el *"Mensaje de Datos*: la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología". En otras palabras, es la información que será cifrada por el firmante con la firma electrónica para dar seguridad de que se contenido no será alterado y de que proviene de quien aparece como el emisor (firmante), el cual expresa su consentimiento y lo reconoce como propio, lo que le impedirá impugnarlo válidamente como ajena.

Figura 7. Comunicados

CONDUSEF ALERTA DE NUEVO CORREO APÓCRIFO PRESUNTAMENTE ENVIADO POR BBVA BANCOMER

México, D.F., a 21 febrero de 2014

Comunicado No. 12

Ante la posibilidad que piratas cibernéticos puedan acceder a datos personales de clientes del servicio de banca electrónica, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), emite una nueva alerta por un correo falso que circula por la red, presuntamente enviado por BBVA Bancomer.

El correo electrónico apócrifo indica que la cuenta y la tarjeta del usuario fueron bloqueadas por motivos de seguridad, debido a que en su última consulta en cajero automático, la sesión no fue cerrada de manera correcta.

CONDUSEF descalifica este correo y reitera que es una medida que utilizan los hackers para llevar a los usuarios a un sitio de internet falso, donde solicitan los datos personales del cliente de servicios financieros, tales como nombre, domicilio, contraseñas, número de identificación personal (NIP), número de cuenta bancaria de tarjetas de crédito, débito y cualquier otra información personal, para posteriormente cometer fraude con sus cuentas bancarias.

Asimismo, conviene recordar que en ningún caso los bancos o instituciones como Visa o MasterCard piden a sus clientes actualizar mediante correo electrónico, información personal, contraseñas, NIP o cualquier dato de sus cuentas bancarias.

A los usuarios del servicio de banca electrónica, se les hacen las siguientes recomendaciones en materia de seguridad:

No realizar transacciones financieras en computadoras de uso público.

Utilizar claves fáciles de recordar, pero difíciles de adivinar.

Cambiar las contraseñas de manera regular.

Procurar utilizar contraseñas diferentes, si se cuenta con el servicio de banca por internet, en más de una institución financiera.

Desactivar la opción "recordar contraseñas" en el servicio de banca por internet.

No apartarse de la computadora cuando se tenga abierta una sesión de banca por internet, ni dejar los token a la mano.

A continuación te mostramos el falso correo que circula por la red:

Para cualquier duda o consulta adicional favor de comunicarse a CONDUSEF al teléfono 01 800 999 80 80 o bien, visitar nuestra página de internet www.condusef.gob.mx también nos pueden seguir en Twitter: @CondusefMX y Facebook: CondusefOficial.[13]

[13] Condusef, Alerta de nuevo correo apócrifo presuntamente enviado por BBVA Bancomer [http://www.condusef.gob.mx/index.php/prensa/comunicados-2014/1021-condusef-alerta-de-nuevo-correo-apocrifo-presuntamente-enviado-por-bbva-bancomer], consultado el 26 de febrero de 2014.

ALERTA CONDUSEF POR CORREO FALSO PRESUNTAMENTE ENVIADO POR BBVA BANCOMER

México, D.F., a 14 de enero de 2015
Comunicado No. 005

Recuerda a los usuarios que este tipo de mensajes maliciosos puede derivar en fraudes.

Si vas a usar banca por internet, te recomendamos que ingreses por la liga oficial de la institución.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) emite una nueva alerta a los clientes de BBVA Bancomer, por la circulación de un correo electrónico apócrifo que circula por la red "presuntamente" enviado por dicha institución bancaria.

En el e-mail apócrifo se informa al usuario que no ha realizado el proceso de actualización de su tarjeta, y que debe llevarlo a cabo para que por medio de su registro esté informado sobre cualquier anomalía con su plástico. Asimismo, hace referencia que es un procedimiento forzoso, ya que con dicho registro supuestamente la institución mantendrá contacto con el usuario.

En CONDUSEF reiteramos que este tipo de mensajes contienen ligas que dirigen a los usuarios a un sitio de internet falso, donde les solicitan datos personales como nombre, domicilio, contraseñas, número de identificación personal (NIP), número de cuenta bancaria, así como de tarjetas de crédito y débito, para posteriormente cometer fraude con sus cuentas bancarias.

Cabe destacar que a lo largo del año, se han emitido alertas a los clientes de Scotiabank y BBVA Bancomer por *phishing* (técnica utilizada para captar datos bancarios de los usuarios, a través de la utilización de la imagen de la institución financiera).

Es necesario recordar que en ningún caso los bancos o instituciones como Visa o MasterCard piden a sus clientes actualizar mediante correo electrónico, información personal, contraseñas, NIP o cualquier dato de sus cuentas bancarias.

CONDUSEF reitera a los usuarios, las siguientes recomendaciones al realizar operaciones de banca en línea:

No realizar transacciones financieras en computadoras de uso público.

Utilizar claves fáciles de recordar, pero difíciles de adivinar.

Cambiar las contraseñas de manera regular.

Procurar utilizar contraseñas diferentes, si se cuenta con el servicio de banca por internet, en más de una institución financiera.

Desactivar la opción "recordar contraseñas" en el servicio de banca por Internet.

No apartarse de la computadora cuando se tenga abierta una sesión de banca por Internet, ni dejar los token a la mano.

Para cualquier duda o consulta adicional favor de comunicarse a CONDUSEF al teléfono 01 800 999 80 80 o bien, visitar nuestra página de Internet www.condusef.gob.mx también nos pueden seguir en Twitter: @CondusefMX y Facebook: CondusefOficial.14

[14] Condusef, Alerta por correo falso presuntamente enviado por BBVA Bancomer, [*http://www.condusef.gob.mx/index.php/prensa/comunicados-2015/1145-alerta-condusef-por-correo-falso-presuntamente-enviado-por-bbva-bancomer*], consultado el 14 de enero de 2015.

REGISTRA CONDUSEF NUEVO CASO DE "*PHISHING*" CONTRA USUARIOS DE BBVA BANCOMER

México, D.F., a 17 de abril de 2015
Comunicado No. 037

- **En lo que va del año CONDUSEF ha difundido 4 alertas por correos electrónicos apócrifos**
- **Los bancos más afectados han sido BBVA Bancomer y Santander**

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), hace un llamado a la población a no dejarse engañar por nuevas tácticas de *Phishing* en donde falsos correos electrónicos, supuestamente enviados por instituciones financieras, mencionan al usuario que ha recibido una transferencia a su cuenta que se encuentra retenida por anomalías en su estado financiero.

Esta actividad denominada *Phishing*, consiste en captar datos personales y bancarios de los usuarios a través de la utilización de la imagen de la institución financiera, para posteriormente cometer fraude con las cuentas de las personas que llegan a caer en el engaño.

Cabe recordar que en el año 2014, se registraron 693 mil 290 reclamaciones imputables a un posible fraude en tarjeta de crédito y débito por operaciones sin la presencia física del plástico, de las cuales 547 mil 104 correspondieron a Tarjeta de Crédito, lo que significó un incremento de 3% más con respecto a lo registrado en 2013. Hay que señalar que el *Phishing* es una de las causas de este tipo de reclamaciones.

Algunas instituciones bancarias como Banorte han tomado medidas sobre estos mensajes apócrifos, alertando a sus clientes mediante correo electrónico o anuncios al inicio de la sesión de banca en línea, ya que la actualización de datos nunca se realiza mediante e-mail.

En el nuevo caso de *Phishing* detectado por esta Comisión Nacional, el correo proviene aparentemente de BBVA BANCOMER y le informa al usuario que "acabas de recibir una Transferencia a tu Cuenta, la cual se encuentra retenida debido a anomalías en tu estado financiero".[15]

Te informamos que acabas de recibir una Transferencia a tu Cuenta, la cual se encuentra retenida debido a anomalías en tu estado financiero. Para más detalles sobre esta situación le adjuntamos un documento en formato Microsoft Word donde explicamos el motivo de la retención y los pasos a seguir para regularizar este problema.

Importe de la operación $ 87,979.20

Fecha: 16 de Abril de 2015, 07:41:24 PM

Folio Internet: 081525418

ESTADO: RETENIDA

Recomendamos seguir a la brevedad los pasos descritos en el documento adjunto en este correo.

Este correo constituye sólo una referencia de los términos en que se realizó la operación, el único comprobante oficial es el estado de cuenta de cheques que emite el GFBBVA Bancomer, S.A.

Posteriormente incluyen enlaces falsos que te llevan a sitios en donde solicitan ingreses tus datos personales para concluir supuestamente con el desbloqueo de la cuenta.

Por ello, CONDUSEF hace un llamado a los usuarios de banca electrónica para que sigan las siguientes recomendaciones:

- No realices transacciones financieras en computadoras de uso público.
- Utiliza claves fáciles de recordar, pero difíciles de adivinar.
- Cambia tus contraseñas de manera regular.
- Procura utilizar contraseñas diferentes, si cuentas con el servicio de banca por Internet, en más de una institución financiera.
- Desactiva la opción "recordar contraseñas" en el servicio de banca por Internet.
- Procura no apartarte de la computadora cuando tengas abierta una sesión de banca por Internet, ni dejar el T*oken* a la mano.

Para cualquier duda o consulta adicional favor de comunicarse a CONDUSEF al teléfono 01 800 999 80 80 o bien, visitar nuestra página de Internet www.condusef.gob.mx también nos pueden seguir en Twitter: @CondusefMX y Facebook: CondusefOficial.

[15] Registra Condusef nuevo caso de *phishing* contra usuarios de BBVA Bancomer [http://www.condusef.gob.mx/index.php/comunicados-de-prensa/1196-nuevo-caso-de-phishing-bbva], consultado el 16 de septiembre de 2015.

SE INCREMENTAN LAS RECLAMACIONES EN LA BANCA REMOTA

México, D.F., a 26 de agosto de 2015
Comunicado No. 068

- **En 2014 la banca remota registró 698 mil reclamaciones por un monto de 2,625 millones de pesos.**
- **Mientras que entre 2011 y 2014 crecieron 19%, el monto abonado se redujo 9 puntos porcentuales, pasando del 60 al 51%.**

Las reclamaciones derivadas de la utilización de la denominada "banca remota" registraron un incremento de 19%, entre 2011 y 2014, al pasar de 587 mil 593 a 698 mil 732.
En tanto que las originadas por movimientos generados por el banco (errores operativos) en las terminales punto de venta, así como en las sucursales registraron disminuciones de 33, 11 y 10% respectivamente.
Con excepción de las operaciones por internet de personas morales, todos los canales que conforman la "banca remota" registraron incrementos en el número de reclamaciones destacando por su crecimiento: la banca móvil 334%, las operaciones por internet de personas físicas 297%, los corresponsales bancarios 155% y los pagos por celular.
Lo anterior se explica en buena medida por la mayor incorporación de usuarios al uso de la banca remota, pero también por el incremento del <fraude cibernético como el *phishing* del que no se puede responsabilizar directamente a las instituciones bancarias. (énfasis añadido)

RECLAMACIONES A LA BANCA MULTIPLE POR CANAL 2011-2014

CANAL	2011					2014				
	Reclamaciones			Monto Abonado		Reclamaciones			Monto Abonado	
	Numero	Monto en ($)	Promedio	$	(%)	Numero	Monto en ($)	Promedio	$	(%)
Total Banca Múltiple	4,230,372	10,942,882,085	2,586.7	5,039,876,581	53.4	4,370,570	14,043,186,309	3,213.1	6,829,084,907	48.6
Banca Remota	**587,593**	**2,124,097,639**	**3,614.9**	**1,272,436,646**	**59.9**	**698,732**	**2,625,489,677**	**3,757.5**	**1,336,376,406**	**50.9**
Cajeros Automat. (ATM)	556,196	1,264,445,782	2,261.2	807,687,757	63.9	589,958	1,575,412,488	2,551.4	925,852,866	67.3
Oper. Internet Pers. Fis.	9,513	181,799,078	19,110.6	36,814,863	20.3	37,841	494,728,334	13,073.9	147,006,176	29.7
Oper. Internet Pers. Mor.	8,548	639,432,062	74,804.9	408,671,410	63.9	5,631	632,369,571	112,301.5	220,911,314	34.9
Corresponsales	9,023	20,802,267	2,305.5	10,353,072	49.8	23,073	53,695,648	2,324.6	23,636,625	44.0
Pagos por Celular	80	69,363	867.0	14,125	20.4	38,142	20,172,720	528.9	7,096,414	35.2
Banca Móvil	845	3,885,969	4,598.8	325,931	8.1	3,670	37,244,769	10,148.4	11,222,068	30.1
Banca por Teléfono	388	13,663,098	35,214.2	8,579,488	62.8	417	11,926,147	28,599.9	673,043	5.6
Comercio a distancia	**281,035**	**502,540,016**	**1,788.7**	**377,086,914**	**75.0**	**660,226**	**947,536,341**	**1,435.2**	**708,590,821**	**74.8**
Por Internet	205,279	413,775,354	2,015.7	304,255,459	73.5	433,159	674,563,562	1,557.3	524,313,472	77.7
Por Teléfono	75,756	88,764,662	1,171.7	72,831,455	82.1	227,067	272,975,779	1,202.2	184,277,349	67.5
Term Punto de Venta (TPV)	2,197,105	3,339,188,016	1,519.8	2,164,528,477	76.5	1,954,468	4,511,319,597	2,308.2	2,751,962,847	61.0
Sucursales	365,419	4,096,121,470	24,762.1	1,224,065,623	29.9	146,080	3,567,686,142	24,093.0	1,494,446,102	41.9
Mov. Gen. por el Banco	973,152	800,990,943	823.1	362,101,367	45.2	649,240	1,405,375,144	2,164.6	266,057,473	18.9
Otros	26,068	79,944,001	3,066.7	49,657,754	62.1	250,824	985,774,406	3,794.0	271,651,176	27.6

El monto reclamado a través de los canales que conforman la "banca remota" para 2014, fue de 2 mil 625 millones de pesos, lo que representó un incremento de 23.6% con respecto a 2011 y el monto abonado a los usuarios que llevaron a cabo reclamaciones fue de 1 mil 336 millones de pesos; es decir 50.9% que si bien es mayor en 2.3 puntos porcentuales al promedio general de la banca, resulta inferior en 9 puntos porcentuales al porcentaje abonado en 2011.
En otras palabras, el porcentaje de abono en 2011 fue del 60% del monto reclamado para el caso de "banca remota", mientras que en 2014 fue del 50.9%.

En este sentido destaca el incremento con respecto a 2011, en los montos abonados ante las reclamaciones de: Banca Móvil (22 puntos porcentuales) Pagos por Celular (14.8 puntos porcentuales) y Operaciones por Internet de Personas Físicas (9.5 puntos porcentuales); por el contrario; llama la atención la disminución de los montos abonados ante las reclamaciones de: Banca por Teléfono (-57.1 puntos porcentuales) y Operaciones por Internet de Personas Morales (-29 puntos porcentuales), más aún y cuando este canal registra el monto promedio de reclamación más elevado ($112,301), cifra 30 veces superior al promedio de reclamación en la banca remota ($3,757.5).
Finalmente la CONDUSEF te recomienda que al utilizar las nuevas tecnologías que nos facilitan el acceso a los productos y operaciones bancarias tengas en cuenta las siguientes recomendaciones:

- Ten en cuenta que ni las entidades financieras, ni VISA o MasterCard u otro operador de tarjetas, solicitan datos personales a sus clientes o verificación de sus cuentas, mediante correo electrónico.
- Realiza tus compras seguras por internet, verificando que el sitio cuenta con el protocolo de seguridad https:// y un candado cerrado en la barra de direcciones.
- No respondas ningún mensaje de correo sospechoso, de remitentes desconocidos o aquellos que te dicen haber ganado un premio, viaje o sorteo, generalmente te pedirán tus datos personales.
- Si realizas compras en línea, verifica su dirección y teléfonos, así como sus políticas de pago, envíos, reclamación y de privacidad de la información.
- Conexión a sitios *web*: Nunca ingreses tus contraseñas, sobre todo bancarias, a algún sitio al que se llegó por un correo electrónico o chat. Ingresa directamente a la dirección oficial de la institución financiera.
- Evita realizar sesiones de compras o transferencias electrónicas en computadoras de uso público o compartido.
- Procura no apartarte de la computadora cuando tengas abierta una sesión de banca por Internet, ni dejar el token a la mano.

Para cualquier duda o consulta adicional favor de comunicarse a CONDUSEF al teléfono 01 800 999 80 80 o bien, visitar nuestra página de Internet www.condusef.gob.mx también nos pueden seguir en Twitter: @CondusefMX y Facebook: CondusefOficial. [16]

[16] Se incrementan las reclamaciones en la banca remota [http://www.condusef.gob.mx/index.php/comunicados-de-prensa/1236-se-incrementan-las-reclamaciones-en-la-banca-remota], consultado el 16 de septiembre de 2015.

A la fecha, se han emitido alertas por parte de la Condusef por correos falsos no solo de BBVA Bancomer, sino también de otras instituciones como Banorte, Santander y Banamex, lo que nos indica que los *phisher* de manera activa continúan engañando a las personas para obtener recursos de manera ilícita a través del *phishing*.

Las alertas de la Condusef con relación a los correos apócrifos que supuestamente envían las entidades financieras fueron difundidas en medios de comunicación como periódicos, y buscan informar a los clientes de instituciones bancarias sobre este tipo de fraude, sin embargo, en las indicaciones de las medidas, no se precisa a los usuarios cuáles se deben adoptar para denunciar este tipo de correos fraudulentos que tienen por objeto el *phishing*, sino que sólo se hacen recomendaciones respecto al uso y creación de contraseñas, pero considero que es importante que se informe sobre los servicios financieros por Internet, dónde o cómo se pueden denunciar estas páginas apócrifas a fin de que los usuarios puedan solicitar que sean dadas de baja.

El mecanismo que tiene que promover la Condusef es sus comunicados para dar de baja los dominios de Internet donde se realiza el *phishing* es el CERT de la UNAM, para lo cual, será "necesario que los usuarios afectados *envíen las cabeceras/encabezados del correo*. […] El procedimiento para ver las cabeceras varía dependiendo de cada cliente de correo, a continuación se indican los pasos para notificar un correo fraudulento desde la interfaz *web* de la página http://www.correo.unam.mx".[17]

[17] Manual para identificar y notificar correo fraudulento (*phishing scam*), *http://www.seguridad.unam.mx/documento/?id=81*. Consultado el 22 de noviembre de 2013.

Considero que este tipo de mecanismos para dar de baja los dominios fraudulentos es una solución eficiente, no obstante se dependa de la denuncia para detectarlos. Mientras no exista una difusión efectiva de este tipo de servicios, se pierde efectividad; adicionalmente, cada institución de crédito debe tener o contratar un proveedor de servicios de incidencias de respuesta inmediata (CERT) para hacer frente a la incidencia de páginas apócrifas que se vinculan a dicha institución, esto en beneficio de los clientes de la banca electrónica, ya que las alertas existentes sólo se limitan a comunicar consejos de seguridad, cuando se podrían tomar acciones efectivas para prevenir este tipo de delitos.

Ante el incremento en los casos de fraudes por medio de transacciones de la banca electrónica, la Policía Cibernética hizo un llamado de alerta a los usuarios de dichos servicios, pues las víctimas son tanto grandes como pequeñas empresas. Los montos de los fraudes van de los 40 mil, la cantidad más baja, hasta los 285 mil pesos.[18]

Un resumen estadístico de la Amipci (Asociación Mexicana de Internet) arrojó los siguientes resultados: de los 40.6 millones de internautas mexicanos, el 64% son mayores de edad, y por tanto, susceptibles de poseer algún producto bancario; *el 52%, efectivamente, utiliza algún servicio de la banca,* y el 40% visita los portales de al menos una institución bancaria. Finalmente, el 30% realiza transacciones de banca en línea. Este último porcentaje posee un promedio de 2.1 cuentas de banca por Internet. A partir de estas cifras generales, el corte de noviembre de 2012 del estudio refleja que el 74% de los internautas visita portales

[18] "Alerta policía cibernética por fraudes en banca electrónica", *NorteDigital.mx* [http://www.nortedigital.mx/article.php?id=44848], consultado el 22 de noviembre de 2013.

bancarios, independientemente de que realicen transacciones o no. Esta cifra es un 4% mayor que el 70% del último corte de julio de 2012.[19]

[19] "Crece el uso de la banca electrónica en México: 30 por ciento de los internautas hace transacciones en la banca electrónica", Amipci [http://www.amipci.org.mx/?P=articulo&Article=184], consultado el 24 de noviembre de 2013.

Capítulo II.

El *phishing* como una modalidad del delito de fraude.

Capítulo II. El *phishing* como una modalidad del delito de fraude

1. Fraude genérico

El fraude como "Acto mediante el cual una persona engañando a otra o aprovechándose el error en que se halla, obtiene ilícitamente una cosa o un lucro indebido"[20] es una definición con la que el maestro Rafael De Pina describe de manera general la conducta delictiva del fraude, la cual requiere de una acción por parte del sujeto activo (defraudador) para obtener una cosa o lucro de otra, que se encuentra en un estado de error o engaño (sujeto pasivo).

Primero, debemos entender qué es el fraude, para lo cual podemos señalar que "defraudar es engañar; y el engaño se logra mediante maquinaciones, elucubraciones, falacias, mentiras que hacen caer a la víctima en un error; del cual se aprovecha el sujeto activo para hacerse ilícitamente de alguna cosa u obtener un lucro indebido en beneficio propio o de un tercero".[21] En mi opinión, el engaño puede ser verbal, escrito o a través de mecanismos utilizados por medios electrónicos y no reviste una forma en particular; de manera general, podemos indicar que engañar es inducir a alguien a tener por cierto lo que no lo es, valiéndose de palabras o de obras aparentes y fingidas.

"Son elementos constitutivos del delito de fraude genérico simple: a) Engaño o aprovechamiento del error; b) Obtención ilícita de una cosa o un lucro indebido; y c) Nexo o relación de causalidad, entre la conducta engañosa y su resultado, no otro que la adquisición antijurídica de la cosa o del lucro."[22] Estos elementos se encuentran presentes cuando se hace creer a las personas que realizan operaciones financieras frente a su institución bancaria y el defraudador

[20] Rafael De Pina, *Diccionario de Derecho*, 3ª. ed., México, Porrúa 1973, p. 186.

[21] Sara Pérez Kasparian, *op. cit.,* nota 7, p. 170.

[22] Sergio García Ramírez y Victoria Adato de Ibarra, *Prontuario del Proceso Penal Mexicano*, 5ª ed., México, Porrúa 1988, p 197.

obtiene un lucro derivado del engaño que comete con los clientes de las instituciones bancarias.

"Los elementos materiales del fraude son: a) el engaño a una persona o el aprovechamiento del error en que se halle; b) que por este medio se obtenga ilícitamente una cosa o se alcance un lucro indebido. Además, la doctrina ha establecido unánimemente que para la integración del delito de fraude debe existir una relación inmediata y directa entre los dos elementos indicados, o sea, que el engaño o aprovechamiento del error debe ser previo a la obtención ilícita de las cosas o al alcance del lucro indebido, y al mismo tiempo la causa determinante de una y otro."[23] La relación causal entre el engaño y la obtención del lucro indebido, son elementos base del tipo penal de fraude genérico, no se podría concebir dicho delito si falta uno de los dos, se necesita que una persona engañe a otra y que tenga por objetivo la obtención de un lucro.

El fraude se tipifica en el Código Penal del Distrito Federal de la siguiente manera: *"*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" (art. 230). El tipo penal señalado recoge como verbo rector el engaño, aunado a la traición y el dolo. Estos elementos constituyen la base del delito de fraude y se encuentran actualizados en el fraude con la utilización de medios electrónicos o digitales, como es el *phishing*, materia del análisis del presente trabajo.

La Suprema Corte de Justicia, en la Tesis Aislada con registro 181331, se establece que el delito de fraude se consuma en el momento en el cual se hace un traspaso indebido de una cuenta a otra:

[23] Raúl Carranca y Trujillo y Raúl Carranca y Rivas, *Código Penal Anotado*, 21 ed., México, Porrúa 1998, p. 948.

FRAUDE. EL DELITO SE CONSUMA EN EL MOMENTO DEL TRASPASO INDEBIDO DE NUMERARIO DE UNA CUENTA A OTRA, A TRAVÉS DE LOS SISTEMAS Y TECNOLOGÍAS APLICABLES AL MANEJO NACIONAL E INTERNACIONAL DE VALORES Y DIVISAS, CON INDEPENDENCIA DEL MATERIAL APROVECHAMIENTO DEL LUCRO OBTENIDO. Si bien el delito de fraude es calificado como de lesión, ello no significa que para acreditarlo tenga que evidenciarse el material aprovechamiento del lucro indebido por parte de los activos, esto es, el disfrute específico del producto del ilícito. Por el contrario, la descripción legal del delito contiene *expresis verbis* los elementos referidos a la conducta (obtener mediante maquinaciones o aprovechamiento del error) y la naturaleza patrimonial de afectación al bien jurídico tutelado (lucro indebido o perjuicio); además, de manera sub *intellegentia* contiene también la exigencia implícita del elemento subjetivo genérico o dolo; sin embargo, resulta evidente que bajo esa descripción quedan plenamente captados no sólo aquellos supuestos en los que, conforme a una concepción tradicional, se patentice el traslado materializado del monto patrimonial de afectación más allá de la consumación y abarcando, incluso, los fines perseguidos por el delincuente, sino que también se comprenden aquellas hipótesis en las que, dada la marcha evolutiva de los sistemas y tecnologías aplicables al manejo nacional e internacional de valores y divisas por medios electrónicos u otros similares, se logran concretizar, para todos los efectos legales, operaciones de transacción válida; de manera que si éstas se obtienen fraudulentamente nada impide considerar la consumación del ilícito de fraude desde el momento en que se traspasa indebidamente el numerario de una cuenta a otra, pues desde ahí se produce el perjuicio para unos y un lucro o beneficio indebido para otros, con independencia de que los activos alcanzaran sus ulteriores fines de aprovechamiento personal del lucro obtenido, pues esto, que no se exige por la descripción típica, queda fuera y más allá de la consumación instantánea del delito en cuestión.

Amparo directo 442/2003. 12 de noviembre de 2003. Unanimidad de votos. Ponente: José Nieves Luna Castro. Secretario: Jorge Hernández Ortega.

Véase: *Semanario Judicial de la Federación*, Séptima Época, Volúmenes 139-144, Sexta Parte, página 78, tesis de rubro: "FRAUDE, CONFIGURACIÓN DEL DELITO DE, AUN CUANDO EL ACTIVO NO DISFRUTE DEL LUCRO OBTENIDO".[24]

[24] Tesis II.2o.P.137 P, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t XIX, junio de 2004, p. 1441.

"En el delito de fraude, el engaño se logra desencadenando el error y la confusión en el sujeto pasivo; por lo tanto, ese error del que se aprovecha el sujeto activo, para lograr defraudar, debe ser muy elaborado e idóneo, para ser capaz de hacer caer al pasivo en esta situación".[25]

La definición que podemos adoptar como la más completa es la señalada por Sara Pérez Kaspiran, en la que encontramos el verbo rector del delito, que es el engaño, que se comete por medio de maquinaciones, falacias y mentiras que forman una falsa realidad en la víctima, misma que es aprovechada por el defraudador con el fin de obtener un lucro indebido en su beneficio.

2. Fraude específico

Por otra parte el fraude específico que se tipifica en los códigos penales se refiere a actos en concreto que realiza el sujeto activo para obtener un lucro o beneficio indebido, sin que necesariamente medie el engaño, en algunos casos reviste características particulares que deben materializarse, el catálogo de conductas que se clasifican como fraude en el Código Penal del Distrito Federal son las siguientes:

> A quién:
>
> "I. Por título oneroso enajene alguna cosa de la que no tiene derecho a disponer o la arriende, hipoteque, empeñe o grave de cualquier otro modo, si ha recibido el precio, el alquiler, la cantidad en que la gravó, parte de ellos o un lucro equivalente;
>
> II. Obtenga de otro una cantidad de dinero o cualquier otro lucro, como consecuencia directa e inmediata del otorgamiento o endoso a nombre propio o de otro, de un documento nominativo, a la orden o al portador, contra una persona supuesta o que el otorgante sabe que no ha de pagarlo;

[25] Sara Pérez Kasparian, *op. cit.*, nota 7, p. 171.

III. Venda a dos personas una misma cosa, sea mueble o inmueble, y reciba el precio de la primera, de la segunda enajenación o de ambas, o parte de él, o cualquier otro lucro, con perjuicio del primero o del segundo comprador;

IV. Al que se haga servir alguna cosa o admita un servicio en cualquier establecimiento comercial y no pague el importe debidamente pactado comprobado;

V. En carácter de fabricante, comerciante, empresario, contratista o constructor de una obra, suministre o emplee en ésta materiales o realice construcciones de calidad o cantidad inferior a las estipuladas, si ha recibido el precio convenido o parte de él, o no realice las obras que amparen la cantidad pagada;

VI. Provoque deliberadamente cualquier acontecimiento, haciéndolo aparecer como caso fortuito o fuerza mayor, para liberarse de obligaciones o cobrar fianzas o seguros;

VII. Por medio de supuesta evocación de espíritus, adivinaciones o curaciones, explote las preocupaciones, superstición o ignorancia de las personas;

VIII. Venda o traspase una negociación sin autorización de los acreedores de ella o sin que el nuevo adquirente se comprometa a responder de los créditos, siempre que estos últimos resulten insolutos;

IX. Valiéndose de la ignorancia o de las malas condiciones económicas de un trabajador a su servicio, le pague cantidades inferiores a las que legalmente le corresponden por las labores que ejecuta o le haga otorgar recibos o comprobantes de pago de cualquier clase, que amparen sumas de dinero superiores a las que efectivamente entrega;

X. Valiéndose de la ignorancia o de las malas condiciones económicas de una persona, obtenga de ésta ventajas usurarias por medio de contratos o convenios en los cuales se estipulen réditos o lucros superiores a los vigentes en el sistema financiero bancario;

XI. Como intermediarios en operaciones de traslación de dominio de bienes inmuebles o de gravámenes reales sobre éstos que obtengan dinero, títulos o valores por el importe de su precio a cuenta de él o para constituir ese gravamen, si no los destinaren al objeto de la operación concertada por su disposición en provecho propio o de otro.

Para los efectos de este delito se entenderá que un intermediario no ha dado su destino o ha dispuesto del dinero, títulos o valores obtenidos por el importe del precio o a cuenta del inmueble objeto de la traslación de dominio o del gravamen real, si no realiza su depósito en cualquier institución facultada para ello dentro de los treinta días siguientes a su

recepción en favor de su propietario o poseedor, a menos que lo hubiese entregado dentro de ese término al vendedor o al deudor del gravamen real o devuelto al comprador o al acreedor del mismo gravamen.

El depósito se entregará por la institución de que se trate a su propietario o al comprador.

XII. Construya o venda edificios en condominio obteniendo dinero, títulos o valores por el importe de su precio o a cuenta de él, sin destinarlo al objeto de la operación concertada.

En este caso, es aplicable lo dispuesto en el párrafo segundo de la fracción anterior.

Las instituciones y organismos auxiliares de crédito, las de fianzas y las de seguros, así como los organismos oficiales y descentralizados autorizados legalmente para operar con inmuebles, quedan exceptuados de la obligación de constituir el depósito a que se refiere la fracción anterior.

XIII. Con el fin de procurarse ilícitamente una cosa u obtener un lucro indebido libre un cheque contra una cuenta bancaria, que sea rechazado por la institución, en los términos de la legislación aplicable, por no tener el librador cuenta en la institución o por carecer éste de fondos suficientes para su pago de conformidad con la legislación aplicable. La certificación relativa a la inexistencia de la cuenta o a la falta de fondos suficientes para el pago deberá realizarse exclusivamente por personal específicamente autorizado para tal efecto por la institución de crédito de que se trate;

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; o

XV. Por sí, o por interpósita persona, sin el previo permiso de las autoridades administrativas competentes o sin satisfacer los requisitos señalados en el permiso obtenido, fraccione o divida en lotes un terreno urbano o rústico, con o sin construcciones, propio o ajeno y transfiera o prometa transferir la propiedad, la posesión o cualquier otro derecho sobre alguno de esos lotes.

XVI. Por cualquier forma transmita la propiedad o prometa transferir la propiedad de un bien inmueble en un conjunto habitacional, comercial o mixto, aún sin construirse, en construcción o construido a sabiendas de que no exista, según corresponda:

a) Certificado único de zonificación de uso del suelo;

b) Certificado de acreditación de uso del suelo por derechos adquiridos;

c) Manifestaciones de construcción;

d) Licencia de construcción especial para demolición;

e) Permisos para la ejecución de obras; o

f) Cualquier otro relacionado con la zonificación, el uso del suelo, construcción y demolición, independientemente de su denominación; Que le permita edificarlo en la forma en que se describa o prometa en el contrato."[26]

"El fraude especifico, a diferencia del genérico, contiene varias fracciones que establecen situaciones mucho más concretas, específicas (valga la redundancia), que en casi todos los casos describen en cada fracción supuestos en los que definitivamente el sujeto activo engaña a la víctima de manera tal que la induce al error, o quizá en otras fracciones no se describe una situación engañosa contra la víctima, pero el activo se hace de la cosa u obtiene un beneficio ilícito, para sí o para un tercero; las descripciones mucho más detalladas de fraudes específicos se han ido conformando, derivadas de la triste realidad, pues son problemas que a diario ocurren y que con el transcurso de los años el legislador ha ido enriqueciendo y modificando el tipo penal" [27] como se describe la conducta humana de los defraudadores día con día crea nuevas formas de obtener un lucro indebido con o sin engaño, por lo que el reto del legislador es adecuar la norma a la nueva realidad que se van dando de momento a momento, ahora bien cuando surgen nuevas tecnologías las cuales son aprovechadas para defraudar es importante adecuar los tipos penales a la nueva realidad a la que nos enfrentamos con las nuevas tecnologías.

[26] Artículo 231 Código Penal para el Distrito Federal.
[27] Sara Pérez Kasparian, *op. cit.*, p. 180, nota 6.

3. El *phishing* como modalidad del fraude

Ahora bien, el *phishing* es una modalidad del delito de fraude, sólo que el medio comisivo en este caso son los medios electrónicos o nuevas tecnologías; en este caso, el sujeto activo se aprovecha del error en que se encuentra el sujeto pasivo para obtener las claves y contraseñas (elaboración) a través de una página electrónica falsa (error) y solicitando información como si fuera la institución de crédito (idóneo).

El *phishing* como conducta ilícita se puede encuadrar en la fracción XIV del artículo 231 del Código Penal para el Distrito Federal.

"Análisis típico"[28]:

Sanción: de acuerdo al valor de lo defraudado la pena será de veinticinco días de multa hasta once años de prisión.

Sujeto activo: el que.

Elemento subjetivo del injusto: con el fin de alcanzar un lucro indebido.

Conducta: entre o se introduzca a **Elemento normativo:** los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores.

Medios comisivos: por cualquier medio accese.

El *phishing*, como fraude, es una problemática que aqueja al sector financiero y principalmente a sus cuentahabientes como los sujetos objetivos del delito de fraude, ya que a través de correos y páginas electrónicas falsas son engañados, y por medio de ingeniería social (práctica de obtener información

[28] Alberto E. Nava Garcés, *Análisis de la legislación penal mexicana en informática.1ª.* ed., México, Ubijus, 2015, p. 65.

confidencial a través de la manipulación de usuarios legítimos), se obtienen de ellos claves y contraseñas para acceder en los portales de banca electrónica legítimos para realizar transacciones monetarias en perjuicio de los clientes.

"El *phishing* es un fraude cometido mediante la utilización de medios electrónicos, entendido por éste como el acto mediante el cual una persona engañando a otra o aprovechándose del error en que se encuentre, obtiene ilícitamente una cosa o un lucro indebido".[29] El *phishing* afecta la parte patrimonial de clientes, ya que al ser víctimas de este tipo de fraude sufren quebrantos económicos, sin embargo, la afectación no patrimonial la sufren las instituciones de crédito, ya que la reclamación directa es del cliente a la institución, y cuando en respuesta a su reclamación se evidencia de que el cliente fue objeto de un fraude a través de *phishing* se afecta la reputación de la institución de crédito, ya que la percepción del cliente es que no existe seguridad de sistemas y páginas electrónicas de la institución.

El *phishing* no es un nuevo delito, sino una modalidad, como lo señala Alberto Nava Garcés, quien indica que "en ocasiones parecen existir nuevos delitos no comprendidos en el código punitivo, sin embargo vistos a la luz de la propia esencia, podemos encontrar que, en la mayoría de los casos la tecnología no es una nueva forma de conducta sino un medio para ejercitar las ya conocidas".[30] El fraude como delito de manera genérica o específica, en ambos caso se persigue por querella[31] del ofendido.

[29] Osiris Berenice Pérez Segura, *Contratos y transacciones por medios electrónicos*, México, Trillas, 2013, p. 117.
[30] Alberto E. Nava Garcés, *Delitos informáticos*, 2ª ed., México, Porrúa, 2007, p. 149.
[31] Marco Antonio Díaz de León, *Vademécum Penal Federal*, 3ª. ed. México, 2007, p.242.

Respecto a las nuevas tecnologías, nos encontramos ante el reto de establecer la existencia del delito cuando el medio comisivo es a través de ellas, ya que para señalar la existencia de un delito informático, Nava Garcés nos indica que "las etapas en las que se funda la existencia de un delito informático son tres: la de su inclusión en los códigos penales (legislación), la forma en que se debe investigar (forense informática) y la forma en que se acredita ante un juzgado o tribunal (prueba electrónica)".[32] Por lo tanto, parece que nos encontramos ante un reto legislativo y pragmático, ya que primero se tiene que modificar la norma punitiva, capacitar al órgano encargado de investigar y, por último, que el juzgador tenga el conocimiento técnico para poder analizar y valorar las pruebas que se presenten y que caen en el mundo electrónico.

Además de la afectación reputacional de la que es objeto la institución de crédito, otras consecuencias del *phishing* son los costos directos e indirectos en que incurren dichas instituciones en el desahogo de las aclaraciones de manera directa ante la Condusef, en virtud de que se tiene que llevar a cabo un procedimiento de aclaración en el que la institución de crédito tiene que aclarar y acreditar ante dicho órgano regulador y al cliente mismo que la persona que ha efectuado las operaciones monetarias de manera remota a través de la banca electrónica ha sido el mismo cliente, quien proporcionó por medio del engaño los elementos de identificación y autenticación pactados en los contratos y que son válidos de acuerdo con la regulación[33] de la Comisión Nacional Bancaria y de Valores.

Una vez que se ha analizado la problemática y la forma en cómo operan los *phisher* con los usuarios de banca electrónica y ante la falta de una norma que regule este tipo de delitos, en el siguiente capítulo analizaremos una forma de

[32] Alberto E. Nava Garcés, *La prueba electrónica en materia penal,* México, Porrúa, 2011, p. 122.
[33] Circular única de bancos, Capítulo X de la Comisión Nacional Bancaria y de Valores.

mitigar esta modalidad de fraude electrónico desde el punto de vista tecnológico, hasta en tanto no se den las modificaciones regulatorias que establezcan alguna forma para contenerlo.

Capítulo III.

Nombres de dominio y diseño de estrategia.

Capítulo III. Nombres de dominio y diseño de estrategia

1. Nombres de dominio

"En los inicios de Internet y hasta la década de los 80, los equipos conectados a la red se identificaban a través de una dirección IP (protocolo de Internet), una larga serie de números que los usuarios tenían que recordar por cada sitio de Internet que deseaban visitar, en esta época se introduce el Sistema de Nombres de Dominio (DNS), que simplifica considerablemente el uso de Internet, sustituyendo las direcciones IP por nombres de dominios".[34] Los nombres de domino tienen por finalidad facilitar la ubicación de los sitios en Internet, ya que al escribir un nombre fácil de recordar (como, por ejemplo, *bancomer.com*) se direcciona a la IP[35] que es administrada por el titular del nombre de dominio, de lo contrario, sería muy complejo recordar direcciones numéricas para los usuarios. Los nombres de dominio tienen por objeto que los usuarios de Internet busquen sitios a través de palabras o nombres comerciales, sin embargo, la facilidad de los nombres comerciales hace vulnerables a los usuarios, ya que se pueden registrar nombres de dominio parecidos a los originales sin que el usuario se pueda percatar de que no corresponden a un sitio seguro.

La Corporación de Internet para Nombres y Números Asignados (ICANN) coordina estos identificadores únicos en todo el mundo. Los nombres de dominio se desarrollan para facilitar a las personas el acceso a las páginas en Internet; se toma en consideración la sencillez con la que debe operar Internet para que cualquier persona pueda operar en la red.

---

[34] *Origen de los dominios* [http://www.refineriaweb.com/panel/knowledgebase/6/Origen-de-los-Dominios.html], consultado el 18 de junio de 2014.

[35] *Definición de IP*. Una dirección IP funciona para la comunicación en una red a través de paquetes conmutados, es principalmente usado en Internet. Los datos se envían en bloques conocidos como paquetes (datagramas) de un determinado tamaño. En: http://www.alegsa.com.ar/Dic/ip.php#sthash.fDKxtoRY.dpuf, consultado el 28 de septiembre de 2015.

Para explicar el funcionamiento de los nombres de dominio, expondré un ejemplo: la dirección IP de una página *web* es *110.247.125.147*, pero este número de conexión es muy complejo y largo, así que, como usuario, tengo la opción de solicitar el registro del nombre de una empresa de manera alfabética y lo vinculo a la dirección IP fija del servidor donde esta almacenada la página *web*; entonces, los clientes solo visitan *abcdef.com*, el dominio los reenvía a la IP numérica y ésta los conecta con el servidor *web* que responde enviándoles la página electrónica. Todos estos enlaces se realizan en décimas de segundo, así que pasa desapercibido. Esto sucede como cuando en el teléfono celular por lo general ya no escribimos los números de nuestros amigos, solo seleccionamos los nombres como *Juan* y damos *ok*, y su teléfono ya sabe a qué número conectarse.

Es importante señalar que existen diferentes niveles de nombres de dominio, por lo que de manera muy breve señalaremos cuáles son:

a) "Los conocidos como *Top Level Domain Names (gTDLs)*, que son los genéricos, en esta categoría se encuentran los *.com* (organización comercial), *.org* (organización no lucrativa), *.net* (organización dedicada a la red), *.edu* (Instituto educacional), *.gov* (entidad gubernamental), *.mil* (militar)".[36]

b) Los dominios territoriales son los que identifican el país; los *Country Code Top Level Domain* (ccTLD) se componen de un código de dos letras asignado a cada país. En México corresponde a *.mx*.

[36] Nombres de dominio de primer nivel [http://www.pyme.net.uy/documentos/codigos_dominios.htm], consultado el 28 de junio de 2014.

2. Nuevos Nombres de Dominio de Nivel Superior (gTLD)

Los nuevos gTLD tienen por objeto que las empresas propietarias de marcas reconocidas a nivel mundial puedan registrar con los mismos nombres de dominio (por ejemplo, *.bancomer*) que identifiquen al dueño del nombre de dominio, por lo que cualquier organización del orden público o privado puede solicitar la creación y operación de un nuevo gTLD, para tal efecto, el solicitante deberá demostrar su capacidad operativa, técnica y financiera para operar el registro de dominio. El solicitante deberá presentar una serie de información y documentación para acreditar la estabilidad e interoperabilidad de Internet.

Representantes de una amplia variedad de grupos formados por los gobiernos, particulares, la sociedad civil, el sector empresarial y el de la propiedad intelectual, así como la comunidad tecnológica, participaron en debates durante más de 18 meses sobre cuestiones como la demanda, los beneficios y los riesgos de nuevos gTLD, los criterios de selección que se deben aplicar, cómo se deben asignar los gTLD y las condiciones contractuales necesarias para que los registros de gTLD puedan avanzar.[37]

Por su parte ICANN ha desarrollado una serie de especificaciones técnicas de los DNS-gTDL, que se encuentran en el documento denominado *La Guía del Solicitante*; el proceso de solicitud puede durar varios meses. Los solicitantes usan una interfaz llamada "sistema de solicitud de TLD", en la cual se contestan las preguntas relativas a las capacidades técnicas y comerciales para operar el registro del nuevo nombre de dominio. Durante el periodo de registro se publican las solicitudes de los nuevos gTLD y se pueden presentar objeciones, las cuales se someterán a un procedimiento de disputa; para tal efecto, se estará a la guía del solicitante donde se detallan los procedimientos a seguir.

[37] Véase la *Guía del solicitante de gTLD* [https://archive.icann.org/es/topics/new-gtlds/rfp-clean-30may11-es.pdf], consultado el 29 de junio de 2014.

En el proceso de solicitud se tiene que considerar el costo del registro, que es de US$185,000.00 mediante un primer pago por la cantidad de US$5,000.00, cuando el usuario solicita un cupo de solicitud en el sistema, y la cantidad de US$180,000.00 que se deposita en el momento de completar la solicitud. La tarifa de evaluación del dominio genérico de alto nivel (gTLD) se establece para recuperar los costos asociados con el programa de nuevos dominios genéricos de alto nivel (gTLD).

Se ha analizado brevemente el proceso de solicitud y los costos aproximado del valor de la solicitud de un registro de dominio, más adelante se revisará la forma en que puede ser útil un nuevo gTLD acompañado de un programa de educación financiera o de una campaña de difusión a los usuarios de banca electrónica para mitigar el *phishing.*

Una ventaja de los nuevos gTLD es que pueden representar un elemento de seguridad para los usuarios de Internet. Por ejemplo, los TLDs como *.bank* serán más seguros porque tendrán que cumplir ciertos requisitos. Cuando vaya a introducir información personal en esos sitios, se podrá tener la seguridad de que la información está segura; además, el usuario sabrá que el sitio es auténtico.[38]

El dueño de un nuevo gTLD será responsable de una parte crítica y altamente visible de la infraestructura de Internet, pero tendrá beneficios potenciales como crear un modelo de negocio, establecer políticas de accesibilidad para el nuevo gTLD y tendrá un mayor control, ya que, como administrador de un gTLD, establecerá las reglas y, en su caso, el precio de los registros de su dominio de nivel superior; se podrá posicionar la marca, generar lealtad y la confianza por tener un control total sobre su propio gTLD.

[38] *Los nuevos gTLD y los usuarios de Internet* [http://www.newgtldsite.com/es/nuevos-gtlds-para-usuarios.html], consultado el 30 de junio de 2014.

"Posiblemente el gTLD solicitado podría competir con otro similar e indirectamente con todos los dominios de primer nivel, tanto genéricos como el código de país. Si se aprueba, el nuevo gTLD podría encontrar la competencia de sectores inesperados".[39]

Que las instituciones financieras adquieran un nuevo nombre de dominio de nivel superior es conveniente para que estas administren sus portales electrónicos en Internet, como lo indicaremos en el siguiente apartado, en la parte de una estrategia para mitigar el fraude por medios electrónicos.

3. Diseño de la estrategia

Tomando en consideración que con el uso de nuevas tecnologías se pueden llevar a cabo ilícitos como el fraude a los clientes de banca electrónica mediante el *phishing*, considero importante plantear una solución en función de los siguientes temas:

1. Con el objeto de que los clientes no sean víctimas del fraude conocido como *phishing*, se tienen que diseñar programas de educación financiera donde se capacite a los usuarios de banca electrónica, para que puedan identificar los elementos que debe tener un sitio seguro en Internet, con el objeto de que el cliente tenga la certeza de que está interactuando en el portal financiero de su institución de crédito; por ejemplo, un elemento de seguridad que tiene que revisar un usuario en Internet es que la página este bajo el protocolo *https* (*Hypertext Transfer Protocol Secure*, es decir, "Protocolo seguro de transferencia de hipertexto"), "que es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras […] generalmente

[39] *Beneficios y riesgos de operar un nombre de dominio*, [http://newgtlds.icann.org/en/about/benefits-risks], consultado el 1 de julio de 2014.

para transacciones de pagos o cada vez que se intercambie información sensible".[40]

Adicionalmente, se tiene que indicar a los clientes que deben verificar los elementos de seguridad que las instituciones de crédito están obligadas a presentar cuando están por iniciar una sesión de banca electrónica, como es la información que el cliente proporcionó a la institución de crédito; además, las instituciones deberán establecer mecanismos y procedimientos para que los usuarios del servicio de banca por Internet *puedan autenticar a las propias Instituciones* al inicio de una sesión, por lo que dichas instituciones deberán proporcionar a sus usuarios información personalizada y suficiente para que estos puedan verificar, antes de ingresar todos los elementos de identificación y autenticación, que se trata efectivamente de la Institución con la cual se iniciará la sesión de banca electrónica. Para ello, las Instituciones podrán utilizar la información siguiente:

a) La que el usuario conozca o haya proporcionado a la Institución, o bien, que haya señalado para este fin, tales como nombre, alias, imágenes, entre otros.

b) La que el usuario pueda verificar mediante un dispositivo o medio proporcionado por la institución para este fin.

2. Como parte de la estrategia, las instituciones de crédito tienen que hacer una inversión para adquirir un nuevo nombre de dominio de nivel superior a través de ICCAN, con el objeto de que bajo la administración de dicho nombre de dominio, migren sus portales financieros y sus plataformas de banca electrónica.

[40] *Diccionario de Informática y Tecnología* [http://www.alegsa.com.ar/Dic/https.php], consultado el 22 de septiembre de 2015.

El objetivo de que las instituciones de crédito migren sus plataformas electrónicas a un nuevo dominio de nivel superior es porque dicho dominio sólo podrá ser operado y administrado por dicha institución de crédito, con lo que se garantiza que ese nuevo dominio de nivel superior no pueda ser usado por un tercero que no esté debidamente autorizado por la institución.

Una vez que se obtenga el registro del nuevo gTLD, se tendrá que hacer del conocimiento de los clientes para que antes de hacer nada, en el portal financiero de la institución de crédito que les presta el servicio de banca electrónica se verifique que dicha página electrónica esté bajo el dominio de su institución para poder tener un elemento de seguridad a los que ya me he referido, a fin de que el cliente identifique y verifique que se encuentra en un sitio en Internet administrado por su banco.

3. Para que la solución sea eficaz, como lo hemos señalado, debe estar acompañado de un programa de educación financiera y divulgación en medios de comunicación directa a los clientes, en donde se den a conocer los elementos de seguridad que debe verificar en su banca electrónica con el fin de se pueda evitar o mitigar el riesgo de *phishing*.

El proceso de educación financiera también debe incluir dar a conocer a los clientes la forma de operar de los *hackers*, es decir, incluir en dichos programas que las instituciones de crédito indiquen cuál es la forma en la actúan estos ciberdelincuentes, para hacer conciencia de la importancia de ubicar los diferentes elementos de seguridad a que me he referido, para evitar se aprovechen del error o el engaño en que pueden incurrir y que les permite obtener datos personales, números de identificación, así como las claves de autenticación tanto fijas como dinámicas para poder ingresar a sus cuentas por los medios electrónicos.

4. No obstante que la solución empresarial está dirigida a las instituciones de crédito, la misma estrategia podría ser implementada por un órgano regulador bancario, que, en este caso, considero que el más indicado sería la Comisión Nacional Bancaria y de Valores, organismo que tiene a su cargo la regulación y supervisión en materia de medios electrónicos, en la que puede establecer como obligación que todas las instituciones de crédito migren sus portales financieros a un nombre de dominio *.cnbv* con el mismo enfoque que hemos señalado, además de que podemos sumar a la Comisión Nacional de la Defensa de los Usuarios de Servicios Financieros, con el objeto de que difunda en medios masivos los elementos de seguridad que debe considerar el cliente de banca electrónica en los portales de sus instituciones de crédito.

Conclusión

Conclusión

La finalidad práctica de usar los nuevos nombres de dominio de nivel superior (gTLD) es brindar certeza a los clientes para que tengan conocimiento de están operando en una página de su institución de crédito, sin embargo, la base será la educación financiera y la difusión a los clientes de banca electrónica, ya sea por medio de cursos, propaganda, folletos, notas informativas, noticias, desplegados u otros para que conozcan qué elementos debe tener el portal financiero con el cual interactúan y no utilicen otro sitio que pudiera aparentar ser auténtico que utiliza un dominio genérico como lo son *.com* o *.com.mx.*

Con la solución planteada, además de dar certeza a los clientes, la institución de crédito puede tener beneficios, ya que al dar a conocer las medias de seguridad a que me he referido, evitará aclaraciones de los clientes que representan costos directos e indirectos en los que incurre, esto sin contar el detrimento que sufre en la parte reputacional frente a los usuarios, que es un último elemento imposible de cuantificar y que ante un mal manejo en redes sociales puede causar cierto agravio a cualquier institución.

Es necesario implementar este tipo de soluciones en virtud de que nuestra legislación en materia penal, aunque pudiera estar preparada para perseguir dichos delitos, los agentes de Ministerio Público de las procuradurías de justicia al día de hoy no están preparados para poder investigar y perseguir dichos delitos informáticos, por lo que hasta en tanto las autoridades no evolucionen a un mayor conocimiento de las nuevas tecnologías de la información y comunicación, las empresas deberán implementar esquemas como el de adquirir un nombre de dominio de nivel superior para así brindar un elemento adicional de seguridad a los usuarios de los servicios financieros por Internet.

Bibliografía

Carranca y Trujillo, Raúl y Carranca y Rivas, Raúl, *Código Penal Anotado*, 21 ed. México, Porrúa 1998.

De Pina, Rafael, *Diccionario de Derecho*, 3ª. ed., México, Porrúa 1973.

Díaz de León, *Marco Antonio. Vademécum Penal Federal*, 3ª. ed. México, 2007.

García Ramírez, Sergio y Adato de Ibarra, Victoria. *Prontuario del Proceso Penal Mexicano*, 5ª ed., México, Porrúa 1988.

.

Nava Garcés, Alberto E., *El derecho en la era digital,* México, Porrúa, 2013.

_____, *La prueba electrónica en materia penal, México,* Porrúa, 2011.

_____, *Delitos informáticos*, 2ª ed., México, Porrúa, 2007.

_____, Análisis de la legislación penal mexicana en informática, 1ª ed. México, Ubijus, 2015.

Pérez Kasparian, Sara, *Manual de delitos en particular,* 2ª ed., México, Porrúa, 2014.

Pérez Segura, Osiris Berenice, *Contratos y transacciones por medios electrónicos*, México, Trillas, 2013.

Jurisprudencia

Tesis II.2o.P.137 P, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t XIX, junio de 2004, p. 1441.

Mesografía

"Alerta policía cibernética por fraudes en banca electrónica", *NorteDigital.mx* [http://www.nortedigital.mx/article.php?id=44848], consultado el 22 de noviembre de 2013.

Amipci, "Crece el uso de la banca electrónica en México: 30 por ciento de los internautas hace transacciones en la banca electrónica", [http://www.amipci.org.mx/?P=articulo&Article=184], consultado el 24 de noviembre de 2013.

Beneficios y riesgos de operar un nombre de dominio, [http://newgtlds.icann.org/en/about/benefits-risks], consultado el 1 de julio de 2014.

Circular única de bancos, Capítulo X de la Comisión Nacional Bancaria y de Valores.

Código penal para el Distrito Federal.

Condusef, Alerta de nuevo correo apócrifo presuntamente enviado por BBVA Bancomer [http://www.condusef.gob.mx/index.php/prensa/comunicados-2014/1021-condusef-alerta-de-nuevo-correo-apocrifo-presuntamente-enviado-por-bbva-bancomer], consultado el 26 de febrero de 2014.

____, Alerta por correo falso presuntamente enviado por BBVA Bancomer [http://www.condusef.gob.mx/index.php/prensa/comunicados-2015/1145-alerta-condusef-por-correo-falso-presuntamente-enviado-por-bbva-bancomer], consultado el 14 de enero de 2015.

DelitosInformáticos.com
[http://www.delitosinformaticos.com/03/2012//fraudes/informacion-sobre-phishing-ofertas-de-trabajo-falsas-y-blanqueo-de-capitales#.UxyN2fl5MxM], consultado el 8 de marzo de 2014.

Diccionario de Informática y Tecnología [http://www.alegsa.com.ar/Dic/https.php], consultado el 22 de septiembre de 2015.

Guía del solicitante de gTD [https://archive.icann.org/es/topics/new-gtlds/rfp-clean-30may11-es.pdf], consultado el 29 de junio de 2014.

Los nuevos gTLD y los usuarios de Internet [http://www.newgtldsite.com/es/nuevos-gtlds-para-usuarios.html], consultado el 30 de junio de 2014.

Manual para identificar y notificar correo fraudulento (*phishing scam*) [http://www.seguridad.unam.mx/documento/?id=81], consultado el 22 de noviembre de 2013.

Nativos e inmigrantes digitales [http://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf], consultada el 15 de abril de 2016.

Nombres de dominio de primer nivel [http://www.pyme.net.uy/documentos/codigos_dominios.htm], consultado el 28 de junio de 2014.

Origen de los dominios [http://www.refineriaweb.com/panel/knowledgebase/6/Origen-de-los-Dominios.html], consultado el 18 de junio de 2014.

Phishing, [http://www.seguridad.unam.mx/usuariocasero/diccionario/?txtbusq=phishing], consultado el 22 de noviembre de 2013.

Phishing scam, [http://www.seguridad.unam.mx/usuariocasero/eduteca/main.dsc?id=166#queEs], consultado el 7 de marzo de 2014.

Phishing [http://www.ecured.cu/index.php/Phishing], consultado el 8 de marzo de 2014.

Protege tu información, Banca *online* [http://www.protegetuinformacion.com/docs/11/banca_online_2_phising.pdf], consultado el 8 de marzo de 2014.

Qué es el *phishing* [http://www.microsoft.com/business/eses/Content/Paginas/article.aspx?cbcid=125], consultado el 25 de febrero de 2014.

Registra Condusef nuevo caso de *phishing* contra usuarios de BBVA Bancomer [http://www.condusef.gob.mx/index.php/comunicados-de-prensa/1196-nuevo-caso-de-phishing-bbva], consultado el 16 de septiembre de 2015.

Se incrementan las reclamaciones en la banca remota [http://www.condusef.gob.mx/index.php/comunicados-de-prensa/1236-se-incrementan-las-reclamaciones-en-la-banca-remota], consultado el 16 de septiembre de 2015.

Symantec, *Tendencias de seguridad cibernética en América Latina y el Caribe*, publicado en junio de 2014.