

DELITOS CIBERNÉTICOS

*Ing. Alejandro Peña Casanova
**M.A. José Raymundo López Esparza
***Lic. Víctor Manuel León León
****Yohana Saldívar Ovando Valencia

*Ingeniero en Sistemas Computacionales. Ingeniero en Sistemas Computacionales. Egresado del Instituto Tecnológico de Querétaro. Profesor en el Instituto Tecnológico de Villahermosa. Estudiante de la Licenciatura. En Derecho. Universidad Juárez Autónoma de Tabasco. E mail: apena_mx@yahoo.com.

**Contador Público egresado de la Universidad Nacional Autónoma de México. Profesor en el Instituto Tecnológico de Villahermosa. E mail: rayesparza@hotmail.com

***Contador Público egresado de la Universidad Juárez Autónoma de Tabasco. Profesor en el Instituto Tecnológico de Villahermosa. E mail: león-victor@hotmail.com

**** Alumna de la Carrera de Ingeniería en Sistemas Computacionales. Instituto Tecnológico de Villahermosa.

Artículo Recibido: 20 de enero 2017. Aceptado: 10 de marzo 2017.

RESUMEN. En el año 2016, se llevó al cabo una investigación documental para describir cuáles son los delitos más comunes que se cometen utilizando computadora y dispositivos móviles a través de la INTERNET, así mismo se muestran recomendaciones para tratar de evitar dichos actos delictivos. Este tipo de delitos son regulados, principalmente, por las ramas del Derecho Penal, Mercantil, Civil y Derecho Informático.

Palabras Clave: Cibernética. Ciberdelitos. Informática. Internet. Dispositivos móviles.

INTRODUCCIÓN.

Los delitos informáticos, cibernéticos o ciberdelitos son aquellos que regularmente se cometen a por medio de una computadora o dispositivo móvil a través de la Internet y la mayoría de las veces se perpetran desde lugares y países lejanos

para tratar de evitar la aplicación de las leyes y hacer más difícil su aplicación. La Procuraduría General de Justicia del Distrito Federal. PGJDF (2011) señaló en el año 2011, que los delitos más comunes de este tipo son: 1.-Pornografía Infantil. 2).-Fraudes electrónicos. 3).-Extorsión por

medio de la internet o mensajes instantáneos. 4).-Robo de identidad. 5).- Comercialización de videos y música sin autorización. A las personas que cometen este tipo de delitos se les denomina hackers o crackers y regularmente son personas inteligentes, profesionistas, con elevados conocimientos en computación. La proliferación de este tipo de ilícitos se debe al elevado crecimiento del número de computadoras y de dispositivos móviles inteligentes en el mundo y al incremento del acceso a los servicios de redes interconectadas a través de casi todos los países por medio de la Internet. Tan solo en México, en el año 2014 había 52.3 millones de usuarios **(INEGI, 2014) y en el mundo había más de tres mil millones de internautas (Vanguardia, 2014)**, lo cual ha tenido consecuencias de que cualquier persona pueda acceder a información de todo tipo (cuentas bancarias, claves secretas, direcciones de correo electrónico, etc.), desde su dispositivo ubicado en cualquier lado del planeta sin tener que desplazarse físicamente a algún lugar. Este tipo de delitos se realizan de manera virtual y son muy difíciles de rastrear ya que se llevan al

cabo en cuestión de segundos, en todo tipo de países y en algunos de ellos no existen convenios de colaboración entre autoridades para combatir estos ilícitos y las personas que se dedican a esto, poseen a veces, elevados conocimientos informáticos, los cuales les permiten borrar y no dejar rastro o huella de las actividades maliciosas que realizan. Este ensayo trata de conceptualizar los delitos cibernéticos más comunes y de qué manera pueden ser prevenidos.

DESARROLLO.

Según diversas fuentes, los delitos cibernéticos más comunes son:

1).-Venta de bienes o servicios que resultan ser falsos.

Este tipo de delitos cibernéticos ha tenido mucho auge, consiste en estafar a las personas vendiendo productos muy por debajo del precio del mercado o se les atribuyen propiedades y cualidades milagrosas que no tienen o se colocan imágenes que no corresponden a la realidad, la gente los compra en línea y nunca reciben dichos productos o se reciben otros que no son los anunciados o

se reciben incompletos, también se ofrecen servicios, por los cuales se cobran cantidades pequeñas por adelantado y no se cumplen de ninguna manera, lo cual hace muy difícil su persecución debido al monto de que se trata, sin embargo los estafadores acumulan grandes ganancias pues estafan a un número elevado de personas.

2).-Suplantación de identidad (pishing).

En este tipo de estafa por medio de la Internet, se obtienen de manera fraudulenta números de tarjetas de crédito, cuentas bancarias, claves de acceso, contraseñas e información personal para después utilizarse de manera ilegal en compras, retiros de dinero y otras actividades a nombre de la persona, cuando en realidad es otra las que la realiza. En este tipo de delito se suplanta el nombre o la imagen de algún banco o empresa real y se engaña a la víctima para que proporcione datos personales sin saber que está siendo engañado. Existen varias formas para cometer estos delitos, algunas de ellas son: por medio del envío de correos electrónicos fraudulentos, publicación de sitios web falsos, acceso a ligas de sitios web maliciosos, aparición de

ventanas emergentes cuando la persona se encuentra navegando en Internet y mensajes de texto hacia celulares pidiendo datos personales. Según datos de la CONDUSEF en México, los delitos de suplantación de personalidad subieron de 352,000 a 700,000 en tan solo cuatro años y los hackers obtuvieron dos mil millones de pesos en el año 2014 por concepto de operaciones ilícitas.

3).-Acoso cibernético.

Este tipo de delito llamado grooming o cyberbullying ha proliferado en la actualidad a través de las redes sociales, en los salones de chat, a través de mensajes de texto, videos o correos electrónicos y consiste en actividades de acoso sexual, amenazas, chantajes, extorsión y otras manifestaciones ilícitas que llevan al cabo personas malintencionadas denominadas cyberstalkers o depredadores en línea. Las víctimas principales son menores de edad entre 12 y 17 años, mujeres o personas mayores de edad o carentes de experiencia informática, los cuales sin ningún problema proporcionan datos personales e información confidencial a través del ciberespacio otorgando a los delincuentes herramientas para llevar al

cabo sus ilegales propósitos de acoso hacia otras personas. Según Rodas(2015), 18 millones de menores en México están expuestos a este tipo de delitos y se tienen documentados cuarenta mil casos, los cuales podrían ser más ya que una gran cantidad de ellos no se documentan.

4).-Pornografía Infantil.

Este es uno de los delitos más aberrantes que existen sobre la tierra y consiste en la distribución de material pornográfico a través de la Internet en donde se muestra a niños y niñas manteniendo relaciones sexuales con adultos o dichos menores de edad son abusados física o psicológicamente. El material pornográfico es explícito y puede distribuirse a través de videos, fotografías, escritos y otros medios digitales. El artículo 2 de la Convención sobre los Derechos del Niño de la Organización de las Naciones Unidas conceptualiza la pornografía infantil como:

“Toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes

genitales de un niño con fines primordialmente sexuales.”

La pornografía infantil existe desde hace mucho tiempo, sin embargo con la aparición de la Internet su distribución y comercialización ha tenido un enorme auge, inclusive hay personas que comparten o distribuyen este tipo de material sin pedir alguna contraprestación económica. Las actividades que pueden ser delictivas dentro de este rubro, según poder_judicial(2014) son: a).-La venta de este material a través de un medio informático. b).-La distribución del material pornográfico vía Internet. c).-La difusión del material. d).-La adquisición. e).-La posesión de material pornográfico en dispositivos electrónicos o los situados en la nube a través de Internet.

Combatir este tipo de delitos es muy difícil pues se lleva al cabo en el ámbito internacional en donde la legislación, en cada país, es muy diversa y a veces proviene de lugares en donde no se tienen relaciones internacionales ni convenios para combatir este terrible delito.

5).-Llamadas Internacionales falsas.

Este tipo de estafas tiene un gran auge (Consumidor, 2015) se da a través de llamadas, utilizando la Internet u otros dispositivos hacia teléfonos móviles o fijos. Consiste en que el usuario recibe una llamada de un solo timbrado, entonces la persona checa que tiene una llamada perdida de un número de celular que desconoce. Llevado por la curiosidad o porque tal vez está a la espera de una llamada de este tipo, el usuario regresa la llamada al número que le marco y allí inicia la estafa. Al contestar se reciben mensajes ya sea de máquinas automáticas o de personas los cuales contestan frases como: “Espere un momento, está siendo atendido.....”, sin embargo allí inicia el cargo de llamadas internacionales y este tipo de acciones a veces son bastante caras debido a que estamos llamando a lugares en África o el Caribe u otros destinos lejanos del lugar de nuestra residencia, con el consiguiente cargo en la factura de nuestro proveedor de telefonía o si tenemos precargado saldo inmediatamente lo descuentan con el costo de la llamada que estamos haciendo. También aquí se pueden encuadrar las llamadas a números telefónicos de lugares

de diversión, de chats, o sitios de adultos o el mal uso de nuestro número para otros fines, ya que continuamente vemos sitios web, los cuales para cualquier trámite nos solicitan nuestro número de celular y nosotros lo proporcionamos, después de estas acciones nos llegan cargos elevados en las facturas del servicio, los cuales desconocemos e inicia un tortuoso camino con nuestro proveedor de servicios telefónicos para tratar de revertir esta situación.

6).-Oportunidades falsas de trabajo.

Las altas tasas de desempleo y la dificultad de obtener uno bien remunerado a potenciado este tipo de delitos a través de la Internet. Por medio de redes sociales o de sitios web, se prometen empleos con salarios muy superiores al promedio o con condiciones diferentes a lo que tradicionalmente se maneja. En algunos países como España, uno de cada cuatro delitos que se cometen por Internet, tiene que ver con la búsqueda de un empleo y con la oferta de oportunidades de trabajo falsas Según (20minutos.es, 2014). En este tipo de delitos se le pide al candidato que deposite ciertas cantidades de dinero a cambio del empleo que va a conseguir o

se les piden información personal o bancaria para utilizarla con fines delictivos.

Algunos de los diversos fines que persigue este tipo de delitos son los siguientes: a).- obtener información personal. Por medio del llenado de formularios o a través del correo electrónico se obtiene el curriculum vitae de la persona, el cual lo adicionan a sus bases de datos o venden dicha información a terceros. La información personal es muy valiosa, pues en ella se encuentran ingresos, domicilio, teléfonos, direcciones de correo electrónico, lugar de residencia y otros datos más que después son utilizados para campañas masivas de venta de todo tipo de productos o de servicios, los cuales muchas veces son fraudulentos. b).- Obtener beneficio económico. Las personas que se dedican a este tipo de delitos a veces utilizan nombres de empresas verdaderas y se hacen pasar por directivos de recursos humanos, pidiendo dinero a los candidatos para que puedan ocupar algún puesto, lo cual resulta falso y estafan a la persona desempleada. Otra forma de obtener dinero ilegal es decirle a la persona que solicita el trabajo que debe de llevar un

curso de capacitación en línea, el cual tiene un costo, el desempleado deposita el monto y nunca recibe dicho curso de capacitación o si lo recibe no sirve para nada y no tiene que ver con el empleo solicitado o lo direccionan a sitios web falsos. Otra forma de lograr dinero de la persona que busca empleo es darle números de teléfono con tarifas especiales a los cuales debe de llamar con el consiguiente desembolso por parte del desempleado, dichos números son de líneas para adultos, de chistes, horóscopos, etc. Que no tienen nada que ver con el empleo ofrecido c).- Conseguir información de tipo financiero. A veces Se le pide a la persona que busca el trabajo información financiera tales como cuentas de bancos o de tarjetas de crédito o débito, con la mentira de que allí le van depositar su salario, sin embargo esto es una mentira para conseguir dicha información para posteriormente hacer uso indebido de ella. c).- Lavado de dinero. Este delito está teniendo auge en la actualidad, se contrata a la persona como intermediario en transacciones financieras ilegales y se le depositan grandes cantidades de dinero a sus cuentas, las cuales él debe de

transferirlas posteriormente hacia otras cuentas y se les da una comisión. Sin embargo lo que está sucediendo con estas acciones es que se puede incurrir en el delito de lavado de dinero al hacer este tipo de transacciones y meterse en graves problemas de tipo legal. d).-Envió masivo de correos. Este tipo de ilícitos sucede frecuentemente, pues los delincuentes al tener los correos electrónicos de la persona que busca el empleo, lo inundan de mensajes con ofertas de empleos inmediatos, empleos bien pagados, les mencionan que llamen antes de 24 hrs. y otras situaciones, las cuales resultan ser un engaño.

7).-Engaño con paquetes de viajes.

Este tipo de fraudes por Internet toma auge muy cerca de los períodos vacacionales o fines de semana largo en México y en otros países. Consiste en ofrecer a las personas, a través de correos electrónicos o sitios web falsos, paquetes de viaje que incluyen transporte, hospedaje, alimentos y bebidas ilimitadas a precios muy por debajo del mercado. Los destinos nacionales más ofrecidos son: Cancún, Acapulco, Puerto Vallarta, Mazatlán y Huatulco. También se ofrecen viajes internacionales hacia las

Vegas, Disneylandia, cruceros y otros destinos más, sin embargo una vez que la persona paga el paquete no le llegan sus datos de reservación ni algún comprobante o a veces llega a su destino y resulta que todo fue un fraude, la reservación no existe o a veces solo existe parte de lo que se ofreció y el hotel y los servicios no son los que se anunciaron. Según el Secretario de Turismo de Quintana Roo, cada mes se reciben entre 8 y 10 denuncias por este tipo de delito (Sipse, 2015).

8).-Casinos en línea.

El fraude por Internet al jugar en casinos en línea está teniendo mucho auge. Se te pide un número de tarjeta de crédito y si pierdes de allí te descuentan lo perdido y si ganas, en la misma tarjeta te abonan tu ganancia. El problema es que si pierdes te descuentan de inmediato, pero si ganas no te lo abonan de inmediato y en el peor de los casos no te pagan nunca. Además te hacen un sin número de cargos sin tu consentimiento hacia tu tarjeta de crédito. El problema surge cuando las personas quieren hacer una reclamación, pero la mayoría de dicho sitios se encuentran en países lejanos en donde su legislación es desconocida, no hay convenios con

México y en nuestro país tampoco hay leyes claras al respecto. Además dichos sitios fraudulentos venden los datos de tus tarjetas bancarias a otros delincuentes con los consiguientes problemas que esto genera.

Una forma de operar de estos sitios es que ofrecen bonos o promociones de inicio, te dicen que si abres una cuenta de cierta cantidad de dinero te regalan el doble o el triple de lo que inicias, sin embargo al momento que abres una cuenta, ellos te argumentan que los bonos no son válidos en todos los juegos y te ponen una lista restringida de diversiones en donde son válidas dichas promociones y la mayoría de las veces no te las hacen válidas. Lo que sí es seguro que tu dinero inicial jamás lo volverás a ver y la mayoría de las veces tampoco vas a ganar nada.

9).-Comercialización de música y videos de manera ilegal.

El tema de la distribución de música o de videos por Internet es complejo. Existen varias formas de bajar contenidos multimedia desde diversos sitios, algunos de ellos son de paga, tales como: i tunes o

Napster, Si pagamos y bajamos la música no constituye ningún delito pues estamos pagando por el producto, sin embargo si dicha música la vendemos o distribuimos a terceros sin permiso de los autores, eso sí constituye un delito, pues estamos comercializando algo que no nos pertenece. Otras veces bajamos música desde páginas que la ofrecen de manera gratuita, lo anterior pudiese constituirse en un delito, ya que son productos que pertenecen a alguien. Existen varias controversias acerca del tema, algunos jueces, como en España (música, 2014), han determinado que no es delito bajar música siempre y cuando sea para que la escuchemos nosotros sin comercializarla ni obtener algún lucro con ella. Sin embargo las legislaciones de otros países no opinan lo mismo y mencionan que es necesario pagar por el servicio.

Por igual podemos usar un sistema de intercambio de música punto a punto (P2P), cuando nos comunicamos directamente con otras computadoras, en esta situación, estamos descargando sin pagar un producto musical o de videos la cual está destinada a ser vendida en

canales comerciales y por tanto según la ley cometemos un delito. Sin embargo, las autoridades no siempre están de acuerdo. Algunos entienden que si la música solo se baja para disfrutar de ella y no para comercializarla ésta práctica no constituye algún delito. En Barcelona, España, el colegio de abogados ha determinado que el bajar material multimedia no constituye algún delito siempre y cuando no se comercialice el producto. Sin embargo debemos de tener cuidado pues en cada país las leyes pueden ser diferentes y podemos estar cometiendo delitos sin saberlo.

Gómez (2013) establece en su página web varios elementos que pueden constituir un delito en México y que continuamente la mayoría lo hacemos: Subir y bajar videos a facebook y YouTube sin permiso expreso de los autores. Elaborar Memes y Gifs con fotografías sin permiso de los participantes. Compartir contraseñas de páginas que ofrecen servicios de televisión o música digital, tales como Netflix y Spotify.

CONCLUSIONES Y RECOMENDACIONES.

Como se puede observar es alarmante el número de delitos que se pueden cometer a través de la Internet utilizando dispositivos electrónicos, así mismo se nota que es relativamente fácil cometer este tipo de ilícitos y es muy difícil castigarlos.

La Policía Cibernética de México, dependiente de la Comisión Nacional de Seguridad, establece de manera general las siguientes recomendaciones de seguridad para prevenir delitos que se realizan a través de Internet, tanto en computadoras de escritorio como en dispositivos móviles inteligentes. (Ciberdelitos, 2014).

Recomendaciones:

- 1.-Sentido Común.
- 2.-No proporcionar información personal ni confidencial a nadie.
- 3.-Instalar software especializado de seguridad en nuestros dispositivos electrónicos.
- 4.-Validar por otros medios las ofertas de trabajo y de productos que recibamos por Internet.

5.-No ingresar a sitios web de dudosa procedencia y reputación.

6.-No bajar material musical, videos, fotografías sin permiso de los autores.

7.-No subir material que no nos pertenece a la red.

8.-No bajar, distribuir, vender, ni reproducir material pornográfico.

9.-Aleccionar a los menores acerca de la seguridad cibernética

10 No amenazar, blasfemar o propagar rumores falsos a través de la Internet.

LITERATURA CITADA.

Ciberdelitos(2014).<http://mexicosos.org/multimedia/infografias/398-7-recomendaciones-evitar-ciberdelitos>).

20minutos.es(2014).<http://www.20minutos.es/noticia/2039298/0/identificar/estafas-laborales/empleo-internet/>.

Consumidor(2015). <https://www.consumidor.ftc.gov/blog/la-estafa-de-un-timbrazo-en-el-telefono-celular-puede-resonar-en-tu-bolsillo>.

Gómez, J.(2013). <http://www.merca20.com/10-cosas-ilegales-que-estas-haciendo-en-internet/>.

<http://archivo.eluniversal.com.mx/nacion-mexico/2015/crece-robo-de-datos-bancarios-en-internet-1102453.html>. <http://www.delitosinformaticos.com/04/2015/delitos/prevenir-ciberdelitos>

<http://www.delitosinformaticos.com/09/2014/delitos/los-delitos-informaticos-mas-comunes-en-nuestro-pais>.

<http://www.elfinanciero.com.mx/nacional/fraude-difamacion-y-amenazas-delitos-online-mas-comunes.html>.

https://es.wikipedia.org/wiki/Convenci%C3%B3n_sobre_los_Derechos_del_Ni%C3%B1o.

INEGI(2014).<http://mexico.cnn.com/tecnologia/2012/11/29/mexico-tiene-409-millones-de-usuarios-de-internet-inegi>.

Música(2004).<https://alhadradigital.wordpress.com/2010/03/03/%C2%BFes-ilegal-descargar-musica-desde-internet/>.

PGJDF(2011).<http://cofradia.org/2011/01/10/los-5-delitos-informaticos-mas-frecuentes-segun-la-pgjdf/>

Poder_judicial (2014). www5.poderjudicial.es/CVdi/TEMA04-ES.pdf.

Sipse(2014). <http://sipse.com/novedades/aumenta-numero-de-fraudes-de-agencias-de-viajes-patito-49413.html>.

Vanguardia(2014). <http://www.vanguardia.com/actualidad/tecnologia/260604-el-40-de-la-poblacion-mundial-tiene-internet>.