CAPÍTULO III.- EL PHISHING COMO NUEVA MODALIDAD DE FRAUDE EN LA ERA DIGITAL

Autores: Carlos Alcívar Trejo, Mgs.
Coordinador Académico y Docente de la Facultad de Derecho de la Universidad Tecnológica ECOTEC

Juan Tarquino Calderón Cisneros, Mgs.
Docente Titular de la Facultad de Ciencias de la Salud de la Universidad Estatal de Milagro (UNEMI).

INTRODUCCIÓN

El proceso de revisar tu estado de cuenta bancaria, cambio de contraseñas, transacciones de dinero y mucho más ha sido un beneficio de las entidades bancarias hacia sus clientes pero una de las desventajas para estos procesos es el tiempo ya que para realizar cada uno de ellas se debería de disponer un tiempo específico para acercarse al banco, como nuestra sociedad ha ido creciendo a pasas agigantados en cuanto al mundo tecnológico los propietarios de las cuentas bancarias ya sean estas cuentas corrientes o cuentas de ahorros, cada vez tienen menos tiempo para poderse acercar a las entidades a realizar sus transacciones debido a sus múltiples ocupaciones.

Por tal motivo aproximadamente desde hace 5 años se ha venido realizando este tipo de transacciones de manera online la cual permite al usuario que desde cualquier parte del mundo pueda tener acceso a la información de su cuenta bancaria y también realizar consultas online con servicio al cliente y realizar transacciones bancarias en menor tiempo y sin interrumpir sus labores cotidianas. En el siguiente texto se describirá el delito informático que se comete contra la información bancaria y la manera de hacer phishing en contra de una entidad bancaria.

EL término phishing fue creado a mediados de los años 90 y proviene de la palabra inglesa “fishing” que significa pesca, esto hacía alusión a que la persona que lo realizaba lo que pretendía es que el dueño de la cuenta pueda morder el anzuelo, y la persona que realiza esta actividad se lo llama phisher(etapa,2016).

El término phishing fue creado por crackers que intentaban obtener las contraseñas de los miembros de AOL para utilizarlas con propósitos específicos como eran: usar los servicios de la compañía AOL a través de números de tarjetas de crédito.

El phishing en AOL estaba relacionado con la comunidad warez que se dedicaba a intercambiar softwares falsificados (etapa, 2016). El phisher una vez que ya había obtenido el código de acceso al sistema como trabajador de la compañía AOL lo que hacía era enviar correo a las víctimas que ya se habían establecido con el fin de que la víctima diera información relevante para ellos. Una vez que el usuario enviaba su contraseña el phisher podía tener acceso a la cuenta de la víctima y utilizarla para diferentes delitos y beneficio propio.

En 1997 la compañía AOL reforzó su política de seguridad con respecto al phishing y los warez por la cual fueron expulsados de los servidores de la compañía además de eso ellos como seguridad en el sistema de mensajería incluyeron un mensaje que decía (<<Nadie que trabaje en AOL le pedirá su contraseña o información de facturación >>) y desactivaban las cuentas que habían sido inmersas en phishing de manera automática antes de que las víctimas respondieras los mensajes fraudulentos.

De acuerdo con el informe anual "Fraudes en Línea al Consumidor en Instituciones Financieras", elaborado por RSA, la división de Seguridad de la empresa EMC, el 82 por ciento de los titulares de cuentas son menos propensos a responder un correo electrónico de su banco debido a las estafas de phishing.

Para evitar ser víctimas de un fraude electrónico, el 91 por ciento de los titulares de cuentas bancarias encuestados están dispuestos a utilizar un nuevo método de autenticación más allá del usuario y contraseña.

Sin embargo, la confianza de los usuarios en la banca electrónica sigue disminuyendo, ya que ahora están más conscientes de las amenazas.

Al menos el 70 por ciento de los encuestados está familiarizado con el término phishing, en tanto que el 44 por ciento mostró una preocupación ante el incremento de otro tipo de ataques con virus o troyanos.

Buscan otra protección

Aunque el 90 por ciento de los usuarios encuestados están dispuestos a utilizar un método de seguridad distinto a las contraseñas, las preferencias varían pues van desde dispositivos tokens, imágenes personalizadas y autenticación basada en el riesgo.

El 73 por ciento se inclinó por el uso de autenticación basada en el riesgo, que implica una evaluación de la identidad del usuario incluyendo la ubicación de conexión al sistema, dirección de internet y comportamiento de la transacción.

“Para el 2007 la firma prevé que la seguridad de la banca en línea evolucione, pero al mismo tiempo esperan un incremento en las amenazas informáticas”. (Valencia, 2007, p.7)

El delito informático produce un impacto económico negativo: no solo el daño directo para el que sufre o asume la estafa, sino también las pérdidas derivadas de la erosión de la imagen del suplantado; ambas provocan un impacto social, que se traduce en un freno al desarrollo de la Sociedad de la Información.

• El spam o mensajes de correo electrónico no solicitados que son enviados en cantidades masivas a un número muy amplio de usuarios suponen, en muchos casos, la cabeza de puente para la comisión de un fraude electrónico (phishing, scam, “cartas nigerianas”, bulos, etc.).

Observatorio de la Seguridad de la Información

• Una primera clasificación distinguiría entre los delitos que tienen su origen en técnicas de ingeniería social y los que tratan de aprovecharse de vulnerabilidades de los sistemas. No obstante, en algunos ciberdelitos se combinan ambos orígenes.

Siguiendo el Código Penal español de 1995, se distingue entre los supuestos basados en técnicas de ingeniería social, que son tipificados en el mismo apartado que las estafas tradicionales (Art. 248.1 Código Penal), y los supuestos de utilización de código malicioso (malware) o de intrusión en sistemas de información recogidos en el artículo 248.2 del CP.

Dentro del primer grupo se encuentran algunas de las estafas tradicionales “puestas al día” para el mundo Internet. Forman parte del segundo grupo aquellos fraudes que utilizan códigos maliciosos o métodos de intromisión ilegal en los sistemas de información, por lo que es normalmente necesaria, una mayor habilidad técnica por parte del ciberdelincuente. (INTECO, 2007)

Definición de Delito Informático

Aunque no hay una definición específica acerca de “Delito Informático”, varios tratadistas y doctrinarios en el tema han hecho el esfuerzo por dilucidar un concepto claro y conciso respecto a este ilícito de la nueva era. Es así que entre los más conocidos tenemos las siguientes definiciones:

Nidia Callegari define al “delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas”. El Departamento de Investigación de la Universidad de México, señala como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático”. El italiano Carlos Sarzana, define el Delito Informático como "cualquier

comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".

María de la Luz Lima dice que el "delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el Delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. (Conde et al., 2009)

Definición de Phishing

Es una técnica que se utiliza para duplicar una página web o manipular el diseño de correo electrónico logrando que cualquier enlace que generen los phishers parezca legítimo y así hacen creer al usuario que se encuentran en una página oficial y que el correo que reciben proviene de una identidad segura y lo utilizan generalmente en páginas de instituciones bancarias para poder tener el login y la contraseña del cliente de la institución y así poder realizar diversos delitos.

Carlos Lang, presidente de Hauri Latinoamérica comenta que aun cuando este ilícito en el país es menor respecto a lo que sucede en Estados Unidos y Brasil, las pérdidas asumidas por las instituciones financieras mexicanas están en franco aumento.

Durante el 2004, precisa a El Economista, los fraudes cometidos en contra de los clientes o usuarios, tuvieron un costo para las instituciones financieras de más de 11 millones de dólares, cifra que para el primer trimestre de este año ascendió a 50 millones de dólares.

Esto es, que, en tan solo tres meses, los costos por este ilícito no solo superaron la cifra total que se reportó en un año, sino que aumentó cinco más, de ahí la importancia de contar con soluciones tecnológicas que permitan proteger a los usuarios y clientes de la banca, destaca.

Además, de que ya no se habla de hackers sino de la participación de bandas organizadas, agrega.

"Ya no es un muchacho que está con su computadora en la noche tratando de ingresar al sistema de una compañía para inyectar un virus o simplemente tener acceso a su información, sino que ya hablamos de bandas organizadas que se dedican al fraude por el internet", refiere.

Con base en las estadísticas de la Policía Federal Preventiva al 2004, cinco de los grupos financieros más importantes del sistema financiero han resultado ser los más afectados:

HSBC con 28%, Bancomer con 22%, Banamex con 21%, Banorte con 19%, Santander Serfin con 8.0% y Banco Azteca con 2.0 por ciento.

Debe quedar claro que el objeto de fraude no es el banco, sino el cliente o usuario, ya que las instituciones mexicanas cuentan con todos los mecanismos de seguridad en sus servidores y áreas de comunicación.

Situación que no se observa en el sistema bancario de Estados Unidos, en donde de acuerdo con sus leyes, el culpable del fraude es el cliente o usuario, los cuales durante el 2004 asumieron una perdida por 2.4 billones de dólares. (Reynold, 2005)

Métodos de phishing

URLs manipuladas, o el uso de subdominios los cuales son trucos comúnmente utilizados por los phishers ejemplo: http://www.nombredelbanco.com/ejemplo, el cual no es la dirección original si no que se agrega algo al final que direccione a otro enlace para capturar la información.

Para disfrazar enlaces utilizando en las direcciones de las páginas el símbolo @ para así poder solicitar usuario y contraseña y captar esa información ejemplo: http://www.nombredelbanco.com@members.tripod.com/ en la que el usuario cree que ingresa a un sitio oficial pero en realidad está ingresando a members.tripod.com/ solo para capturar los datos. (UAL, 2016)

El método Cross siete Scripting en este ataque utilizan el propio código del banco para que todo el ambiente parezca oficial de la institución bancaria y el cliente recibe un mensaje diciendo que debe verificar sus cuentas, la cual es un enlace modificado para obtener datos del cliente.

El phishing se ha sofisticado y mutando, lo que ha hecho que cada vez sea más difícil prevenirlo o encontrar a sus autores. Los phishers ya no sólo utilizan los correos electrónicos para enganchar a sus víctimas, sino que se valen de nuevas tácticas. Han alcanzado tales niveles, que ahora con la variante del spear phishing pueden localizar de manera focalizada a una víctima para defraudarla. También estos delicuentes lo que están haciendo es diseñar las páginas de phishing en Flash, en vez de lenguaje HTML, para evitar así las herramientas que existen en contra de este ataque. Entrevistado por TECNOLOGÍA, Alfredo Reyes Krafft, Vicepresidente Ejecutivo de la Asociación Mexicana de Internet (AMPICI), explicó las diversas formas de ataque que utilizan los phishers?: El phishing se puede hacer a través de correo tradicional, a través del teléfono por medio de un centro de contacto, por un mensajero instantáneo o incluso a través de aplicaciones como Google Talk?. Puntualizó que esta nueva

forma de realizar ataques para robo de identidad se debe a que son más intrusivos; como el correo electrónico ya puede detectar si un mensaje es spam o no lo es, los usuarios se toman más tiempo en revisar sus bandejas de entrada. En cambio, si reciben una liga por medio de un mensaje instantáneo en su PDA o teléfono inteligente, por la premura es más probable que los usuarios accedan a los sitios de phishing. Incluso, a través de un mensaje de texto, SMS, en teléfonos celulares que tienen acceso a Internet, se puede realizar un fraude. Ataque nuevo, métodos tradicionales (Nájera, 2017).

Juan Carlos Guel, jefe de Seguridad en Cómputo de la UNAM, reveló que, según datos de la Secretaría de Seguridad Pública federal, entre el 1 de enero y la primera quincena de abril, las autoridades tomaron conocimiento de 884 casos, cuando en el primer cuatrimestre de 2008 fueron 461.

El especialista en delitos cibernéticos detalló que en todo 2008 se reportaron mil 396 incidentes de ese tipo, es decir, que el promedio semanal fue de 29 eventos, mientras que en este año es de 59.

A este ritmo, el récord de 2008 será superado en junio, e incluso podría llegar a los 2 mil 50 casos que se reportaron en 2006, que es el máximo que la Policía Cibernética registra desde hace tres años, cuando el "phishing" comenzó a representar una amenaza para las instituciones mexicanas y sus usuarios.

Guel advirtió, durante una ponencia en la UNAM, que esa tendencia es preocupante porque las dependencias y los bancos ya han mejorado sus "candados" electrónicos y sistemas de seguridad virtual.

Incluso, en 2007 se creó "E-Crime", un grupo interdisciplinario en el que participan gobierno, academia, iniciativa privada y asociaciones civiles, para analizar la problemática e implementar acciones conjuntas para reducir los delitos en internet.

Según el especialista, el tipo de "phishing" más recurrente en México es que sufren las instituciones bancarias y que consiste en el envío masivo de correos electrónicos provenientes de supuestos entes oficiales y benéficos, pero cuyo objetivo es el de obtener información financiera confidencial -como nips o números de cuenta- para realizar fraudes (Baranda, 2009).

El phishing funciona de tres maneras

- Haciendo que respondas un correo electrónico en el cual podrá hacerse pasar por cualquier institución y solicitar datos personales, o usuario y contraseña de dicha institución.

- Haciendo que la víctima haga clic en un enlace que los phisher envía por correo electrónico suplantando una página web y solicitando loogin y contraseña.
- Simplemente haciéndote enviar un mensaje de texto con usuario y contraseña para validación de información tomando el puesto de una institución. (UAL, 2016)

Las identidades que pueden verse suplantadas son:

- Bancos
- Instituciones Públicas (Policía, SRI, etc.…)
- Centros Educativos (Universidades)
- Entre otras.

Las medidas que han tomado las entidades bancarias

Actualmente, como medida de seguridad, los bancos han creado unos teclados virtuales con orden alfabético aleatorio para que de esa manera la información que se ingresa ahí como login y contraseña no sea interceptada por un keylogger ni por cualquier información ilícita.

Además de ellos han agregado en sus páginas oficiales comunicados en la cual indica que el banco no solicita información personal ni cambio de clave por medio de correo electrónico ni sincronizaciones de tarjetas de crédito.

También se han agregados números telefónicos para que se comuniquen con servicio al cliente si reciben información sospechosa.

La única información enviada por entidades bancarias

- Acceso éxito
- Acceso denegado
- Notificación cuando ocurre cambio de contraseña
- Mensajes de bienvenida
- Solicitudes de código de autorización
- Modificación de clave de débito
- Activación de tarjeta de débito
- Transacciones realizadas (pagos,retiros,transferencias). (BP, 2016)

¿Cuál es la finalidad del Phishing?

- Fraude y robo en instituciones bancarias.
- La suplantación de Identidad
- Envíos de Virus y span para ocasionar caos.
- Robo de datos personales

El Phishing Una Nueva Modalidad De Fraude En Ecuador:

Bogotá, 23 feb (EFE). - Brasil y Ecuador fueron los países latinoamericanos con mayor cantidad de víctimas en 2015 de ataques "phishing", en los que los usuarios son engañados mediante correos electrónicos o páginas falsas, según un estudio mundial sobre seguridad en internet.

"Latinoamérica siempre ha sido un territorio bastante atractivo para los criminales cibernéticos y, por ello, podemos ver, además, la presencia de los países de la región en el 'top' de los emisores de 'spam'", dijo hoy a Efe Dmitry Bestuzhev, director para América Latina del equipo de Análisis e Investigación Global de la compañía de seguridad informática Kaspersky Lab, firma autora del estudio.

El estudio indica que Japón es el país con mayor número de usuarios afectados por "phishing", con un 21,68 %, seguido de Brasil (21,63 %), India (21,02 %), Ecuador (20,03 %) y Mozambique (18,30 %).

Según el informe, los temas más usados el año pasado para este tipo de fraudes fueron los Juegos Olímpicos en Brasil, la situación política de Ucrania, la guerra en Siria, las elecciones en Nigeria y el terremoto en Nepal.

El documento muestra también que Estados Unidos sigue siendo la mayor fuente de "spam" o correo no deseado del mundo (15,2 %), seguido por Rusia (6,15 %), Vietnam (6,13 %) y China (6,12 %).

Dentro de las naciones latinoamericanas, Argentina (2,90 %) ocupa el lugar nueve, Brasil (2,85 %), el puesto diez, y México (1,93 %), el quince.

En cuanto a víctimas de "spam", Alemania figura en el primer puesto con 19,06 % de los ataques, seguido por Brasil (7,64 %) y Rusia (6,03 %).

El informe detalla que el volumen de correos electrónicos no deseados el año pasado se redujo hasta el 55,28 % del total, lo que representa un descenso del 11,4 % respecto al año anterior, y advierte que los dispositivos móviles son el nuevo objetivo para los ataques o fraudes informáticos.

"Aún se vive en la ingenuidad de pensar que los dispositivos móviles no son vulnerables a los ataques informáticos. Dichas circunstancias le hacen el escenario perfecto para los atacantes", indicó Bestuzhev.

En 2015, los ciberdelincuentes continuaron enviando correos electrónicos falsos desde dispositivos móviles y notificaciones de aplicaciones móviles que contenían malware o mensajes publicitarios, sostiene el informe.

"El aumento del uso de dispositivos móviles en nuestra vida diaria para intercambiar mensajes y datos, así como para tener acceso y controlar cuentas bancarias, también ha tenido como resultado el aumento de oportunidades de explotación para los ciberdelincuentes", afirmó Daria Loseva, experta en Análisis de Spam de Kaspersky Lab.

"Por tal razón, los usuarios de dispositivos móviles tienen que estar atentos y no bajar la guardia, ya que las actividades de los ciberdelincuentes en esta área es muy probable que aumente, junto con nuestra dependencia de los dispositivos", agregó. (EFE, 2016)

En Latinoamérica, el 21% de los internautas hacen transacciones en línea todos los días, pero un 42% hace menos de una al mes o no usa este mecanismo de pago.

¿Por qué? El temor al robo o fraude electrónico y la percepción de que no es seguro es la principal razón citada por casi de cuatro de cada 10 de ellos.

Esta es una de las conclusiones del informe Visión de los Consumidores Latinoamericanos sobre el Fraude Electrónico 2013", realizado por Easy Solutions en Costa Rica, República Dominicana, Panamá, Colombia, Venezuela, Ecuador, Chile, Argentina, México y Brasil.

Aun así, la banca móvil y en línea continua su crecimiento en términos de uso y preferencia, mientras que las oficinas físicas y los cajeros electrónicos pierden favoritismo.

Internet se mantiene como el canal más frecuentemente usado para las transacciones bancarias (el 77% de los encuestados manifestó su predilección por este canal). Los usuarios optaron por este canal en promedio 3,9 veces por mes, y el 65% de ellos realiza algún tipo de transacción al menos una vez a la semana (Jiménez, 2015).

Kaspersky Lab anunció el descubrimiento de una nueva campaña de ciberespionaje con el nombre clave de 'Machete', la cual se ha dirigido a víctimas de alto perfil, incluyendo gobiernos, fuerzas militares, embajadas y las fuerzas del orden desde hace por lo menos 4 años.

El campo principal de su operación ha sido América Latina: la mayoría de las víctimas parecen estar ubicada en Venezuela, Ecuador y Colombia. Entre otros países afectados se encuentran Rusia, Perú, Cuba y España.

El objetivo de los atacantes es recopilar información sensible de las organizaciones comprometidas. Hasta ahora es posible que los atacantes hayan podido robar gigabytes de datos confidenciales exitosamente.

Parece ser que los cibercriminales de América Latina están adoptando las prácticas de sus colegas en otras regiones. Anticipamos que el nivel tecnológico de los cibercriminales locales aumente considerablemente, por lo que, probablemente, nuevas campañas de ataques

dirigidos pueden llegar a ser muy similares, desde el punto de vista técnico, a aquellas consideradas como las más sofisticadas del mundo" dijo Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky Lab.

Con base en la evidencia descubierta durante la investigación de Kaspersky Lab, los expertos concluyeron que los atacantes de la campaña parecen hablar español, y tener raíces en algún lugar de América Latina

La mejor protección contra campaña de ciberespionaje tales como Machete es aprender como el spear-phishing funciona y no caer en sus trampas, así como contar con una solución de seguridad funcional y actualizada. Los productos de Kaspersky Lab identifican y protegen contra este ataque dirigido.

ANÁLISIS LEGAL

Con el rápido avance de la tecnología en los últimos 30 años cada vez a pasos más acelerados y la democratización del acceso al Internet en casi todo el planeta, podemos decir sin lugar a dudas que el mundo se ha digitalizado. Desde los aspectos más humanos y sensibles como la música o el cine, hasta los más especializados procesos y actividades desarrolladas por el hombre, como son las complejas transacciones financieras que hoy en día atraviesan el mundo en fracciones de segundo se manejan hoy a través de computadores y redes globales.

Constitución Del Ecuador

Comunicación e Información

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.

Sección novena

Personas usuarias y consumidoras

Art. 52.- Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características.

La ley establecerá los mecanismos de control de calidad y los procedimientos de defensa de las consumidoras y consumidores; y las sanciones por vulneración de estos derechos, la reparación e indemnización por deficiencias, daños o mala calidad de bienes y servicios, y por la interrupción de los servicios públicos que no fuera ocasionada por caso fortuito o fuerza mayor.

Sección cuarta

Acción de acceso a la información pública

Art. 91.- La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley.

Sección quinta

Acción de hábeas data

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP)

SECCIÓN TERCERA

Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de

tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.