Vicerrectoría de Estudios de Posgrados

Trabajo Final para optar por el Título de:

Maestría en Gerencia y Productividad

“Análisis de los Fraudes en los Sistemas Electrónicos de la Banca de la República Dominicana 2010 - 2014”.

Postulante:

Nombre:	Matrícula
Deivy Sánchez	2013-0855

Asesor(a):
Edda Freites, MBA.

Santo Domingo de Guzmán, D. N.
Abril, 2015

Resumen

El propósito de la presente investigación consistió en la identificación de aquellos elementos que han incidido en los fraudes cibernéticos del Sistema Bancario Dominicano ya que la delincuencia es un mal global y nuestro sistema financiero no está exentó de dichas amenazas donde varias empresas y usuarios de los servicios electrónicos se han visto afectados a través de la internet, en el uso de sus tarjetas de créditos, telefonía residencial o móvil perdiendo cuantiosas sumas monetarias. La metodología empleada en este proceso de investigación fue de naturaleza descriptiva haciendo uso del método deductivo. Se abordaron las técnicas documentales, descriptivas y de campo. Por tal razón se analizaron los datos suministrados por la Superintendencia de Bancos, el Departamento de Investigaciones de Crímenes de Alta Tecnología (DICAT), y entrevistas realizadas a expertos en la materia, los cuáles arrojaron evidencias de los tipos de fraudes más comunes utilizados en nuestro país para el periodo analizado 2010-2014 permitiéndonos identificar que el margen de delitos y las amenazas de los fraudes electrónicos se han incrementado de manera creciente en los últimos años ya que un gran porcentaje de los clientes de las instituciones bancarias han sido afectados por el ciberdelito, siendo el phishing sin lugar a dudas una de las estrategias más utilizadas por los ciberdelincuentes seguida por la clonación de tarjetas, transferencia de dinero y la usurpación de la identidad personal. Esto es debido a la falta de educación de los usuarios ante la seguridad de información, la vulnerabilidad de los sistemas electrónicos y las medidas de seguridad contra estas amenazas cibernéticas.

TABLA DE CONTENIDO

DEDICATORIAS.....vi

AGRADECIMIENTOS vii

INTRODUCCIÓN.....1

MARCO TEÓRICO.....3

CAPITULO I- EVOLUCIÓN DE LA BANCA DOMINICANA E INCIDENCIA DE LOS FRAUDES ELECTRÓNICOS. 6

1.1. Antecedentes y Origenes de la Banca 6

1.2. Evolución del Sistema Bancario Dominicano. 9

1.3. Implementación de los Servicios Electrónicos Bancarios en RD. 14

1.4. Historia de las tarjetas de crédito en la República Dominicana.....15

1.5. Concepto de Ciberespacio 15

1.6. Concepto de Extranet e Intranet.....16

1.7. La Banca Electrónica en República Dominicana.....18

1.8. La brecha digital en República Dominicana 20

1.9. Delitos Electrónicos en República Dominicana 21

1.10. Clonación de tarjetas y "phishing" en República Dominicana. 23

CAPITULO II- MARCO LEGAL 28

2.1. Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología 28

2.2. Intención Legislativa.....29

2.3. Fuentes de la Ley.....31

2.4. Entidades encargadas del cumplimiento de la ley 53-07 33

2.5. Proyectos Pendientes 35

2.6. Ley 153-98 General de Telecomunicaciones.....37

2.7. Clasificación de los Servicios 38

2.8. Órgano Regulador 38

2.9. Empresas Participantes 39

2.10. Sanciones, Penalidades e Infracciones 39

2.11. Ley 310-14 que regula envió de correos electrónicos comerciales no solicitados SPAM 46

CAPITULO III- ANÁLISIS DEL CRECIMIENTO DE LOS FRAUDES ELECTRÓNICOS EN REPÚBLICA DOMINICANA 2010 – 2014. 48

3.1. Principales Tipos de Fraudes Electrónicos en República Dominicana. .. 48

3.2. El ciberdelito a través de las redes sociales en República Dominicana. .. 53

3.3. Total de casos relacionados con Redes Sociales. 56

3.4. Población con Acceso a Internet en República Dominicana 58

3.5. Casos Resueltos de Phishing por Entidades Bancarias en R.D. 63

3.6. Análisis de las denuncias, fraudes, sometimientos y casos resueltos por el DICAT. 64

CAPITULO IV- MEDIDAS DE PREVENCIÓN MEDIANTE LOS FRAUDES CIBERNÉTICOS EN REPÚBLICA DOMINICANA. 66

4.1. Identificación del Ciberdelincuente 66

4.2. Mitigación de Riesgos para Fraudes Electrónicos 70

4.3. Medidas de Prevención para minimizar los riesgos en la red del usuario 71

CONCLUSIONES 74

RECOMENDACIONES 76

BIBLIOGRAFIA 79

ANEXOS 81

LISTA DE TABLAS

Tabla No.1 ..... **52**

Tabla No.2 ..... **57**

Tabla No.3 ..... **64**

LISTA DE FIGURAS

Figura No. 1 ..... **24**

Figura No.2 ..... **49**

Figura No.3 ..... **51**

Figura No.4 ..... **53**

Figura No.5 ..... **58**

Figura No.6 ..... **59**

Figura No.7 ..... **59**

Figura No.8 ..... **60**

Figura No.9 ..... **61**

Figura No.10 ..... **62**

Figura No.11 ..... **65**

Figura No.12 ..... **68**

Figura No.13 ..... **69**

DEDICATORIAS

A Dios:

Padre Celestial porque una vez más pude comprobar, cómo en los momentos más difíciles me diste las fuerzas y firmeza para alcanzar lo que me había propuesto, hoy quiero honrarte con el resultado de este trabajo.

A mis padres:

Sarah de Sánchez y Manuel Sánchez, por la entrega continua al desempeñar sus roles como padres ejemplares, por creer en mí, por el apoyo incondicional en tiempo y fuera de tiempo, por el amor, la dirección y el cuidado que en esta vida me han dado haciendo de mi con esto, un hijo tres veces dichoso.

Mis hermanas:

Swany y Sabrina, no puedo pasar por alto el agradecer a Dios por la fraternidad que en esta vida comparto junto a ustedes y expresarles que este es nuestro logro, siempre han estado ahí a la disposición de mis necesidades reconociendo que en tiempos gratos y difíciles he podido apreciar el apoyo incondicional por su parte.

Mi Esposa:

Marlen Merejo, eres una persona ejemplar a seguir con una personalidad muy particular la cual te hace ser única y especial, gracias por siempre tener esa palabra de optimismo y esperanza para alcanzar los sueños que nos proponemos, por exhortar a perseverar aún parezca imposible continuar.

AGRADECIMIENTOS

En primer lugar agradezco a Dios, por su tangible apoyo desde el comienzo de esta meta la cual ha sido el resultado de su divina voluntad.

A mi familia, de manera muy especial, a mi esposa Marlen Merejo, por todo su apoyo incondicional a pesar de las largas horas tomadas para la dedicación de la maestría, a mis padres Manuel Sanchez y Sarah Henríquez, mis hermanas Sabrina y Swany Sánchez, por estar ahí para mí cuando los necesité. Hoy puedo decir que este logro no es solamente mío sino también de ustedes.

A mi asesora de tesis, la Licda. Edda Freites, quiero expresar mi gratitud por su dedicación, su ardua labor, y su continúo seguimiento en mi trabajo de investigación.

A mis compañeros de Maestría, por el apoyo brindado durante este tiempo de capacitación profesional.

INTRODUCCIÓN

En la actualidad las entidades financieras están expuestas a las amenazas cibernéticas alrededor del mundo. Cada vez la tecnología nos acerca a la obtención de los productos y servicios financieros a través de los medios electrónicos a nivel global. Los usuarios desde la red virtual o cualquier medio electrónico se encuentran vulnerables, si no cuentan con la seguridad adecuada de su información personal, cualquier hacker puede apropiarse de dicha información para fines de fraudes.

En República Dominicana, uno de los fraudes más comunes es el Phishing, consiste en enviar información en camuflaje a los usuarios, con una imagen e identidad fantasma donde solicitan las informaciones del usuario para copiar y acceder a los datos confidenciales de las víctimas a través del ciberespacio. El 12 de Febrero de 2014, el Banco Central emitió un comunicado a través de diferentes medios indicando lo siguiente: ‘’En los últimos 6 años, la República Dominicana ha sido víctima de estos fraudes electrónicos sumando pérdidas cuantiosas de hasta RD$ 120MM´´. Cabe destacar que además del Phishing, existen otros tipos de fraudes electrónicos como la clonación magnética de las tarjetas de crédito, y delitos a través de la telefonía residencial y móvil.

Previo a la realización de este trabajo de investigación se consultaron varias fuentes inclinadas al tema en cuestión, las cuales trataron aspectos como el ciberterrorismo, fraudes de tarjetas de créditos y delitos electrónicos pero de una manera generalizada mientras que la presente investigación se enfoca en identificar los fraudes electrónicos más comunes del sistema financiero basados en estadísticas actualizadas ofrecidas por los órganos reguladores y supervisores de nuestro país dándonos a conocer cuáles son las estrategias

más frecuentes por los delincuentes para efectuar dichos actos delictivos para así determinar las posibles contingencias.

Por las razones expuestas procedemos a identificar las causas que inciden en el incremento de dichos fraudes que afectan a los usuarios cibernéticos, a la vez buscar las alternativas de defensa y prácticas ante esta amenaza electrónica que afronta el Sistema Bancario Dominicano.

El análisis del presente estudio de investigación será estructurado de la siguiente manera: Marco Teórico, Capítulo I- Evolución de la Banca Dominicana e incidencia de los fraudes electrónicos, Capitulo II- Marco Legal, Capitulo III- Análisis del crecimiento de los fraudes electrónicos en República Dominicana para el periodo 2010 – 2014, Capitulo IV- Medidas de Prevención mediante los fraudes cibernéticos en República Dominicana y para finalizar nuestras conclusiones y recomendaciones de lugar.

MARCO TEÓRICO

La Banca Electrónica es la misma a la cual tenemos el acceso a través de la internet, esto no se limita por ser entidades financieras físicas o que se encuentren a distancia para responder a las opciones de servicios de clientes internos o externos de la empresa ya que el internet o la telefonía permiten el mecanismo perfecto de comunicación y transacción en los negocios.

El fraude y el robo a bancos es una realidad que siempre ha existido, incluso antes de Internet. Décadas atrás, bastaba que alguien llamara por teléfono y engañara a las personas para obtener la información requerida y lograr sus delitos. Hoy en día, con el phishing en Internet, sucede similar, porque se presenta la imagen del portal muy similar al Banco, las personas entran en confianza con una identidad falsa para sustraer los datos. La diferencia con el fraude bancario que se daba hace unos años y el que existe hoy es que, gracias a la tecnología y al Internet, es posible ser atacado desde cualquier parte del mundo sin importar la distancia. El término 'phishing', del inglés 'fishing' (pescar), surgió a mediados de los años 90 asociado al método utilizado por los atacantes para sustraer las contraseñas de acceso a Internet a los usuarios del proveedor America On Line (AOL). Microsoft lo define como un tipo de robo de identidad en línea, a través del correo electrónico y páginas de Internet fraudulentas diseñadas para robar información personal, como números de tarjetas de crédito, contraseñas y datos de cuentas. Una vez que el atacante, también denominado phisher, conseguía la cuenta de la víctima, podía suplantar al usuario legítimo en el servicio y llevar a cabo cualquier acción fraudulenta como el envío de spam o ataques indiscriminados.[1]

Transcurridos diez años desde esos primeros ataques, y en pleno apogeo del phishing, podemos comprobar que el método original y primitivo se mantiene.

[1] articulo informativo. (2011) [en línea] 'phishing' y troyanos bancarios: evolución del fraude por internet, disponible en: http://poblado.mforos.com/1695798/3132581-virus-y-temas-informaticos/?pag=4

El principal cambio no tiene que ver con la técnica, que básicamente sigue aprovechándose del factor humano como eslabón más débil. Actualmente son los clientes de entidades financieras el blanco de los ataques, los criminales han encontrado en esta estafa una forma sencilla y directa de lucrarse. Además se han profesionalizado, son grupos organizados formados por varios integrantes que captan intermediarios, conocidos como "mulas", para blanquear el dinero transferido y dificultar su seguimiento. Es importante destacar que el Ciberdelito crece en América Latina y el Caribe con amenazas a cada momento más sofisticadas, esto da lugar a extremas consecuencias gravosas para las economías regionales y altos costos millonarios que desfavorecen a las entidades financieras afectadas. Según Latin American Network Information Center (LACNIC) a través de la investigación: "Panorama del Ciberdelito en Latinoamérica" se estima en menos de una década, pérdidas alrededor de 93 mil millones de dólares en Pishing. El Registro de Direcciones de Internet para América Latina y el Caribe lanzó la primera encuesta sobre Ciberdelito en la región para conocer las debilidades en el uso de las tecnologías regionales y la falta de concientización sobre los posibles fraudes a los que pueden ser víctimas los usuarios de Internet, si protegen sus dispositivos con contraseñas y si han sido contactados por personas extrañas a través de las redes sociales, ya que hoy en día es muy fácil obtener información de usuarios desprevenidos en Facebook, Twitter, Linkedin, Orkut, MySpace, Instagram, entre otros. Se señala que el robo a los bancos de la región a través de internet supera los 50 millones de dólares anuales.[2]

Según Prandini y Maggiore (2013) alertaron bajo el amparo del resultado de estas investigaciones la considerable y creciente magnitud del cibercrimen en regiones determinadas y estimaron en unos 196 millones de dólares anuales el monto de los fraudes en el comercio electrónico en América Latina. Brasil lidera el ranking en América Latina de los países con mayores ciber amenazas (códigos maliciosos, spam, phishing, bots, network attacks). Seguido en orden

[2]Boletín Informativo Lacnic News (2014). [en línea] Encuesta e Impacto del ciberdelito en América Latina y el Caribe. Disponible en: http://prensa.lacnic.net/news/edition/febrero2013_es

de amenazas cibernéticas, México, Argentina, Chile, Colombia, Uruguay, Venezuela, Perú, República Dominicana y Panamá.[3] Según la publicación Fraudes Cibernéticos Bancarios de Diario Libre en febrero de 2014 especifica que en los últimos 6 años, la República Dominicana ha recibido ataques masivos "phishing" los cuales han desviado más de RD$120 millones de pesos de los sistemas financieros bancarios de 11 entidades bancarias con fraudes reportados, los clientes de dos fueron los más perjudicados. Sólo una compañía financiera fue víctima de 168 casos que involucraron $14 millones de pesos, $74 miles de dólares y miles de euro, La otra empresa fue afectada con 139 casos, con fraudes de $8 millones de pesos. Los principales autores de estos robos cibernéticos son los malware y los troyanos, pues son los programas responsables del delito. De ellos, uno de los últimos más utilizados y renombrados es "Zeus", un troyano que se instala en los computadores, roba información del usuario para propósitos delictivos. Siendo este el más conocido, su amenaza crece cada día, porque su uso no requiere gran conocimiento.[4] Según la publicación de Apresan dos y persiguen otro por clonar tarjetas de Listín Diario en Junio de 2008 nos habla de cómo la policía capturo dos empleados de la empresa visanet quienes estaban en complicidad a un líder delictivo y prófugo con quien se dedicaron a la extracción de datos de las bandas magnéticas de las tarjetas clonadas. A su vez, la policía informo que el líder de esta banda era responsable de estafar alrededor de RD$ 40 millones de pesos a varias entidades financieras del país mediante la clonación y la fabricación de tarjetas de crédito falsas. Esta es una muestra de lo cuan riesgoso es el sistema electrónico bancario en nuestro país y el resto del mundo, por tal razón, esto no quiere decir no debemos utilizar la tecnología como medio de transacciones financieras sino más por el contrario, hacer uso, pero tomando en cuenta todos los medios de seguridad que como usuarios debemos tomar en cuenta.

[3] proyecto amparo (2013). [en línea] ciberdelito en américa latina y el caribe. disponible en: http://www.proyectoamparo.net/

[4] diario libre (2014) en línea] ataques pishing desviaron rd$120 millones en bancos. disponible en: http://www.diariolibre.com/destacada/2014/02/12/i478961_ataques-phishing-desviaron-rd120-millones-bancos.html

CAPITULO I- EVOLUCIÓN DE LA BANCA DOMINICANA E INCIDENCIA DE LOS FRAUDES ELECTRÓNICOS.

En el siguiente capítulo estaremos presentando los antecedentes de la Banca al igual que su origen desde su primera aparición, con el propósito de reconocer cual fue la necesidad que motivo al hombre a la creación de tal perfil jurídico constitutivo para los servicios de negocios en productos de valores financieros, a la vez conoceremos su aparición y evolución en la Republica Dominicana e identificando así su expansión en un mercado de emergentes competencias a través de los años donde la tecnología ha impulsado a la Banca tradicional a convertirse en una Banca Digital a través de medios electrónicos sin olvidarnos de mencionar los posibles riesgos delictivos que asechan a los usuarios así como a las grandes instituciones financieras.

1.1. Antecedentes y Orígenes de la Banca.[5]

El origen de la Banca tiene sus orígenes desde la antigüedad, con la particularidad de que una persona es propietaria de algún valor y requiere que alguien más le garantice el salvaguardarlo, o facilite su comercialización negociable.

En el periodo 3000 a 2500 años a.C., en los palacios reales y templos de la antigua Mesopotamia, se otorgaban territorios con el objetivo de proteger los granos y diferentes productos. Se utilizaban recibos para saldar el compromiso, enajenar o transferir dichos valores, tanto a los depositantes originales como a terceras personas. Con el paso del tiempo, se crearon regulaciones que fueron incluidas en el famoso Código de Hammurabi el cual contiene normas referentes a negociaciones y conceptos relacionados a la Banca como garantía, deudas, dinero, intereses, etc.

[5] La Banca en República Dominicana Ayer y Hoy. Superintendencia de Bancos (2011). Disponible en: http://www.sb.gob.do/pdf/La-Banca-en-Republica-Dominicana-Ayer-y-Hoy.pdf

Por un lado, en Egipto, unos 1800 años a.C., Se llevó a cabo las órdenes autorizadas por los propietarios para el retiro de lotes de granos a favor de sus depositantes, que fueron utilizadas como medio de pago a deudas, impuestos, y otras mercancías, en sí, esta autorización era considerada como una especie de dinero.

Antes de la aparición del dinero metálico, se utilizaba como medio de intercambio los valores negociables. Las primeras monedas que se conocen, se acuñaron en Lidia, Asia Menor (actual Turquía) en el siglo VIII a.C., y eran un compuesto natural de oro y plata, siendo el oro, el metal más valioso seguido de la plata para todos los pueblos, patrón que trasladó de forma espontánea a la fabricación del dinero, y luego como respaldo del mismo.

La aparición del dinero ocurre no sólo para facilitar el intercambio de bienes y servicios comerciales, sino más bien por la necesidad de los poderes públicos de organizarse, y lograr conseguir estabilidad económica financiera.

Aproximadamente 700 años a.C., en Grecia, se efectuaban operaciones utilizando su patrimonio, respaldado por las dadivas de los fieles, y los cuantiosos depósitos que los mismos confiaban a su administración.

La costumbre de la acuñación de monedas se incorporó como una actividad dispersa hasta la época del Imperio Romano (31 a.C – 476 d.C), El emperador Augusto, aseguró el poder de su gobierno realizando reformas significativas, estableciendo con esto la unidad política y cultural. De esta manera el Imperio Romano coloco en circulación su denarium (moneda acuñada de plata).

Alrededor de 500 Reyes y 1400 ciudadanos griegos acuñaron sus propias monedas, de esta manera fue estableciéndose la tradición de plasmar sobre la moneda un sello con el emblema local.

En Europa, durante la época de las Cruzadas (1095 - 1291) reaparecieron los bancos a raíz de la necesidad de transferir importantes cantidades de recursos para financiar el pago de provisiones, equipos, alianzas y rescates,

requería métodos seguros, confiables y rápidos, lo que impulsó el crecimiento de la banca.

Durante la Edad Media, Italia se constituyó en la primera región de Europa en renovar y relanzar el comercio. Surgiendo de esta manera la etimología de la palabra “banco”, cuyo nombre procede del mueble utilizado, un simple banco o mesa, durante el Renacimiento por los banqueros florentinos y los llamados lombardos, quienes hacían sus transacciones sobre un banco o una mesa cubierta por un mantel verde, posicionándose al servicio en las plazas de las ciudades, en ocasiones frente a la catedral.

Por otro lado, los términos de “bancarrota” o “quebrado” provienen de la manifestación pública que hacían los banqueros de ese entonces cuando fracasaban en sus negocios, lo cual les impedían asumir sus obligaciones, dicha acción pública era muy gráfica y evidente, para que todos se enteraran: rompían con un hacha la banca en que habían estado efectuando sus operaciones.

Las ciudades italianas son las precursoras de la banca moderna. En el año 1171 se instaló el primer banco privado de depósito más antiguo específicamente en Venecia. En lo adelante para el año 1270 se emitieron disposiciones a su vez promulgando la primera Ley sobre la ejecución de la banca.

Entre el siglo XII y XIV los bancos conocieron un florecimiento importante, muchos comerciantes acudían a los bancos para tratar sus negocios con terceros, y éstos obtenían una comisión. Para esta época se desarrollaron una gran diversidad de operaciones y servicios bancarios, de igual forma la contabilidad fue perfeccionada conjunto al sistema de partida doble. Esto permitió a los banqueros tener el impulso de expansión en sus servicios, además del financiamiento de negocios y particulares, además hacían préstamos con garantía.

El siglo XV, y el Descubrimiento de América, se produjeron una serie de desafíos para el progresivo pero aún débil sistema bancario y financiero europeo.

El Banco de Inglaterra, denominado The Governor and Company of the Bank of England, fue fundado en 1694 basado en una nueva ley financiera. Entre sus principales aportaciones tenemos la emisión de billetes como sustituto del dinero metálico. De esta manera nace un nuevo tipo de dinero, el fiduciario, a diferencia de las monedas de la época, el billete poseía un valor representativo. Además se le deben importantes contribuciones, como: el cheque moderno, las notas de caja, las letras de cambio, los pagarés y las obligaciones.

Se establece la primera centralización bancaria en 1844, donde quedan prohibido el asentamiento de nuevos bancos emisores, esto provoco que el Banco de Inglaterra siendo el más significativo, de ser banco privado se convirtiese en el primer Banco Central y de Emisión.

Hoy día el sistema financiero exhibe una impresionante variedad de productos y servicios en todo el mundo, donde en el tiempo presente se nos está otorgando la disponibilidad de una modalidad de servicios bancarios a la que llamamos servicios electrónicos y digitales.

1.2. Evolución del Sistema Bancario Dominicano.

La evolución del Sistema Financiero Dominicano nos permite comprender las diferentes etapas coyunturales que ha atravesado nuestro país reflejando diversos niveles de desarrollo económico, bancario e institucional. A continuación, presentamos una breve reseña cronológica del sistema bancario de nuestro país según lo muestra la Superintendencia de Bancos en su libro: La Banca en República Dominicana Ayer y Hoy (2011).

En el año 1869 se crea el Banco Nacional de Santo Domingo, la primera institución bancaria que se estableció en la República Dominicana, se encargó

de emitir billetes nacionales con el propósito de convertirlos en monedas de oro o plata acuñadas. Dicho banco inicio sus operaciones desde el 01 enero de enero de 1870, cerrando sus puertas a los cuatro meses del mismo año a causa de la decadente situación económica y poca educación bancaria de la época.

En el año 1872, en el gobierno de Báez se adjudicó una concesión para instituir un banco, con la facultad de emitir, pero al ocurrir el derrocamiento a este gobierno, no se efectuó dicha operación.

En el año 1874, surge la misma intención de crear un banco con la capacidad de emitir billetes durante el gobierno de Ignacio María González a través de la firma American Dominican Company, dicho requerimiento fue anulado posteriormente y no fue concretizada ninguna acción.

En el año 1875, la Cámara Legislativa permitió que el estado dominicano se constituyera como accionista con la designación del Banco Nacional de Santo Domingo, por lo tanto esta fue la primera iniciativa para la incursión del Estado en el área bancaria. Cabe destacar que este derecho se materializa en años posteriores.

En el año 1881, se crea el Banco de Santo Domingo, el cual tuvo una permanencia muy efímera. Posteriormente, ocho años más tarde, se establece el nuevo Banco Nacional de Santo Domingo, el cual operó hasta el año 1914.

En el año 1909, se promulga la primera Ley sobre Instituciones Bancarias, Ley No. 4911, durante el periodo del presidente Ramón Cáceres donde se disponen regulaciones orientadas para Bancos Hipotecarios, Emisores y Refaccionarios.

En el año 1912, The Royal Bank of Canada se instituye en República Dominicana el primer banco extranjero. Cinco años más tarde, The National City

Bank abre sus puertas al público, a través de su subsidiaria, la International Bank Corporation y asi mismo en el año 1918, El Banco Territorial y Agrícola de San Juan de Puerto Rico es autorizado a operar, posteriormente dos años después The Bank of Nova Scotia, inicia sus operaciones.

En el año 1928, se crea La Compañía Bancaria Nacional, el primer banco de inversión local, siendo la primera entidad de capital nacional que recibió depósitos del público y realizó operaciones crediticias, dichas operaciones fueron detenidas por el régimen de Trujillo.

En el año 1941, se funda el Banco de Reservas de la República Dominicana mediante la Ley 586 la cual dio inicio a un sistema nacional de crédito, ya que esta institución ha sido agente financiero y fiscal del gobierno dominicano, y a la vez permite operaciones bancarias con el sector privado.

En el año 1945, mediante la Ley No.908, se creó el Banco Agrícola de la República Dominicana, constituida en la segunda institución bancaria que promueve el desarrollo económico, para el fomento público de la agricultura e industria.

En el año 1947, el estado dominicano decide crear el Banco Central de la Republica Dominicana mediante la Ley 1529, el país goza de una buena imagen financiera por el saldo de la deuda externa y se pone a la par con la moneda norteamericana a la vez cabe destacar que después de la guerra esta parte de la época impulsaba hacia la recuperación económica, el crecimiento y el desarrollo institucional.

El Banco Central inició sus labores el 23 de octubre de este año y se establece como órgano regulador del sistema monetario nacional y el crédito bancario y público, con la capacidad para de emisión de billetes y monedas en Republica Dominicana y custodiar su circulación. Cabe destacar que estas

legislaciones dan origen a nuestra consagración soberana monetaria y financiera. En este mismo año nace la Superintendencia de Bancos de la República Dominicana, en virtud de la referida Ley General de Bancos No. 1530, en función del establecimiento de disposiciones de supervisión y regulación de todo el Sistema Financiero Dominicano.

En el año 1949, es fundado con capital nacional el Banco de Crédito y Ahorros. Posteriormente, el año 1962, se establecen en el país The First National City Bank, y The Chase Manhattan Bank, dos empresas del sector privado de capital extranjero.

En el año 1963, se crea el Instituto de Desarrollo y Crédito Cooperativo (IDECOOP) a través de la Ley No.31, para el año 1964, pone en ejecución sus operaciones El Banco Popular Dominicano y reconociendo que fue fundado el año anterior.

En el año 1966, se establece la Ley No.292 sobre Sociedades Financieras de Empresas la cual insta el Desarrollo Económico, más adelante conocidas como Bancos de Desarrollo.

En el año 1971, se crean los Bancos Hipotecarios bajo la Ley No.171 con el objetivo de impulsar la industria de la construcción.

En el año 1977, el Banco Condal Dominicano empezó a operar bajo la denominación de Banco de Santander Dominicano. Por otro lado en 1980, se fundó el Banco Nacional de Crédito (Bancrédito), para un año más tarde iniciar sus operaciones.

En el año 1984, inicio sus operaciones el Banco Dominicano del Progreso. Dos años después comenzaron a operar los siguientes bancos El Banco Gerencial & Fiduciario, el Banco Domínico – Hispano, el Banco Cibao, el Banco

Mercantil, el Banco BHD, el Banco Antillano, Banco Español, el Banco Dominicano del Caribe, el Banco Intercontinental (Baninter) y el Banco Panamericano.

En el año 1992, la Junta Monetaria aprobó que las instituciones financieras puedan ofrecer “servicios múltiples bancarios”, asumiendo a la vez otros requerimientos, como, unirse a un banco comercial, un banco de desarrollo, un banco hipotecario y dos o más entidades financieras, de igual naturaleza que las anteriores, incluyendo las asociaciones de ahorros y préstamos. Dos años tarde, también se autoriza que estos bancos autorizados puedan hacer negociaciones en dólares y cualquier moneda extranjera.

En el año 1999, El Banco Santa Cruz es autorizado a ejercer sus funciones como banco de servicios múltiples e igualmente el Banco BDI en el año 2001.

En el año 2002, se establece la nueva Ley Monetaria y Financiera, No. 183–02, la cual otorga al Banco Central y a la Superintendencia de Bancos el marco jurídico de actuación que tiene en la actualidad, el 25 de octubre del mismo año, el Banco VIMENCA inicia sus operaciones como banco de servicios múltiples.

En el año 2003, el Banco Nacional de Crédito recibe la autorización para modificar su nombre, denominándose Banco Múltiple León. En el año 2004, se autoriza al Banco Múltiple León la fusión por absorción del Banco Profesional.

En el año 2005, se crea la Ley No. 288-05: que regula la Protección al Titular de la Información, con el propósito de promover la confidencialidad y el uso adecuado de la información para disminuir el riesgo en el funcionamiento del sistema bancario dominicano.

En el año 2006, comienza a operar El Banco Múltiple López de Haro, posteriormente en 2009, son fundados: Banco Múltiple de las Américas, Bancamérica, y el Banco Múltiple Promérica.

En el año 2010, comienza sus operaciones el Banco Multiple Banesco, en el 2012 el Banco Múltiple LAFISE y en el año 2013, el Banco BellBank.

Por otro lado, en el año 2014, La Junta Monetaria, aprobó en su más reciente sesión la fusión del Banco BHD y el Banco Léon, con lo que queda legalmente instituido a partir de hoy 1 de julio, el Banco BHD León.

1.3. Implementación de los Servicios Electrónicos Bancarios en RD.

Es importante reconocer la importante razón por la cual el sistema financiero dominicano se ha visto en la obligación de expandir sus servicios a través de tecnología, siendo la respuesta, la competitividad. El ritmo de la vida y la rapidez del desarrollo de la tecnología no tan solo empujan a las empresas sino que provoca a la población al uso de dichas herramientas y servicios, convirtiéndose en una necesidad específica donde se obtienen resultados totalmente favorables para las empresas como la satisfacción de aquello que requiere el cliente. Por esto, vemos como en las últimas décadas el dinero plástico o tarjetas de créditos es uno de los medios electrónicos que no tan solo satisface el fácil uso de los clientes sino que también ha arrojado grandes beneficios en ganancias para las empresas, de igual forma la diversidad de productos y servicios electrónicos hoy día continúan evolucionando conforme el liderazgo del mercado demanda como las necesidades de los clientes.

1.4. Historia de las tarjetas de crédito en la República Dominicana[6]

Para 1960 el país incursiono en la emisión de tarjetas de crédito a través de la compañía Créditos Comerciales S.A.; a la vez ingresó la American Express, para uso internacional. Más adelante, la Compañía de Crédito e Inversiones ofrece al público dominicano la tarjeta "Servicios e Inversiones".

Los inversionistas locales notaron la gran aceptación del producto y esto impulso a que otras empresas emergieran con la emisión de este plástico comercial, sin dejar de mencionar la cantidad de bancos comerciales que se unieron a la misma acción. De esta manera el Banco Condal Dominicano introduce al pueblo dominicano la tarjeta de Condalcard, la cual más adelante se denominó Bankcard, convirtiéndose en la primera tarjeta de crédito Dominicana. Posteriormente, ya para 1991 otras empresas bancarias extendieron sus mercados al unirse con entidades emisoras de tarjetas de crédito con carácter internacional donde a raíz de esto surge como pionero el Banco Popular Dominicano ofreciendo las con las tarjetas Visa y Mastercard.

1.5. Concepto de Ciberespacio

El Diccionario de la Real Academia Española (RAE) lo define: “Ámbito artificial creado por medios informáticos”.[7] Ampliando esta definición, podríamos decir que nos referimos a un espacio virtual creado por la interconexión de equipos informáticos con el objetivo de interactuar en una Red. El mayor ámbito del ciberespacio es Internet, intranet y extranet. De igual forma podemos describir el ciberespacio como el medio en dónde el usuario y la comunidad pueden interrelacionarse, transferir información, hacer transacciones u otro tipo

[6] El Origen y Evolución Histórica de las Tarjetas de Crédito (2007). Disponible en: http://edrismilgrullon.blogspot.com/2007/01/sabia-usted-acerca-de.html
[7] Diccionario en CD/Room de la Real Academia Española (RAE) Microsoft 2009

de actividad, que adquiere lo que llamaremos: vida (realidad virtual) siendo todo esto el resultado del accionar de un soporte técnico y una gran infraestructura de comunicaciones. Lo interesante del ciberespacio es que no se limita por un espacio territorial definido como lo es un estado o nación, otra característica es que no está marcada por una tradición ni religión específica. Es por esto que podríamos considerar el ciberespacio como la máxima expresión de la sociedad globalizada y manifiesta el auge de la comunicación de la información. En el ciberespacio los límites físicos: tiempo y espacio son redefinidos, generando una transformación radical en la cultura de sus usuarios.[8] En palabras más sencillas podemos decir, que el ciberespacio es un término no físico que sirve para representar hechos informáticos producidos a través de redes interconectadas conocidas comúnmente como Internet.

1.6. Concepto de Extranet e Intranet

Según Rijo (2013) explica que el extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella usualmente utilizando Internet. La extranet suele tener un acceso semiprivado. Para acceder a la extranet de una empresa no necesariamente el usuario ha de ser trabajador de la empresa, pero si tener un vínculo con la entidad. Es por ello, que una extranet requiere o necesita un grado de seguridad mayor, para evitar el acceso no autorizado de intrusos. Otra característica de la extranet es que se puede utilizar como una Intranet de colaboración con otras compañías. El principal aspecto en común entre Internet, Intranet y Extranet es que los tres utilizan la misma tecnología. Las diferencias de la extranet con Internet y la Intranet se dan

[8] Georgetown University. Disponible en: www.cs.georgetown.edu/

principalmente en el tipo de información y en el acceso a ella. Además, una extranet requiere mayor seguridad e implica acceso en tiempo real a los datos, ya que estos tienen que estar actualizados. La extranet se dirige a usuarios tanto de la empresa como externos, pero la información que se encuentra en la extranet es restringida, en teoría solo tienen acceso a esta red aquellos que tengan permiso. En cambio a la intranet solo acceden los empleados y las áreas internas de la empresa y permite el intercambio de información entre los trabajadores. Por último, a la Internet puede dirigirse cualquier usuario y tiene distintos usos, como recabar información de los productos, contactar con cualquier persona de la empresa, etc. En la siguiente tabla se muestran de manera resumida las diferencias entre las aplicaciones en una empresa:[9] Esto nos lleva a comprender que aquellas infraestructuras críticas del estado dominicano o empresas privadas que posean un sistema extranet son las que se encuentran en mayor riesgo de convertirse en objetivos ciberterroristas, debido a que sus sistemas informáticos conectados a Internet, brindan la oportunidad a que de manera remota ingresen individuos no autorizaos al sistema y produzcan daños al mismo.

El fraude provee una definición que sin importar su ambigüedad, el significado será no favorable. Esto se debe que a que su aplicación es literalmente una acción delictiva. Es la manera de engañar a alguien para obtener a cambio un beneficio particular, (lo cual está penado por la ley), por eso es importante reconocer que todo acto delictivo sin importar el medio debe estar expuesto a disposición de la ley, es por esto que la modalidad puede ser a través de la internet, clonación de tarjeta de crédito o llamada telefónica, el delincuente debe asumir las consecuencias de la justicia.

Por ejemplo, tratándose de clonación de tarjeta de crédito, así como en el lavado de activos, estos casos no concluyen cuando los afectados reciben su crédito o el seguro resuelve la perdida monetaria sino que las consecuencias van alimentándose de la brecha de la delincuencia en cada intento o impacto a

[9] Ibid.

sus víctimas por lo tanto la sociedad va en decadencia moral raíz de la mala influencia que estas acciones delictivas puedan motivar. En el momento que gremios criminales y personas deciden vivir un ritmo de vida delictivo, dichos actos provocan inevitablemente consecuencias:

Sociales: La sociedad y los mercados se estacan por la afección delictiva que producen estos actos así como los de lavados de activos, inspirados en una negociación fantasma donde solo el delincuente sale beneficiado, esto provoca limitación de inversión y negocio por parte de los inversionistas y a la vez por parte de los usuarios de tarjetas de crédito.

Económicas: El dinero que proviene de actividades ilícitas puede crear distorsión en la economía de un determinado país, afectando de igual forma los comercios porque se genera incertidumbre de si confiar o no en realizar compras en los establecimientos afectados o de mayor ocurrencia en los fraudes.

En estos dos impactos, la consecuencia que se repite es la falta de valores éticos, es importante reconocer que la decisión de poner los valores en alto es decisión de cada persona aunque por lo general según estadísticas, las personas que más hacen práctica de la diversidad de delitos, son personas de escasos recursos, poca o ninguna preparación académica, entre otros aspectos. Recordamos que los desfalcos en la Enron y en Arthur Andersen fueron efectuados por sus altos ejecutivos.

1.7. La Banca Electrónica en República Dominicana[10]

Definimos como banca electrónica cualquier transacción que un usuario aplique electrónica y remotamente utilizando los medios de las TICs (Tecnologías de Información y Comunicaciones) o Internet, celulares, etc. A la vez es denominada e-banking, conjunta a su estructura de servicios tradiciones

[10]Hoy.com.do (2007). Respondiéndote que es la Banca Electrónica. Disponible en: http://hoy.com.do/respondiendoteque-es-la-banca-electronica

que incluye cajeros automáticos, lugares específicos de ventas, callcenter, páginas web que requieren el acceso a través de cualquiera de los siguientes medios: computadoras personales, Laptop, televisión interactiva, smartphones o móviles comunes, etc.

La ventaja de los servicios de home banking e internet banking es que tienen la facultad de acercar al cliente a los productos de la empresa sin importar el lugar, ya que puede disponer de los mismos desde su: hogar, lugar de trabajo, de viaje, etc. Esta modalidad de servicios permite a la banca está disponible a sus clientes en cualquier lugar y cualquier hora, aunque ciertos aspectos y temores del sistema tradicional aun no son superados como: el mayor ahorro posible del papel, el temor de ser engañado por o ser víctima de ciberdelito. La Republica Dominicana cuenta con un marco jurídico y regulatorio que ampara dichas operaciones como la Ley 126-02 sobre Comercio electrónico y firmas digitales.

El representante para América Central y el Caribe de la empresa fabricante de antivirus Mcafee, Luis Ortiz, quien ofreció una conferencia en el país sobre las amenazas en el ámbito de la informática que pueden afectar a una empresa, destacó que "El sistema bancario de República Dominicana no es fácil de atacar con virus informáticos que provoquen daños como robo de información o molestias en el servicio que ofrece a los clientes, ya que cuenta una buena protección en este sentido y se encuentra entre uno de los países más seguro en materia de informática a nivel de Latinoamérica."[11]

[11] Audiencia Electronica (2010). Citado por Hiddekel Morrison en su artículo titulado: "Afirman que la banca electrónica de la Republica Dominicana es segura" disponible en: http://www.audienciaelectronica.net/2010/11/19/afirman-que-la-banca-electronica-de-la-republica-dominicana-es-segura/

1.8. La brecha digital en República Dominicana

Según Rijo (2013) hace referencias cuando el Ingeniero en electrónica y telecomunicaciones Hiddekel Morrison en su libro titulado: "La República Dominicana en la Sociedad de la Información" define la brecha digital como: "la separación entre los que están conectados a la revolución digital de las llamadas tecnologías de información y comunicación (TICs) que agrupa la Internet, computadoras, etc. De los que no tienen acceso a los beneficios de esas tecnologías".[12] Concretamente apunta que "La medición de la brecha digital neta en Internet, señala que un 10.3% de la población tiene acceso a Internet, por lo que la brecha digital neta según este cálculo es de casi un 90%. Estos resultados se obtuvieron mediante cálculos realizados en base a valores obtenidos de las estadísticas del Instituto Dominicano de las Telecomunicaciones (INDOTEL), del Banco Interamericano de Desarrollo (BID), la Unión Internacional de Telecomunicaciones (UIT), y del más reciente censo nacional de población y vivienda realizado por la Oficina Nacional de Estadística (ONE).[13]

El nivel tan alto de brecha digital a nivel nacional parece guardar una íntima relación con el alto precio del servicio de Internet que se paga en el país, lo que provoca un muro de contención que impide el acceso de las masas al mismo. Al respecto, el programa "Nuria en el 9, presentó un interesante trabajo en torno al tema, en donde Hiddekel Morrison, señaló que el servicio de Internet en República Dominicana, es el más caro del mundo debido a que a las empresas que brindan este servicio se les cobran impuestos que ascienden a un 28%, el índice más caro de impuestos en América Latina.[14] "En muchos países el

[12] morrison, hiddekel. (2009), libro titulado: "la república dominicana en la sociedad de la información"
[13] Ibid
[14] Audiencia Electrónica (2010). Reportaje televisivo transmitido en el programa "Nuria en el 9" disponible en el sitio Web: http://www.audienciaelectronica.net/2010/04/28/reportaje-de-nuria-internet-en-republica-dominicana/

Internet, no llega a 20 dólares y sin embargo, en nuestro país, cuesta 66 dólares, el más caro del mundo", enfatizó Morrison[15].

Se hace mención de estos datos, debido a que paradójicamente este nivel tan alto de la brecha digital en el país, constituye un ente de retraso para el desarrollo humano de la población, sin embargo, esto también significa que la mayoría de la población no está expuesta a ser víctimas de los ciberdelincuentes en la Web.

1.9. Delitos Electrónicos en República Dominicana

A principios de los años 80, llegan a Republica Dominicana los primeros informes del desarrollo de fraudes informáticos en el extranjero de igual forma inicia una nueva conciencia del uso de las computadoras como nueva forma de delitos cibernéticos donde se establecen disposiciones en la normativa penal nacional. Cabe destacar, que esta seria la fórmula que se conjugaría, aunque momentáneamente toda la gama de situaciones era la elaboración y promulgación de una nueva ley que incriminara y penalizara directamente este fenómeno, esto se debe a que el derecho penal dominicano no describía exactamente el delito informático. Por esto, en virtud del principio de legalidad en materia penal que reza: "Nulla Paean Sine Lege Praevia" que traducido es: "no hay crimen sin ley previa, no hay delito sin ley", así que se mostró el primer anteproyecto de ley en República Dominicana el cual se conoce como: "De los crímenes y delitos de computadora" justo para el año 1988.[16] El mismo no fue aprobado, pero de haber ocurrido, hubiese puesto al país en dicha época, en uno de los primeros del mundo en contar con una legislación sobre el tema.[17]

[15] Ibid

[16] Medina, Pamela, (2009). Artículo titulado: "El delito informático: Realidad procesal en República Dominicana"

[17] Análisis Jurídico (2009). El Delito Informático Realidad Procesal. Disponible en: http://visionlegal-analisisjuridico.blogspot.com/2009/08/el-delito-informatico-realidad-procesal.html

Es una realidad reconocer que los sistemas informáticos se exhiben totalmente vulnerables, sin embargo cuando nos referimos a las amenazas, estas requieren de un protagonista motivado con herramientas, facultad tecnológica y la convicción voluntaria de explotar la misma. Por tal razón, vemos como el grupo hacktivista de origen desconocido Anonymous y el grupo dominicano Resistencia Popular Duartiana (RPD), en 2013 son actores dispuestos a utilizar sus medios para actuar en contraria de la infraestructura crítica del Gobierno Dominicano. Dichas acciones convierte ambos movimientos en dos amenazas a la seguridad de la información electrónica en la Republica Dominicana.

Es de gran notoriedad la delincuencia que amenaza y se desarrolla con gran expansión en todo el planeta, la misma no tan solo asecha sino que afecta nuestro país, por lo tanto esta gran diversidad que ahora se hace más extendida a través de los medios telefónicos ahora en tiempo presente adopta inesperadas novedades fraudulentas. La práctica se centra en la consultas sencillas y de datos generales que la víctima por particularidad maneja, pero lo que más se destaca y permite identificar que dichas llamadas son fraudes es el modo de consultas a preguntas personales, no existe un protocolo de protección al usuario, se solicitan datos que se asume que la empresa ya tiene, ofrecen servicios y la vez informan al cliente de haber sido ganador de un premio, el objetivo es a líneas residenciales de familias como celulares, con el objetivo de timar a sus propietarios. En los móviles un fraude muy peculiar es un mensaje de texto y para que si fuese poco puede ser a nombre de una empresa cualquiera como de servicios telefónicos, donde se le informa al cliente que ganó 150,000 pesos y un celular valorado. Luego del mismo llaman al celular y le dicen que lo estaban localizando y seguido le hablan de los premios que ganó, pero le piden sus datos, como cédula, dirección, nombre y número de otras personas en la familia que tengan celulares con dicha empresa. Luego y según

las fuentes, llaman a uno de esos familiares y le dicen que tienen a su esposo, esposa o hermano secuestrado y que deben pagar para su liberación.[18]

Según Rijo (2013), explica que en los periodos 2007 al 2011 se ha resuelto 116 casos de Hacking, 12 de acceso ilícito y sabotaje y 2 de daños y alteración de datos, para un total de 130 casos relacionados con el acceso ilegal y la protección de datos. Lo importante a resaltar aquí no es si el número de casos es elevado o bajo, sino, que una futura alianza, sea por motivaciones ideológicas o económicas entre uno de estos dos grupos (Anonymous y RPD) y los hackers o piratas informáticos responsables de cometer estos 130 casos de delitos relacionados con accesar ilegalmente a sistemas informáticos y sabotear o dañar datos, es una posibilidad que no debe descartarse ya que según el autor Mario D. Montoya, alianzas similares han acontecido en el pasado entre grupos terroristas latinoamericanos como las Fuerzas Armadas Revolucionarias de Colombia (FARC) y Sendero Luminoso con los carteles colombianos y mexicanos. Una alianza de este tipo entre 161 Resistencia Popular Duartiana o Anonymous y estos hackers que ya han burlado sistemas informáticos en 116 oportunidades, representaría una amenaza aún mayor de la que ya constituyen ambos grupos por separado. Se evidencia a través de esos datos que existe en el país el potencial humano con la capacidad para hackear e ingresar a sistemas informáticos, causar daños y alteración de datos.

1.10. Clonación de tarjetas y "phishing" en República Dominicana.[19]

Desde el 2008 a la fecha, la justicia dominicana ha detenido alrededor de 2,234 de individuos, nacionales y extranjeros, a causa de los fraudes de

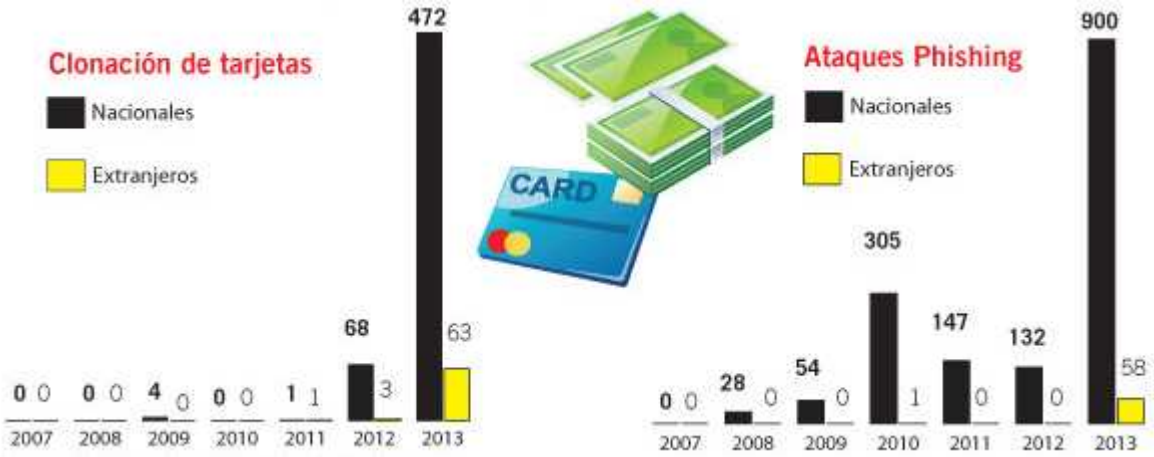
[18] Evidencias Digital (2014). Extorsiones telefónicas a la orden del día en Rep. Dom. Disponible en: http://evidenciasdigital.com/?p=890#sthash.0OvlfRMT.dpuf

[19] SFMNEWS.COM (2014). Fraudes Bancarios. Disponible en: http://www.sfmnews.com/2014/02/fraudes-bancarios-son-el-80-de-los.html

clonación de tarjetas y robo de datos e identidad a través del "phishing". Esta última modalidad mencionada, es utilizada para sustraer dinero e información de cuentas a través del correo electrónico y páginas fantasmas de Internet, los casos representados por esta acción delictiva equivalen a un 72.7 %.

Como se muestra en la Figura No. 1, sobre los casos de individuos sometidos a la justicia, hay un incremento de proceso penal ejecutado en el año 2013 significativamente en comparación a los años anteriores con respecto a los fraudes de tarjetas de crédito y phishing, así lo afirma, el titular de la Procuraduría Especializada contra Crímenes y Delitos de Alta Tecnología, John Henry Reynoso Ramírez, destaca que antes de febrero de 2013, fecha en que se creó esa dependencia, pocas personas eran condenadas por los dos tipos de delitos citados, pues en el 97% de los procesos se llegaba a una conciliación con los bancos o las víctimas, y no había una persecución enfocada en el ciberdelito.

Figura No.1
Casos sometidos a la Justicia en RD por Fraudes Bancarios
(2007 – 2013)



(Fuente: Procuraduría Especializada contra Crímenes y Delitos de Alta Tecnología, 2014).

Las razones son la siguientes: cuando se trataba de clonación de tarjetas de crédito, el usuario ordinario al verse afectado acciona con ir banco reclamar que tiene un seguro que le redime de compromiso antes dichos fraudes hacia su

persona, el mismo al tener todo resuelto, deja todo ahí y la posible persecución e investigación que se pudo haber levantado se detiene ahí. Esto se debe a que si el usuario recupera su dinero no tiene necesidad de perseguir los delincuentes o causas del delito, de igual forma a los bancos no les interesa estar en la persecución de individuos. Desde el 2007 a principios de 2013, se encontraban solamente 69 personas en prisión preventiva por clonación de tarjetas, datos que el Procurador lamenta.

Para finales del 2013, de manera general, había unos 1,850 individuos sometidos, guardado prisión preventiva en espera del proceso judicial correspondiente con el poder de condenarlos hasta 10 años de prisión mientras que 28 de ellos lograron negociar una garantía económica. Todos estos actores de crímenes y delitos tipificados de alta tecnología procesados por la Procuraduría Especializada.

Los extranjeros sometidos entre 2007 y 2013, que pertenecen a redes que se dedican al ciberdelito, cuyas actuaciones han afectado a la banca local, han sido 67 por clonación de tarjetas y 60 por "phishing". "Por lo general aquí se apresan muchos haitianos, canadienses, venezolanos y colombianos", dice el magistrado Reynoso.

También, participan delincuentes de otras nacionalidades. El 27 de octubre de 2013, se apresaron dos búlgaros en Bávaro, acusados de colocar teclados adulterados y otros aparatos en cajeros automáticos de zonas turísticas, para obtener el PIN de las tarjetas de crédito o débito de los usuarios, con el fin de clonarlas, y posteriormente realizar retiros. En total, la estafa rondaba los US$200 mil.

La Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología establece que la obtención ilícita de fondos de un usuario, se sancionará con la pena de tres a 10 años de prisión y multa de 100 a 500 veces el salario mínimo.

Respecto a la transferencia electrónica de fondos a través de códigos de acceso o de cualquier otro mecanismo similar, el castigo va desde uno a cinco años de prisión y multa de dos a 200 veces el salario mínimo.

En tanto que la estafa realizada a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones, se sancionará con la pena de tres meses a siete años de prisión y multa de 10 a 500 veces el salario mínimo. Y el robo de identidad por los mismos mecanismos conlleva penas de tres meses a siete años de prisión y multa de dos a 200 veces el salario mínimo.

Según Ferreras (2013), en su ante proyecto de investigación ‘’Prevención de Fraudes en Tarjetas de Crédito’’ en énfasis a una intermediaria financiera, durante el 2012 los comercios más afectados con el fraude de tarjetas de crédito no es que se conviertan en los únicos establecimientos que requieren de mayor protección para ellos como para los clientes, por lo tanto toda entidad comercial está en la amenaza del riesgo a través de lo que llamamos el plástico o tarjeta de crédito u otros instrumentos de uso financieros.

A continuación veamos los comercios o establecimientos más afectados durante el 2012.

Instituciones Financieras – Cajeros Automáticos: Todas las instituciones financieras fueron afectadas en este renglón, pues del total general, el 38.15% correspondió a retiros en efectivo y compras.

Estaciones de Combustible: El 17.02% corresponde a este renglón. Es en este tipo de negocios donde se hace más frecuente el copiado de banda magnética a través del Skimmer.

Llamadas a través de uso de lectura magnética de banda en teléfonos: Esta modalidad alcanzó un total de 4.84%. Corresponde a la lectura de la banda magnética a través de dispositivos móviles como el celular.

Bodegas: Esta parte se refiere principalmente a lugares donde se venden vinos. El 4.54% corresponde a estos lugares afectados con el fraude a través de

tarjetas de crédito. Aerolínea Jet Blue: La salida de American Airlines del mercado dominicano provocó que las compras de los pasajes aéreos aumentaran en muchas compañías de vuelos comerciales, Es interesante destacar que Jet Blue no reportaba casos fraudulentos en las ventas de sus boletas aéreos a través de las tarjetas de crédito, sin embargo el crimen organizado inicio su ataque. El 3.44% del total de fraudes corresponde a esta empresa.

Restaurantes de comida rápida (Fast Food): El 1.97% de los fraudes en consumos con tarjetas de crédito corresponde a estos tipos de establecimientos. Subastas: El 1.67 de los fraudes con tarjetas de crédito fue en lugares donde se realizaban subastas, ya sea del tipo normal o de compras por internet.

Afiliaciones: El 1.49 de los fraudes con tarjetas de crédito se dieron a través de afiliaciones a cualquier tipo de comercio de esta naturaleza, básicamente usando robo de identidad para recibir beneficios o comprar con ese producto. Restaurantes: Los consumos con tarjetas de crédito en restaurantes ocuparon el 1.04% del total del fraude.

Librerías: Este renglón ocupó el 1.03%. Otros negocios: Tiendas de calzados, computadoras, farmacias, tour operadores, empresas gubernamentales, entre otros, son afectados con el fraude con tarjetas de crédito. En conjunto suman un 24.80% del total de fraudes.

CAPITULO II- MARCO LEGAL

Vivimos en un mundo donde el libertinaje fraudulento y las amenazas son cada vez mayores, los reclamos y denuncias por delitos electrónicos no tan solo en República Dominicana sino también en todo en el planeta, esto provoca que los órganos de seguridad correspondientes puedan emitir leyes que comprometan al ciudadano al respeto del derecho ajeno pero de lo contrario quien no cumpla las normas y las agreda será sometido al peso de la justicia de dichas normas. Hoy día la Republica Dominicana cuenta con leyes que tienen por objetivo proteger a los usuarios de los servicios electrónicos como también de telecomunicaciones, conoceremos cuales son los fundamentos para emitir estas disposiciones como quienes son los órganos asignados para regular el cumplimiento de dichas leyes.

2.1. Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología[20]

Constantemente se pronuncian las demandas por irrespeto a la privacidad ajena, podemos citar en particular las victimas de fraude por extraer datos personales para tener acceso a sus cuentas y demás. A causa de estas acciones delictivas, los reguladores del comercio electrónico a través de la ley de firma digital y el avance futuro del crecimiento del tráfico del comercio electrónico y digital, además de la implementación de gobierno electrónico fueron los indicadores que impulsaron al estado Dominicano a desarrollar un marco regulatorio que figurara y sancionara esta naturaleza delictiva.

La ley 53-07, sobre Crímenes y delitos de Alta Tecnología, es el marco legal de mayor importancia para la regulación de las infracciones informáticas, telemáticas y cibernéticas. Es por esto que cabe destacar que

[20] Agelán Casasnovas. E. (2011) Ciberdelincuencia y Política Criminal. República Dominicana. Editora Premium S.R.L.

el Código Penal Dominicano no distingue dentro de sus tipos de disposiciones penales las acciones delictivas relacionadas con las tecnologías de información y comunicación. Esto trae como resultado la obligación requerida de tipificar dichos fraudes con el objetivo de lograr una persecución eficaz además de sanciones que condicionen dichos actos.

El órgano que insto a la elaboración de esta normativa es el Instituto Dominicano de Telecomunicaciones (INDOTEL). En su recinto se determinó la iniciativa e inmediatamente se escogieron los expertos que prepararían el contexto del anteproyecto de ley, el cual ha permitido en la actualidad que Republica Dominicana cuente con un marco legal que sancione los delitos de alta tecnología.

2.2. Intención Legislativa

El objetivo principal de cualquier regulación es corresponder a las necesidades de una sociedad. Es muy importante que el Legislador debe tomar en cuenta que para satisfacer estas necesidades o requerimientos debe crear una norma que sea parte de la historia innata, política, cultural, social y la economía nacional del país. Esta idea es recolectada en uno de los considerandos de la Ley 53-07, cuando dice: ´´…en la actual era del conocimiento, la información y los instrumentos electrónicos de canalización de la misma, se han vuelto cada vez más importantes y trascendentes en los procesos de desarrollo, competitividad y cambios estructurales registrados en las vertientes económicas, políticas, sociales, culturales y empresariales del país´´.[21]

La creación de la Ley 53-07 en nuestro país, es la respuesta a la obligación requerida de luchar contra aquellas acciones delictivas que hasta

[21] Ibid

su emisión era muy dificultosa perseguir por no estar tipificada, esto peor aún impulsaba al crecimiento de la impunidad.

Esta disposición legislativa, adecuada a las necesidades de una sociedad en específico, obliga El juzgador se ve en la obligación a realizar una interpretación no exacta o profunda de la norma. En ese sentido se pronuncia López Medina, señalando que, contrario a una interpretación apegada de forma radical el texto de ley destaca la obligación del intérprete de analizar la política pública, social y económica que a ley encarna (López Medina 2002).

Con el respaldo de la Ley 53-07, el legislador dominicano busca tutelar los derechos de personas físicas y morales que pueden ser vulnerados en la comisión de infracciones con la utilización de medios tecnológicos, al igual que la seguridad del estado.

La dignidad y la intimidad se pueden citar como derechos de los cuales pueden ser vulnerados por los medios tecnológicos, pero si seguimos nombrando otras como: la indemnidad sexual, el derecho patrimonial y la seguridad del estado, entre otros, todos tutelados por la ley constitucional dominicana.

El fundamento principal para la creación de esta ley ha dado lugar a que sea reconocido por el legislador de que en la medida en que se registran los avances tecnológicos, los instrumentos de comunicación y la tecnología se tecnifican y modernizan, de igual forman han y van evolucionando los delitos.

El contexto de la ley reconoce que su efectividad depende no solo de la acción de los reguladores y la burocracia interna, en base al importante rol desempeñan las entidades estatales y descentralizadas sino más bien la

colaboración internacional, un factor necesario para la persecución de este tipos de infracciones en base a la naturaleza de los delitos.

La constitución dominicana establece la inviolabilidad de la correspondencia y demás documentos privados, así como el secreto de la comunicación gráfica, telefónica y caligráfica. Estos derechos fueron ampliados en la actual constitución en su artículo 44, numeral 3, al abarcar documentos o mensajes privados en cualquier formato físico, digital, electrónico o de cualquier otro tipo.

2.3. Fuentes de la Ley

La Ley 53-07 consagra la intención legislativa en el sentido de establecer los derechos y deberes fundamentales de los ciudadanos en cuanto a la libertad de expresión, integridad e intimidad, así como la inviolabilidad de las comunicaciones, entre otros derechos.

También se consagra el requerimiento de regular por medio de un proceso especial para la investigación y persecución de los fraudes delictivos a través de tecnología moderna, de esta manera se diferencia de los delitos comúnmente conocidos y calificados por el Código Penal y otras leyes especiales. Esto movió al legislador tomar como fundamento principal para su creación y redacción la normativa que se destaca a continuación.

1. La derogada Constitución de la Republica Dominicana, que reconocía en su artículo 8 como finalidad principal del estado, la protección efectiva de los derechos de la persona humana y el mantenimiento de los medios que le permiten perfeccionarse progresivamente dentro de un orden de libertad y de justicia social.
2. La Declaración Universal de Derechos Humanos de 1948 y la convención Americana sobre Derechos Humanos, suscrita en San José,

Costa Rica, el 22 de noviembre de 1969, instrumentos internacionales que reconocen derechos fundamentales de los individuos.

3. El Convenio sobre Cibercriminalidad de Budapest, suscrito el 23 de noviembre del año 2001, por los estados miembro del consejo de Europa y otros países. Fue el primer convenio internacional para enfrentar el crimen cibernético. República Dominicana aun no es signataria de ese convento.

4. El Código Procesal Penal de la Republica dominicana, Ley 76-02, Maco Regulatorio de la norma procesal.

5. El proyecto de Código Penal dominicano que aún está en el congreso Nacional. A pesar de esto, se tomaron las iniciativas contenidas en esta reforma penal, contando quizás con que sería aprobado en un breve plazo, sin embargo esto no sucedió, y a la fecha Republica Dominicana aun cuenta un Código Penal que data del año 1884.

6. El Código Penal Dominicano de 1884, donde se encuentra tipificada la norma sustantiva.

7. La Ley 50-88, sobre Drogas y sustancias Controladas, y la Ley 137-03, sobre Tráfico ilícito de Migrantes y Trata de personas. La Ley 53-07 tipifica el tráfico ilícito de humanos o migrantes y la venta de drogas y sustancias controladas, utilizando como soporte sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones.[22]

8. La Ley 20-00, sobre propiedad industrial, y la Ley 65-00, sobre derecho de autor las infracciones que se tipifican en la ley 53-07, también

[22] Zaffaroni. R. (2003) Manual de derecho Penal parte General. República Dominicana. Editora Ediar. Página 372.

corresponden a tipos penales en blanco, ya que remite a ellas para imponer la sanción.[23]

9. La Ley 136-03, que instituye el Código del Menor y tutela los derechos de los menores. Marco conceptual para tipificar el atentado sexual contra un menor y la pornografía infantil.[24]

10. La Ley Número 96-04, institucional de la Policía Nacional de fecha 28 de enero de 2004. Esta constituye el marco regulatorio de la estructura policial, así como las funciones y actuaciones policiales, imprescindibles para la creación del Departamento de Investigación de Crímenes y Alta Tecnología (DICAT).[25]

11. La Ley 126-02, del 4 de septiembre del 2002, sobre Comercio Electrónico, Documentos y Firmas Digitales. Esta norma supletoria es de vital importancia para la persecución de los delitos de alta tecnología, porque es a partir de ella que se le da reconocimiento jurídico a los documentos digitales y mensajes de datos, otorgándole validez como medio de prueba.

12. La Ley General de Telecomunicaciones No. 153-98 del 04 de mayo del 1998. Esta ley plasma la política estatal en materia de telecomunicaciones, regulando los servicios ofertados por las prestadoras de servicios y la competencia entre estas.[26]

2.4. Entidades encargadas del cumplimiento de la ley 53-07

Según la Ley 53-07 en su artículo 30, influye la creación y estructuración de la Comisión Internacional contra Crímenes y Delitos de

[23] Artículo 25, de la ley 53-07 sobre crímenes y delitos de alta tecnología.
[24] Artículos 23 y 24, Ibid
[25] Artículo 36, Ibid
[26] El Artículo 4 de la ley No. 126-2 sobre comercio electrónico, documentos y firmas digitales 2002.

Alta Tecnología (CICDAT), la cual está compuesta por un representante de:[27]

a) La Procuraduría General de la República
b) El Ministerio de las Fuerzas Armadas (MIFFAA)
c) El Ministerio de Interior y Policía
d) La Policía Nacional
e) La Dirección Nacional de Control de Drogas (DNCD)
f) El Departamento Nacional de Investigaciones (DNI)
g) El Instituto Dominicano de las Telecomunicaciones (INDOTEL)
h) La Superintendencia de Bancos de la República Dominicana

La Ley 53-07 por medio de su artículo 43, funda la División de Investigaciones de Delitos Informáticos (DIDI) como dependencia del Departamento Nacional de Investigaciones (DNI). De igual forma estos tienen oficiales conectados al departamento de investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional, del Ministerio de las Fuerzas Armadas y de la Dirección Nacional de Control de Drogas.

Esta unidad trabaja los casos relacionados a:[28]

a) Crímenes contra la humanidad
b) Crímenes y delitos contra la Nación el Estado y la paz pública
c) Amenazas o ataques contra el Estado dominicano, la seguridad nacional o que involucren la figura del presidente de la República, secretarios de Estado o funcionarios electos.

[27] Artículo 30 de la Ley No. 153-98 Ley General de las Telecomunicaciones 1998

[28] Artículo 43 de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología 1998

La Ley 53-07, articulo 36, se inspira para la creación del departamento de investigación de crímenes y delitos de alta tecnología (DICAT); como entidad subordinada a la Dirección Central de Investigaciones Criminales de la Policía Nacional. Las funciones del DICAT son:[29]

a) Investigar todas las denuncias de crímenes o delitos considerados de alta tecnología.
b) Responder con capacidad investigativa a todas las amenazas y ataques a la infraestructura de tecnología critica nacional.
c) Desarrollar inteligencia en Internet.

2.5. Proyectos Pendientes

a) Convenio sobre cibercriminalidad con Consejo de Europa

Este convenio surge por la necesidad de aplicar una política penal común a nivel internacional, encaminada a proteger a la sociedad global frente a la ciberdelincuencia, adoptando la legislación adecuada y manteniendo una política de cooperación internacional. A partir de la aprobación de la promulgación de la Ley No. 53-07 sobre crímenes y delitos de alta tecnología en el año 2007 la República Dominicana fue invitada a adherirse al convenio sobre cibercriminalidad del Consejo de Europa, el cual actualmente se encuentra en el proceso de ratificación por parte del Congreso Nacional, sin embargo, aunque no se ha ratificado, fue en base a las recomendaciones hechas por el mismo que se redactó la Ley 53-07.[30]

[29] Artículo 36 de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología
[30] taiguey.org. 2009. Presidente de Indotel llama a atacar ciberdelincuencia. Disponible en: http://taiguey.org/cact-dom/prensa.php?msg=prensa_tics_dom-1923&lang=es

Al respecto, el director del Departamento de Delitos Electrónicos y Propiedad Intelectual de la Procuraduría General de la República, Licenciado Pedro Féliz comentó a la prensa nacional que la ley 53-07 fue redactada conforme a las recomendaciones establecidas en ese convenio, por lo que exhortó a los distintos sectores nacionales a que "se integren al respaldo del ingreso de República Dominicana al Convenio de Europa, porque el mismo ayudará al combate del crimen cibernético que se está propagando a escala transnacional."[31]

b) Valoración de la Naciones Unidas Contra la Droga y el Delito (UNDOC)

Según Rijo (2013) expresa que hace un considerable tiempo que ciertas instituciones internacionales tales como: la (CITEL) Comisión Interamericana de Telecomunicaciones, el (CICTE) Comité Interamericano contra el Terrorismo y la (REMJA) Reunión de Ministro, de Justicia o Procuradores Generales de las Américas están trabajando en la adopción de una estrategia hemisférica para la seguridad cibernética en la región, conforme a lo dispuesto por la Resolución AG/RES. 2004 (XXXIV-0/04) de la Asamblea General de la Organización de Estados Americanos (OEA) de fecha 8 de junio de 2004, para la Adopción de una Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética. Según estas instituciones internacionales la República Dominicana al promulgar estas leyes da el primer paso hacia el futuro establecimiento en nuestro país de una estrategia interamericana integral para combatir el terrorismo y las Amenazas a la Seguridad Cibernética.[32]

[31] Dacanet.com. 2008. "Procuraduría solicita ingreso de Rep. Dom. a convenio contra el cibercrimen" Disponible en: http://www.dacanet.com/?p=36

[32] Undoc . Valoración de la UNDOC. Disponible en: http://www.undoc.org/

Esta es la principal razón por la cual la institución internacional denominada “Naciones Unidas Contra la Droga y el Delito” (UNDOC) resaltó los avances legislativos logrados por la República Dominicana para el establecimiento de un régimen legal contra el ciberterrorismo. La organización destaca que del año 2006 a la fecha, la situación del país se transformó de no tener ninguna disposición legal nacional para combatir el terrorismo a contar con dos instrumentos legales e integrales contra ese flagelo. Indica además que el país ha ratificado 12 de los 16 instrumentos internacionales existentes contra el terrorismo, cuando en 2006 apenas había ratificado 4, el número más bajo del hemisferio americano.[33]

2.6. Ley 153-98 General de Telecomunicaciones[34]

La Ley General de Telecomunicaciones No. 153-98 tiene como objetivo fomentar el desarrollo de las telecomunicaciones, promover la competencia justa, eficaz y sostenible, defender y preservar los derechos de los consumidores, promover el servicio universal y administrar eficientemente el espectro radioeléctrico. Las disposiciones de la Ley No. 153-98 se encuentran complementadas por los Reglamentos y las Resoluciones dictadas por el INDOTEL

La Ley define las telecomunicaciones como la transmisión y recepción de señales por cualquier medio electromagnético. Por lo cual, el campo de aplicación de la ley se extiende a los servicios de teléfono, radio, televisión, cable, facsímil y transmisión digital de información.

[33] Ibid
[34] OMG (2014). Noticias y Publicaciones. Disponible en: http://www.omg.com.do/guia_de_negocios/Telecomunicaciones/

2.7. Clasificación de los Servicios

Los servicios públicos de telecomunicaciones son los actividades comerciales que se dan al público en universal, en contextos de no discriminación, a cambio de un pago. Según lo determinado en la Ley, los servicios públicos de telecomunicaciones se clasifican en:

a. Servicios portadores
b. Servicios finales o tele servicios
c. Servicios de valor agregado
d. Servicios de difusión

2.8. Órgano Regulador

El Instituto Dominicano de Telecomunicaciones “INDOTEL” es el órgano regulador de las telecomunicaciones y tiene como propósito promover las inversiones en el área, establecer las políticas y normas que rigen el sector, supervisar los proveedores de los servicios, defender a los consumidores, manejar el espectro radioeléctrico, resolver las controversias y administrar el fondo de desarrollo de las telecomunicaciones.

Uno de los objetivos primordiales del INDOTEL es garantizar la existencia de una competencia efectiva, leal y sostenible en la prestación de servicios públicos de telecomunicaciones.

2.9. Empresas Participantes

Conforme las estadísticas del Órgano Regulador, en el país operan 18 empresas telefónicas. Las 4 principales son: La Compañía Dominicana de Teléfonos, C. Por A., Orange Dominicana, S.A., Tricom, S.A., y Trilogy Dominicana, S.A.. Además, existen registradas 149 estaciones de radio bajo amplitud modulada (A.M.), 222 estaciones de radio bajo frecuencia modulada (F.M.), 69 estaciones de televisión y 117 empresas concesionarias de servicio de difusión por cable.

2.10. Sanciones, Penalidades e Infracciones[35]

A continuación, haremos mención de las acciones que se consideran Infracciones en la Ley No. 53-07, del 23 de abril del 2007, sobre Crímenes y Delitos de Alta Tecnología:

1. Divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o descifrar de cualquier modo, los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones (de manera conjunta, lo designaré como "sistema") o sus componentes (Art. 5, parte capital).

2. La clonación para la venta, distribución o cualquier otro uso, de un dispositivo de acceso a un servicio o sistema (Art. 5, Párrafo).

[35]La Ley No. 53-07, del 23 de abril del 2007, sobre Crímenes y Delitos de Alta Tecnología (la "Ley No. 53-07").

3. El acceso no autorizado a un sistema o sus componentes, utilizando o no una identidad ajena o excediendo una autorización (Art. 6, parte capital).

4. La supresión, modificación o revelación no autorizada de datos obtenidos del sistema accesado ilegalmente (Art. 6, Párrafo I).

5. La explotación no autorizada de un acceso no intencional a un sistema (Art. 6, Párrafo II).

6. Utilizar un programa, equipo, material o dispositivo para obtener acceso a un sistema o sus componentes, para ofrecer servicios a terceros sin pagar al proveedor (Art. 7, parte capital).

7. Aprovechar las actividades fraudulentas de un tercero (citadas en el numeral anterior) para recibir un beneficio para sí o un tercero (Art. 7, Párrafo).

8. Producir, usar, poseer, traficar o distribuir sin autorización, programas informativos, equipos, materiales o dispositivos destinados a la comisión de crímenes electrónicos (Art. 8).

9. Interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar un dato, señal o transmisión de datos o señales perteneciente a otra persona, por cuenta propia o a encargo de cualquier persona, sin autorización previa del tribunal competente (Art. 9).

10. Borrar, alterar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas, con fines fraudulentos (Art. 10).

11. Alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema (Art. 11).

12. Atentar contra la vida de una persona a través de medios informáticos (Art. 12).

13. Efectuar robos a través de sistemas o dispositivos electrónicos (Art. 13).

14. Obtener fondos a través de violencia o presión ejercida contra el usuario de un servicio financiero informático (Art. 14, parte capital).

15. Realizar transferencias electrónicas de fondos a través del uso ilegal de códigos de acceso (Art.14, Párrafo).

16. Estafar a cualquier persona, asistiéndose de medios electrónicos (Art. 15).

17. Efectuar chantaje a través de medios electrónicos, con el propósito de obtener fondos, la firma o entrega de algún documento, un código de acceso, etc. (Art. 16).

18. El robo de identidad (Art. 17).

19. Falsificar, desencriptar, decodificar o descifrar, divulgar o traficar documentos, firmas, certificados, etc. (Art. 18).

20. Utilizar equipos electrónicos para invadir la privacidad de una persona, sin autorización de tribunal competente (Art. 19).

21. Efectuar comercialización no autorizada o ilegal de bienes y servicios a través de Internet o asistiéndose de un sistema. Esto incluye el tráfico de personas, drogas o sustancias controladas (Art. 20).

22. La difamación e injuria cometida a través de medios electrónicos (Art. 21 y 22).

23. Ejercer un atentado sexual contra un menor de edad, incapacitado o enajenado mental, haciendo uso de un sistema (Art. 23).

24. Producir, difundir, vender o comercializar pornografía infantil, pero también poseerla (Art. 24).

25. Cometer infracciones contra los derechos de propiedad intelectual e industrial, a través de un sistema (Art. 25).

Por otra parte, según el Artículo 26 sobre Delitos de Telecomunicaciones, los que cometan uno o varios de los siguientes hechos, incurren en penas de prisión de tres meses a diez años y multa desde cinco a doscientas veces el salario mínimo[36]:

a) Llamada de Retorno de Tipo Fraudulento: La generación de tráfico internacional en sentido inverso al normal, con fines comerciales, mediante mecanismos y sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones. Este hecho incluye, pero no se limita, a cualquier tipo de retorno de llamada a través de código,

[36] La Ley No. 53-07, del 23 de abril del 2007, sobre Crímenes y Delitos de Alta Tecnología (la "Ley No. 53-07").

asistencia de operador, vía un sistema informático, dependiendo del mecanismo o sistema mediante el cual se transmita la señal de disparo;

b) Fraude de Proveedores de Servicio de Información Líneas Tipo 1-976: La autogeneración de llamadas por parte del proveedor de servicio de información de líneas tipo 1-976, con el propósito de que la prestadora que le ofrece el servicio de telefonía tenga que pagarle las comisiones de estas llamadas será considerada un fraude, constituyendo un agravante, cuando los autores del delito se valgan de medios publicitarios o de cualquier otro tipo y precios reducidos, o de números telefónicos ordinarios para su re direccionamiento hacia líneas de servicio de información, u otros medios similares;

c) Re direccionamiento de Llamadas de Larga Distancia: El fraude en el desvío o redirección del tráfico de larga distancia de la ruta utilizada por parte de las compañías portadoras de señal de larga distancia, para evadir el costo real de la misma, a través de conmutadores colocados en lugares distintos al de origen de la llamada;

d) Robo de Línea: El uso de una línea existente, alámbrica o inalámbrica, de un cliente legítimo, para establecer cualquier tipo de llamadas mediante una conexión clandestina, física o de otra índole, en cualquier punto de la red;

e) Desvío de Tráfico: El desvío de tráfico a través de rutas no autorizadas con el objeto de evitar o disminuir los pagos que corresponden a la naturaleza del tráfico desviado, ya sea un desvío de servicios, desvío de facilidades contratadas, o cualquier otro tipo de desvío ilícito;

f) Manipulación Ilícita de Equipos de Telecomunicaciones: El hecho de manipular ilícitamente, de cualquier forma, las centrales telefónicas u otros componentes de las redes de telecomunicaciones, con el objetivo de hacer uso de los servicios sin incurrir en los cargos correspondientes;

g) Intervención de Centrales Privadas: La utilización de medios para penetrar centrales privadas a través de los puertos de mantenimiento o especiales del contestador automático o cualquier otro medio, que conlleven la realización de llamadas no autorizadas en perjuicio del propietario de la central intervenida.

Según la Ley 53-07 en cláusula: Responsabilidad Civil y Penal de las Personas Morales. Además de las sanciones que se indican más adelante, las personas morales son responsables civilmente de las infracciones cometidas por sus órganos o representantes. La responsabilidad penal por los hechos e infracciones contenidas en esta ley, se extiende a quienes ordenen o dispongan de su realización y a los representantes legales de las personas morales que conociendo de la ilicitud del hecho y teniendo la potestad para impedirlo, lo permitan, tomen parte en él, lo faciliten o lo encubran. La responsabilidad penal de las personas morales no excluye la de cualquiera persona física, autor o cómplice de los mismos hechos. Cuando las personas morales sean utilizadas como medios o cubierta para la comisión de un crimen o un delito, o se incurra a través de ella en una omisión punible, las mismas se sancionarán con una, varias o todas de las penas siguientes[37]:

a) Una multa igual o hasta el doble de la contemplada para la persona física para el hecho ilícito contemplado en la presente ley.

[37] Artículo 60 de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología 2007

b) La disolución, cuando se trate de un crimen o un delito sancionado en cuanto a las personas físicas se refiere con una pena privativa de libertad superior a cinco años.

c) La prohibición, a título definitivo o por un período no mayor de cinco años, de ejercer directa o indirectamente una o varias actividades profesionales o sociales.

d) La sujeción a la vigilancia judicial por un período no mayor de cinco años.

e) La clausura definitiva o por un período no mayor de cinco años, de uno o varios de los establecimientos de la empresa, que han servido para cometer los hechos incriminados.

f) La exclusión de participar en los concursos públicos, a título definitivo o por un período no mayor de cinco años.

g) La prohibición, a perpetuidad o por un período no mayor de cinco años, de participar en actividades destinadas a la captación de valores provenientes del ahorro público.

h) La confiscación de la cosa que ha servido o estaba destinada a cometer la infracción, o de la cosa que es su producto.

i) La publicación por carteles de la sentencia pronunciada o la difusión de ésta, sea por la prensa escrita o por otro medio de comunicación.

2.11. Ley 310-14 que regula envió de correos electrónicos comerciales no solicitados SPAM[38]

La Ley 310-14 fue sometida en el 2011 y aprobada el 08 de agosto de 2013 por el Presidente Danilo Medina, dicha ley regula y normaliza los correos electrónicos no deseados (Spam). A continuación presentaremos los aspectos más importantes de la Ley:

Requisitos de la ley

Entre los requisitos exigidos por la ley para el envío de comunicaciones comerciales, se establece que la comunicación comercial electrónica remitida desde una dirección de correo electrónico debe permitir a quien recibe el mensaje poder notificar su voluntad de no volver a recibir comunicaciones comerciales de la fuente advertida u otro mecanismo virtual.

Otro requisito indispensable es la existencia de un nombre o razón social, con las informaciones generales de domicilio completo y dirección de correo electrónico del emisor de la comunicación.

Asimismo, es obligatorio “que los mecanismos automáticos de respuesta se encuentren operando y en activa capacidad de recibir cualquier informe por parte de los receptores de no recibir comunicaciones comerciales como mínimo dentro de los dos días hábiles después de haber emitido el mensaje”.

[38] La Ley 310-14, del 08 de agosto del 2014, Santo Domingo. Que regula el envío de correos electrónicos comerciales no solicitados (SPAM).

La Ley establece que cuando la comunicación sea emitida desde un dispositivo móvil debe cumplir con el nombre o razón social y número origen del iniciador de la comunicación, entre otros requerimientos.

Algunos artículos de la ley:

- Toda emisión de correo electrónico debe tener en el Subject o espacio de asunto de mensaje la palabra publicidad según el artículo 4.
- Cuando la comunicación contenga información no apta para menores de 18 años de edad, debe se establece que debe contener lo siguiente: publicidad para adultos. (Artículo 4, Párrafo I).
- Toda información contraria o engañosa en el campo de asunto con el cuerpo del mensaje. (artículo 9, acápite 2).
- No se deben emitir comunicaciones a través de correos electrónicos sin haber sido solicitadas por el destinatario. (capitulo III, articulo 7)

Entre las sanciones, La Ley reconoce como fraude informático de 6 meses a 5 años y multa de 200 salarios mínimos a aquellos que envíen comunicaciones comerciales que se consideren ilegales, también está penalizado falsificar el campo asunto así como registrar y recolectar de forma fraudulenta usando información falsa la identidad del receptor (phishing).

CAPITULO III- ANÁLISIS DEL CRECIMIENTO DE LOS FRAUDES ELECTRÓNICOS EN REPÚBLICA DOMINICANA 2010 – 2014.

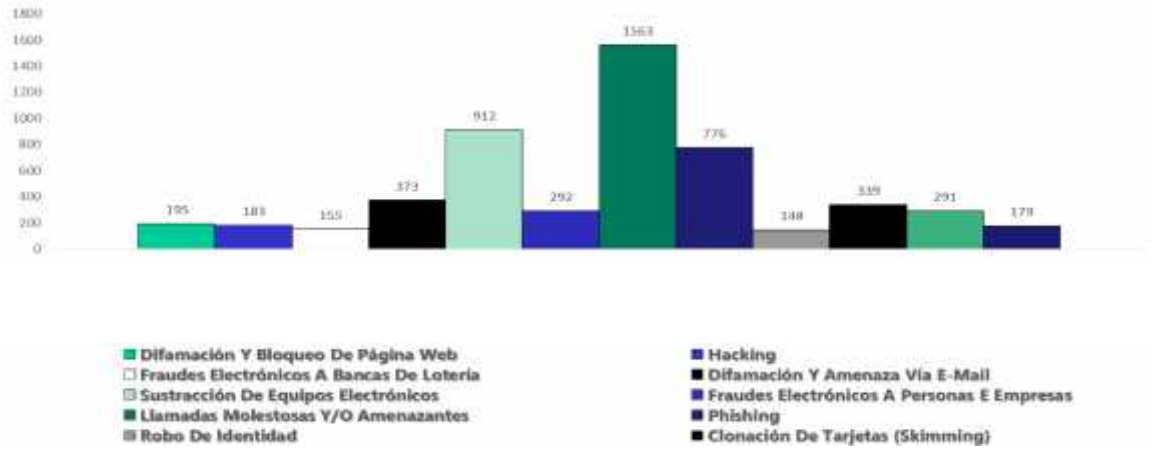
Los ciberdelincuentes cada día son más notorios por sus acciones delictivas y de igual forma la diversidad de medios y estilos que utilizan para tales actividades que van en aumento, las amenazas por igual son más propensas a su ejecución sobre sus víctimas, no tan solo en la Republica Dominicana sino que es una afección mundial. Por esto el presente capitulo muestra datos estadísticos reales facilitados por el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), Policía Nacional y La Superintendencia de Bancos de la República Dominicana, que permitirán evaluar la evolución y el impacto de los diversos medios utilizados por los delincuentes que afectan el Sistema Electrónico de la Banca Dominicana en la actualidad.

3.1. Principales Tipos de Fraudes Electrónicos en República Dominicana.

Según el Ing. Carlos Leonardo, Sub-coordinador de Sección Fraudes Electrónicos del DICAT quien indica los delitos más comunes en la República Dominicana para el período del 2007 al 2014, como se observa en la Figura No. 2, el delito más predominante es el de las llamadas molestosa y/o amenazantes con un total de 1,563 casos identificados, seguido por la sustracción de equipos electrónicos con un total de 912 casos, mientras que 776 casos corresponden al phishing, 373 casos identificados por clonación de tarjetas de crédito por medio del skimmer, 292 casos de fraudes electrónicos a personas y empresas, entre otros.

Figura No.2

Cantidad de delitos electrónicos más comunes en la República Dominicana (2007 – 2014)



(Fuente: Ing. Carlos Leonardo, Sub-coordinador Sección Fraudes Electrónicos, Analista Forense IT, Departamento de Investigación de Crímenes y Delitos de Alta Tecnología DICAT, P.N., 2014).

A continuación conoceremos un listado de todos los tipos de delitos electrónicos investigados e identificados en República Dominicana por el DICAT:[39]

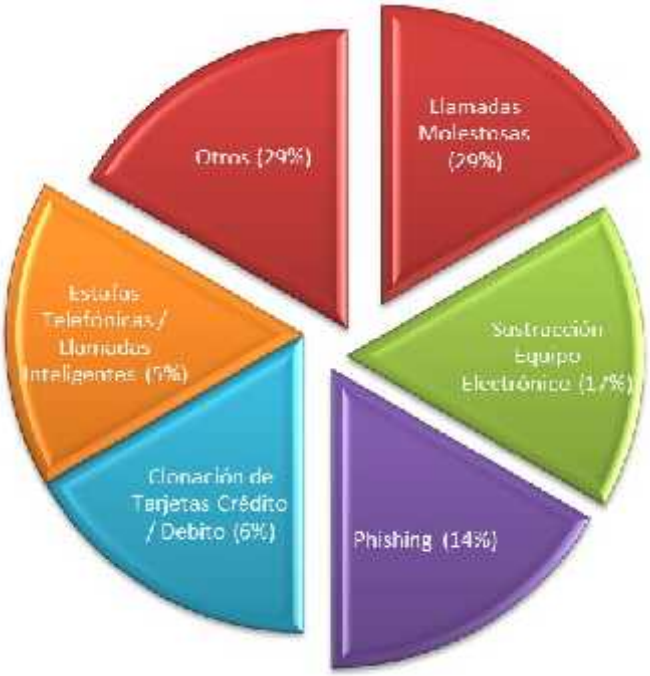
- difamación y bloqueo de página web
- hacking
- fraudes electrónicos a bancas de lotería
- difamación y amenaza vía e-mail
- clonación de cajas de cables modem
- sustracción de equipos electrónicos
- fraudes electrónicos a personas e empresas
- terminación de llamadas ilegal
- llamadas molestosas y/o amenazantes
- robo de e-mail

[39] Ing. Carlos L. Leonardo G., (2015). Sub-coordinador Sección Fraudes Electrónicos, Analista Forense IT, Departamento de Investigación de Crímenes y Delitos de Alta Tecnología DICAT, P.N.

- phishing
- robo de identidad
- acceso ilícito y sabotaje
- clonación cd, dvd de audio y películas
- pornografía infantil
- piratería de software
- activaciones fraudulentas de celulares
- clonación de tarjetas (skimming)
- sustracción de software
- daños y alteración de datos
- estafa vía telefónica
- falsificación de documentos
- publicación ilícita de película
- violación de derecho de autor
- interceptación telefónica

Podemos observar en la Figura No.3, el porcentaje de delitos más comunes en nuestro país reportados por el DICAT, destacándose que un 29% corresponde a llamadas molestosa, seguido de un 17% por sustracción de equipos electrónicos, mientras que el 14% por phishing, 6% clonación de tarjetas de crédito y débito, un 5% estafas telefónicas y el 29% restante corresponden a otros casos reportados.

Figura No.3
Porcentaje de delitos electrónicos más frecuentes en la Republica Dominicana (2007 – 2014)



(Fuente: Ing. Carlos Leonardo, Sub-coordinador Sección Fraudes Electrónicos, Analista Forense IT, Departamento de Investigación de Crímenes y Delitos de Alta Tecnología DICAT, P.N., 2014)

Según la Superintendencia de Bancos de la República Dominicana en la entrevista realizada a través de la Oficina de Acceso a la Información nos ofrece la estadística anual de cantidad de reclamaciones por transacciones fraudulentas para el periodo desde 2011 al 2014.[40]

[40] Norma Molina. Encargado Oficina de Acceso a la Información. Superintendencia de Bancos de la República Dominicana. Entrevista-Oficina de Acceso a la Información. Diciembre 2014.

Tabla No.1
Cantidad de reclamaciones por transacciones fraudulentas
en las entidades financieras dominicanas.
(2011 – 2014)

Año	Cantidad de reclamaciones
2011	3,021
2012	3,041
2013	3,315
2014*	2,467

*Incluye hasta septiembre.
Fuente: Informaciones remitidas por las EIF

De las 2,467 reclamaciones presentadas hasta septiembre de 2014, se ha dado respuesta a 2,127 casos (cabe aclarar que de las pendientes por dar respuestas se evidencian casos que aún no han terminado su plazo de conclusión).

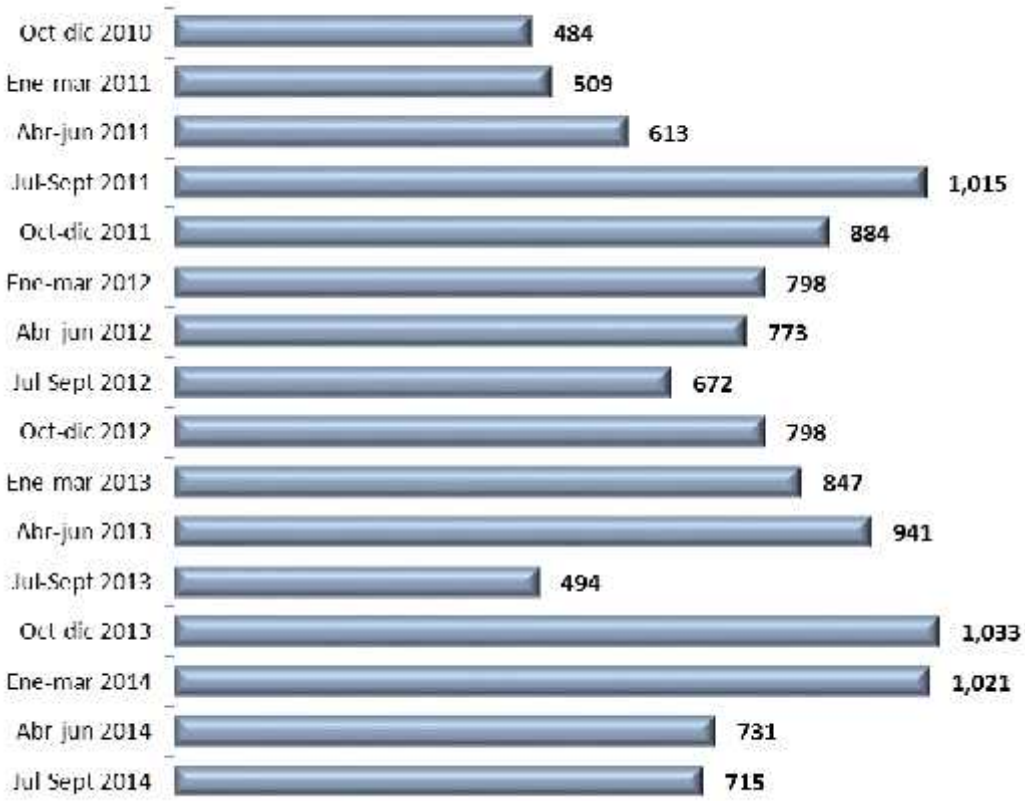
A continuación vamos a observar las reclamaciones de transacciones fraudulentas de manera trimestral de las entidades de intermediación financiera de la República Dominicana para los trimestres Octubre 2010 - Septiembre 2014.[41]

Según se muestra en la Figura No. 4, el trimestre que presentó mayor incidencia fraudulenta de los periodos analizados es Octubre – Diciembre 2013, con 1033 reclamaciones usuarios de las entidades financieras. Asimismo, se observa una leve disminución en los trimestres posteriores de acuerdo a las informaciones obtenidas por la Superintendencia de Bancos.

[41] Ibid

Figura No.4

Cantidades de transacciones fraudulentas de las entidades de intermediación financiera de la República Dominicana.
(Trimestres Octubre 2010- Septiembre 2014)



Fuente: Informaciones remitidas por las EIF

3.2. El ciberdelito a través de las redes sociales en República Dominicana.

El phishing es sin lugar a dudas un gran negocio para los ciberdelincuentes. Desarrollan correos electrónicos, enlaces y páginas web que poseen una identidad usurpada y parecen confiables y así los usuarios puedan compartir sus datos personales los cuales servirán para lograr el fraude. De acuerdo a una investigación llevada a cabo por Kaspersky Lab, el 22% de los fraudes en la Red se realiza en Facebook, de igual forma los

productos anti-phishing de Kaspersky Lab han identificado más del 35% de las páginas de phishing que se hacen pasar por las más conocidas redes sociales. A la vez han descubierto más de 600 millones de intentos por parte de sus usuarios de acceso a páginas de phishing, cada día hay más de 200,000 casos en los que los usuarios de Kaspersky Lab hacen intento de clic en enlaces que dirigen a páginas web de Facebook falsas. Quizás mirando este acto delictivo desde fuera podríamos decir que el ciberdelincuente que ganar accediendo a la cuenta de Facebook de una persona de un usuario, pero las redes sociales son el medio de acercamiento a propósitos muy importantes. Esto se debe a que los usuarios al no confiar en correos de personas o entidades desconocidas, el delincuente adopta la imagen de un conocido para provocar la confianza en medio del fraude, por ejemplo, directamente desde un banco. Otra de las razones de por porque Facebook es uno de los medios preferidos, se debe a que pueden pedir rescate de un usuario, o para vender la cuenta a terceros; esto sirve para enviar mensajes de spam a los amigos de la cuenta hackeada o a usuarios fuera del círculo de amigos de la red social. Ha quedado demostrado que enviar spam desde cuentas reales tiende a tener mayor resultado para los fraudes en vez de crear cuentas fantasmas. [42]

Hoy día la tranquilidad de guardar nuestro dinero en el banco, confianza aún mayor con el uso del dinero plástico, se desvanece con los crímenes de alta tecnología, ya que la delincuencia cibernética nos pone “a un clic del peligro”, haciéndonos propensos al fraude electrónico y otros delitos que protagonizan piratas cibernéticos, aquellos a quienes podríamos llamar depredadores que invaden y abusan de la libertad de la red. Estos se involucran en operaciones delictivas, al igual de aquellos que modifican códigos de móviles para fines de compra y ventas en negocios ilícitos.

[42] Blog.kaspersky.es, (2014). Para los adictos a las redes sociales: Facebook es el portal principal de phishing. Disponible en: http://blog.kaspersky.es/1-de-cada-5-fraudes-de-phishing-afecta-a-facebook/3694/

República Dominicana posee alta incidencia el ataque a clientes de instituciones financieras, con un 80% de los casos. El “phishing” (pesca), el robo de identidad en línea, estrategia que convierte a muchos usuarios en víctimas con la sustracción de dinero e información de cuentas a través del correo electrónico y falsas páginas de Internet diseñadas para extraer números de tarjetas de crédito, datos personales, clave de acceso e información de cuentas. Individualmente o constituidos en bandas, los hackers incurren en actos maliciosos financieros los cuales conocen el manejo de dicho sistema. Por esto es que en los fraudes con tarjetas de crédito los delincuentes arremeten contra las bases de datos de las instituciones financieras, tomando los números de las tarjetas para luego cópialos en una banda magnética con un instrumento denominado “Skimmer”. Algunos pertenecen a mafias internacionales, como la descubierta en 2013 por autoridades de Estados Unidos, la cual fue acusada de fraude bancario, dentro de este grupo se encontraban siete dominicanos. Estos asaltaron una procesadora de tarjetas de créditos, una entidad dentro del círculo del sector financiero la cual estaba encargada de procesar tarjetas de crédito. Falsificaron y aumentaron el límite tope de tarjetas de débito, en tan solo 10 horas robaron US$47 millones en 27 países a través de muletos, individuos que sustraen el dinero de cajeros y lo transportan como mulas. A inicios de 2014, la Dirección Central de Investigaciones Criminales desmanteló dos laboratorios clandestinos en la capital, en los sectores 27 de Febrero y Espaillat, propuestos a clonar tarjetas de crédito y débito para engañar bancos, comercios y usuarios. Se le conquistaron 697 plásticos listos para usarse o en proceso y aparatos electrónicos para clonar las bandas magnéticas y numerar.[43]

[43] hoy.com.do. (2014). A un “clic del peligro” Con clonación de tarjetas de crédito y otros ciberdelitos. Disponible en: http://hoy.com.do/a-un-clic-del-peligro-con-clonacion-de-tarjetas-de-credito-y-otros-ciberdelitos/

3.3. Total de casos relacionados con Redes Sociales.

Es muy importante reconocer que el usuario es el medio más vulnerable para realizar los fraudes electrónicos, por eso presentamos el cuadro siguiente, como los casos denunciados y que están relacionados a las redes sociales. Las redes sociales no tan solo son el canal más efectivo e instantáneo para acercamos a los demás sin importar la distancia o estatus social, esto ha provocado que las instituciones financieras aprovechen este medio para fines de servicios y negocios. Mientras más variable es el modelo comercial a través de las redes sociales más serán las alternativas para los ciberdelicuentes amenazar y atacar.

Según la Tabla No.2, el Ing. Carlos Leonardo, Sub-coordinador Sección Fraudes electrónicos del DICAT nos indica la cantidad de delitos a través del Phishing en las principales redes sociales como Facebook, hi5, Tweeter, Instagram y Ask.fm comprendiendo el periodo 2007 – 2014 donde nos muestra que la red social que posee mayor cantidad de delitos es Facebook, indicando que el 77% de los casos corresponden a difamación, seguido por 11% como robo de identidad, 10% por hacking, el 1% de acoso y finalmente 1% en chantaje.

Tabla No. 2

Impacto de delitos a través del phishing en las principales Redes Sociales.
(2007 – 2014)

DELITOS	DIFAMACION						ROBO DE IDENTIDAD					ACOSO				HACKING				CHANTAJE				TOTAL GENERAL
	facebook	HI5	Twitter	Instegram	Ask.fm	TOTAL	facebook	HI5	Twitter	Instegram	TOTAL	facebook	HI5	Twitter	TOTAL	facebook	HI5	Twitter	TOTAL	facebook	HI5	Twitter	TOTAL	
2007	0	6	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6
2008	2	28	0	0	0	30	0	3	0	0	3	0	0	0	0	3	0	0	3	0	0	0	0	36
2009	13	15	0	0	0	28	1	3	0	0	4	0	0	0	0	2	1	0	3	0	0	0	0	35
2010	46	4	1	0	0	51	2	0	0	0	2	1	0	0	1	2	0	0	2	0	0	0	0	56
2011	35	0	1	0	0	36	0	0	0	0	0	0	0	0	0	7	0	0	7	0	0	0	0	43
2012	33	0	1	0	0	34	2	0	0	0	2	0	0	0	0	5	0	0	5	0	0	0	0	41
2013	24	0	7	2	0	33	16	0	0	0	16	0	0	0	0	5	0	0	5	1	0	0	1	55
2014	21	0	2	2	1	26	5	0	0	1	6	0	0	0	0	0	0	0	0	0	0	0	0	32
TOTAL	174	53	12	4	1	244	26	6	0	1	33	1	0	0	1	24	1	0	25	1	0	0	1	304

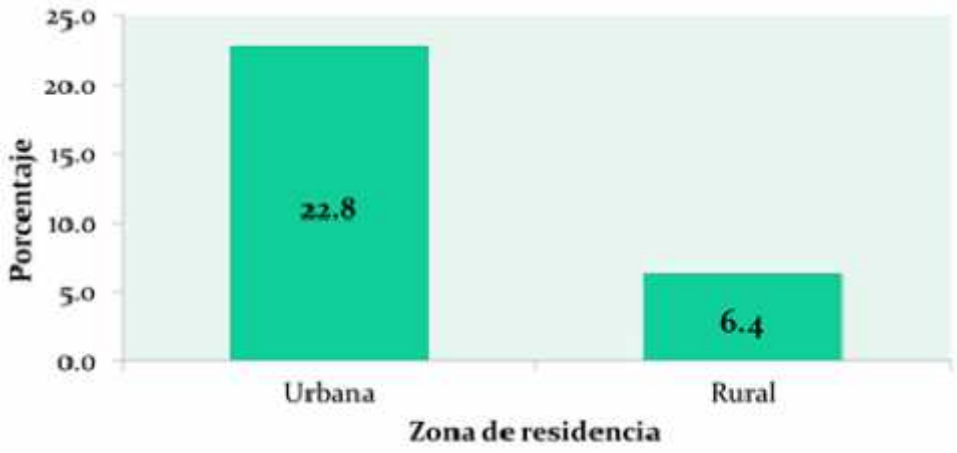
(Fuente: Ing. Carlos Leonardo, Sub-coordinador Sección Fraudes Electrónicos, Analista Forense IT, Departamento de Investigación de Crímenes y Delitos de Alta Tecnología DICAT, P.N., 2014)

3.4. Población con Acceso a Internet en República Dominicana

Según la encuesta por la Oficina Nacional de Estadística 2013, en las Figuras No. 5 y No. 6, informa que en República Dominicana la zona de residencia urbana comprende el 22.8% de hogares que tiene acceso a internet mientras que la zona rural está compuesta por un 6.4%., asimismo podemos decir que el 92.9% de la zona urbana del país a partir de la edad de los 12 años posee celular al igual que el 88.9% de la zona rural. Esto es una muestra de cómo la tecnología se ha convertido en más que un lujo, una necesidad desde temprana edad y conocimientos de los usuarios y la clave para comunicarnos es el internet, pero con la vulnerabilidad de que en el uso de la herramienta podamos ser víctimas de los ciberdelincuentes.

Figura No.5

Porcentaje de hogares con acceso a servicio de Internet, según zona de residencia, ENHOGAR-2013



Fuente: Oficina Nacional de Estadística. ENHOGAR-2013

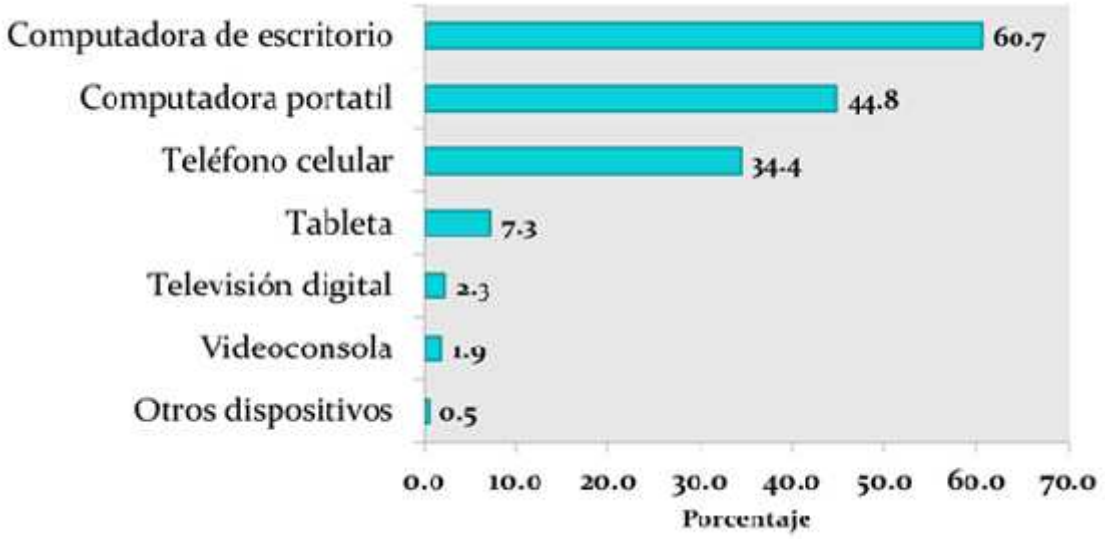
Figura No.6

Porcentaje de personas de 12 años y más que usan teléfono celular, según zona de residencia, ENHOGAR-2013

Fuente: Oficina Nacional de Estadística. ENHOGAR-2013

Figura No.7

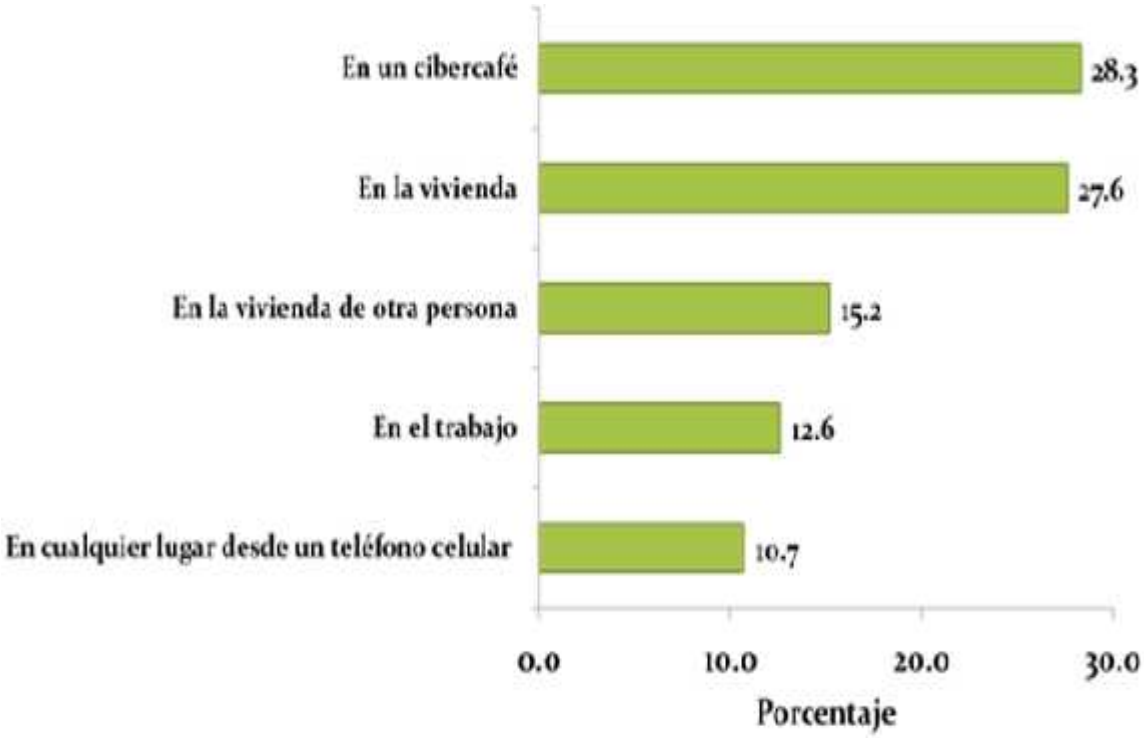
Porcentaje de hogares con acceso a servicio de Internet, según dispositivos para acceder a la Internet, ENHOGAR- 2013.



Fuente: Oficina Nacional de Estadística. ENHOGAR-2013

Figura No.8

Porcentaje de personas de 12 años y más que usan Internet, según lugar de mayor frecuencia de uso, ENHOGAR-2013

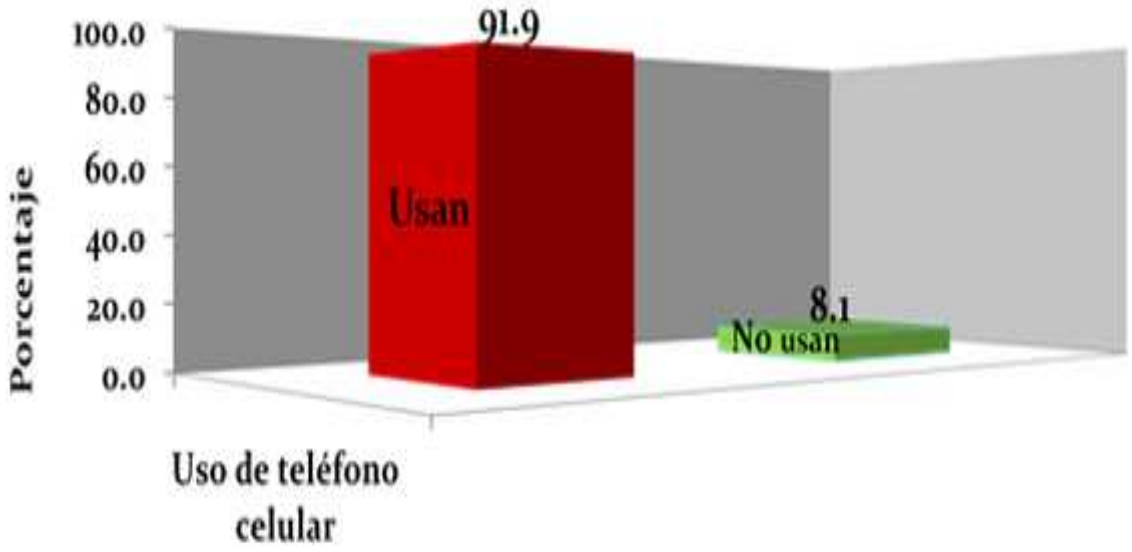


Fuente: Oficina Nacional de Estadística. ENHOGAR-2013

Según la encuesta por la Oficina Nacional de Estadística 2013, en la Figura No. 9, informa que en República Dominicana el Porcentaje de personas de 12 años y más, el 91.9% utilizan celular mientras que un 8.1 no utiliza el dispositivo.

Figura No.9

Porcentaje de personas de 12 años y más, según condición de uso teléfono celular, ENHOGAR-2013

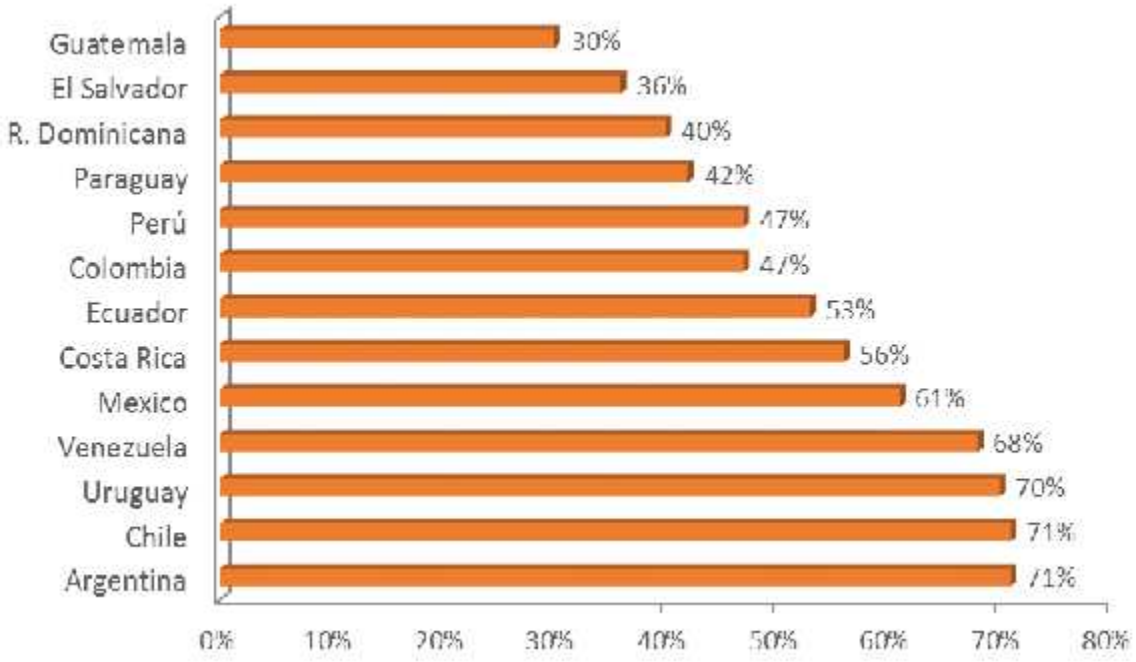


Fuente: Oficina Nacional de Estadística. ENHOGAR-2013

Según Mite Nishio (2014), la Figura No. 10 muestra como los internautas de República Dominicana tuvieron una participación de 40% en compras las cuales ascendieron para el referido año a 737.7 millones de dólares. Esta es una muestra de cómo las tarjetas de créditos permiten lograr un comercio que no se limite a un espacio físico, o tiempo lo cual encierre al usuario en su decisión de compra.

Figura No.10

Porcentaje de Internautas en República Dominicana que compran en internet. Países por debajo del 68%, eMarketer calcula y trae a proyección que habrá para 2015 un incremento impresionante a US$28 mil millones en compras aumentando así también el margen de los participantes.



(Tendencias Digitales 2012)

El comercio electrónico continúa impulsándose cada día en Latinoamérica, según la encuesta realizada por Tendencias Digitales Media Consulting a internautas de 13 países de Latinoamérica, reflejó que el 59% de ellos reportaron que compraron productos por internet durante el último año, donde República Dominicana muestra una participación de 40% de su población local.

Debido al gran impulso comercial que representa la participación de los países por debajo del 68% eMarketer calcula y trae a proyección que habrá para 2015 un incremento impresionante a US$28 mil millones. Según Tendencias Digitales los productos más comprados por internet son: boletos para entretenimiento o pasajes, accesorios para computadoras, indumentaria, zapatos, accesorios y libros.

En República Dominicana las instituciones de Courier han estimado que un promedio de 65,000 dominicanos realizan sus compras mensualmente a través de Internet, lo cual corresponde unos 500,000 al año. En 2011 la Oficina Nacional de Estadística, da a conocer que del 11.7% de los hogares dominicanos con acceso a la web, apenas el 11% compra por esta vía, lo que es igual a un total de 426,756 personas, equivalente al 4.3% de la población de dicho año.[44]

3.5. Casos Resueltos de Phishing por Entidades Bancarias en R.D.

Según la Tabla No. 3, se analizan 11 entidades de intermediación financiera para el periodo 2007 – 2014 que prestan sus servicios en República Dominicana, las cuales presentan una lucha contra el fraude ante la amenaza del pishing, mostrando cantidades de casos resueltos y montos recuperados, por confidencialidad de las empresas, las enunciaremos en anonimato y en nuestro análisis haremos énfasis en las tres entidades que han tenido mayor impacto. La Entidad Bancaria 01, representa el 32% del total de casos resueltos, recuperando RD$ 8, 780,704.00, mientras que la entidad Bancaria 02 representa 15% de la totalidad de casos resueltos, recuperando RD$ 22, 552,944.00 y US$ 12,000.00, seguido por La Entidad Bancaria 03 que muestra el 39% del total de casos resueltos, recuperando RD$ 14, 843,745.00, US$ 74,429.89 y EUR$ 1,000.00, mientras que las demás entidades representan incidencias de menor escala. Esto es una prueba del impacto amenazante que posee la actividad llamada phishing y la simple razón de que la seguridad inicia por el usuario de los servicios financieros. Hoy día, el dinero plástico y el comercio virtual van más allá de una moda ya que es una necesidad latente y comercial.

[44] Listin Diario (2014).Comercio Electrónico. Ventas por Internet se estiman en RD$4,500 MM. Disponible en: http://www.listindiario.com/economia-and-negocios/2014/1/5/305737/Ventas-por-Internet-se-estiman-en-RD4500-MM

Tabla No.3

Estadística de casos resueltos de phishing por Entidades Bancarias de la República Dominicana. 2007 – 2014.

ENTIDADES BANCARIAS	CASOS RESUELTOS	MONTOS EN PESOS	MONTOS EN DOLARES	MONTOS EN EUROS
ENTIDAD BANCARIA 01	139	8,780,704.00	/	/
ENTIDAD BANCARIA 02	66	22,552,944.00	12,000.00	/
ENTIDAD BANCARIA 03	168	14,843,745.00	74,429.89	1,000.00
ENTIDAD BANCARIA 04	7	2,697,192.00	/	/
ENTIDAD BANCARIA 05	11	1,129,242.00	24,784.19	/
ENTIDAD BANCARIA 06	1	1,666,000.00	/	/
ENTIDAD BANCARIA 07	1	/	/	378.00
ENTIDAD BANCARIA 08	8	120,649.14	/	/
ENTIDAD BANCARIA 09	1	/	/	5,777.00
ENTIDAD BANCARIA 10	28	1,805,725.00	1,654,185.00	/
ENTIDAD BANCARIA 11	2	/	/	35,952.00
TOTAL MONTOS	432	53,596,201.14	1,765,399	43,107.00

(Fuente: Departamento de Investigación de Crímenes y Delitos de Alta Tecnología DICAT, P.N.)

3.6. Análisis de las denuncias, fraudes, sometimientos y casos resueltos por el DICAT.

Según la Figura No. 11, se pueden identificar con facilidad las denuncias, casos resueltos por clonación de tarjeta de crédito, phishing, y a la vez los involucrados sometidos de nacionalidad local y extranjera durante el periodo 2007 – 2014. Existen 299 denuncias por clonación de tarjetas de crédito mientras que los casos resueltos comprenden un total de 697 casos resueltos y un total 312 requerimientos compuestos por personas nacionales, sometidas a un proceso penal, mientras que 17 casos sometidos representando personas extranjeras. A la vez encontramos 906 casos denunciados por fraude de phishing mientras que 775 han sido resueltos a lo largo del periodo mencionado, así mismo 734 casos sometidos a personas nacionales mientras que en adición hay 2 casos representados por extranjeros.

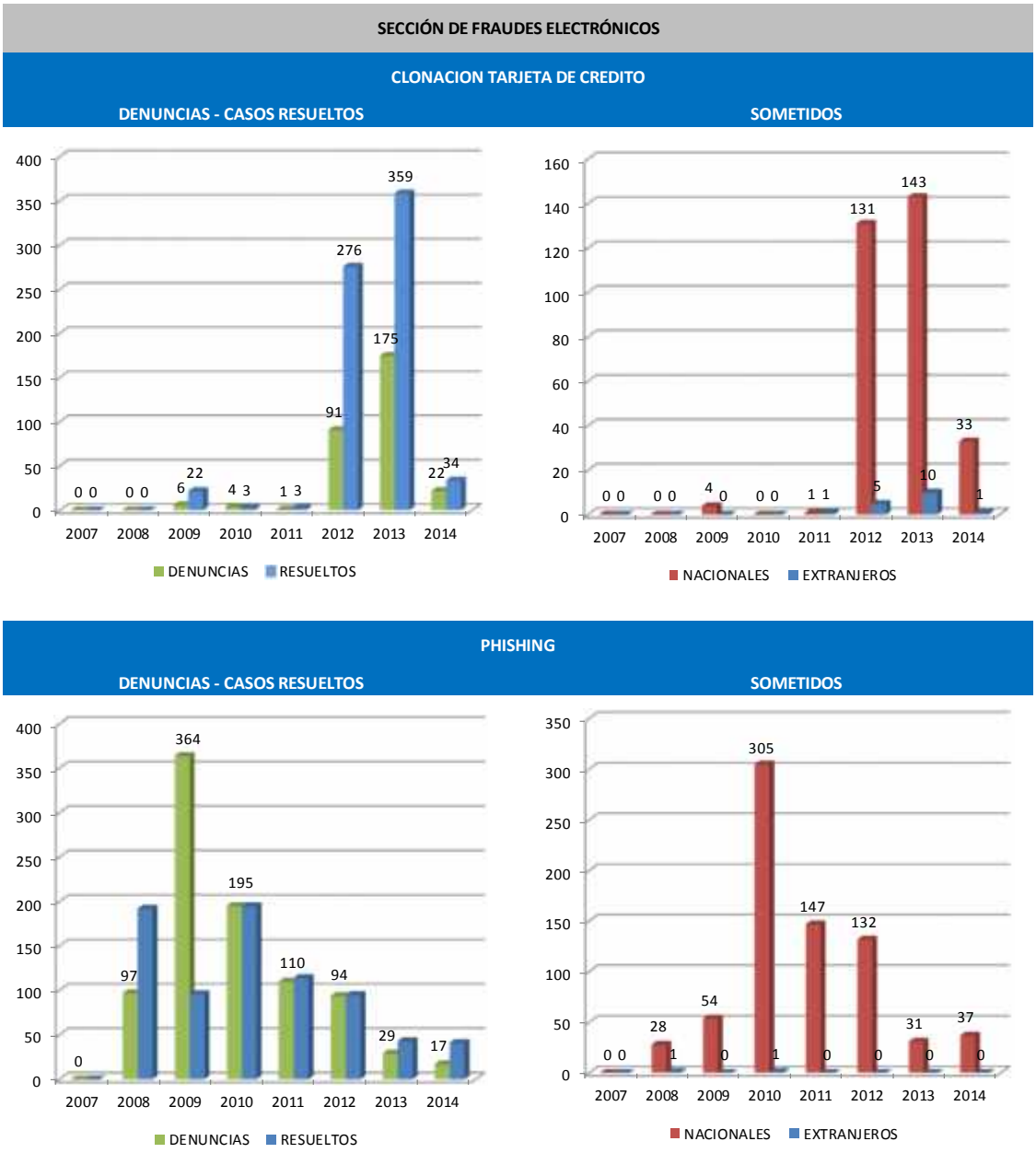
Figura No.11

Sección de Fraudes Electrónicos Tarjetas de Crédito y Phishing 2014.

POLICIA NACIONAL

DIRECCION CENTRAL DE INVESTIGACIONES CRIMINALES

DEPARTAMENTO DE INVESTIGACION DE CRIMENES Y DELITOS DE ALTA TECNOLOGIA



(Fuente: Ing. Carlos Leonardo, Sub-coordinador Sección Fraudes Electrónicos, Analista Forense IT, Departamento de Investigación de Crímenes y Delitos de Alta Tecnología DICAT, P.N., 2014)

CAPITULO IV- MEDIDAS DE PREVENCIÓN MEDIANTE LOS FRAUDES CIBERNÉTICOS EN REPÚBLICA DOMINICANA.

Después de haber conocido de manera real y empírica cual es la volatilidad que conlleva el uso de los servicios electrónicos, a continuación mostraremos propuestas, iniciativas y acciones que debemos tomar en cuenta para evitar ser víctimas de estos delincuentes que cada día están innovando la diversidad del fraude en todo el sistema de los servicios electrónicos de la Republica Dominicana.

4.1. Identificación del Ciberdelincuente

Según Rijo (2013), explica que desde el punto de vista jurídico la identificación del lugar y el usuario que comete la infracción son esenciales para iniciar una exploración y persecución, nos referimos a un cimiento que permita el debido proceso. La Magistrada Esther E. Angelán Casasnovas atestigua que la principal dificultad para reconocer al ciberdelincuente es que las actividades en el ciberespacio, por ser un espacio virtual, complejo y que carece de fronteras físicas por su naturaleza dificulta identificar con seguridad la procedencia de los ataques realizados posiblemente a miles de kilómetros de distancia. Un informe divulgado por el Centro Nacional de Coordinación de Respuesta de Emergencia de la Red de Computadoras, la principal red de supervisión de seguridad informática de China dice: "No podemos estar completamente seguros de que un ataque se llevó a cabo en un país extranjero simplemente porque la dirección IP del atacante se localizó en ese mismo. De la misma manera, es imposible decir con seguridad que los autores de ciberataques, cuyas direcciones IP se ubican en China por ejemplo, son realmente de este país." Asimismo entre las formas de localización del infractor se encuentran las siguientes:

Un número localizador: las computadoras modernas son capaces de direccionar las actividades que realizan. Por medio del IP: consiste en un número binario que permite identificar el ordenador que es utilizado por el infractor. En el caso de República Dominicana este número es asignado por la Internet Corporation for Assigned Names and Numbers (ICANN) la cual es una organización que opera a nivel internacional y es la responsable de asignar las direcciones del protocolo, de los identificadores de protocolo (IP). Por estos medios podemos identificar el lugar y el computador que el infractor ha utilizado para efectuar el delito, sin embargo, en lugares como las zonas WI-FI y los cibercafés existen limitaciones para identificar a estos delincuentes.

Casasnovas expone que las zonas WI-FI son áreas de acceso a Internet inalámbrico que algunas entidades gubernamentales o privadas facilitan a los usuarios de forma gratuita o pagando un valor. En República Dominicana este servicio lo ofrece de forma gratuita el Ministerio de la Juventud, la Suprema Corte de Justicia, algunos Food Shops de las estaciones de combustible vehicular, entre otros. La falta de un estatuto que obligue a los usuarios a identificarse antes de acceder a Internet facilitado por los proveedores en zonas WI-FI, constituye un obstáculo para las investigaciones criminales. Por otra parte, las zonas WI-FI domésticas, afrontan la dificultad de que muchos proveedores de servicios no indican eficientemente a los clientes al momento de adquirir el servicio de Internet inalámbrico, sobre la importancia de tomar medidas de seguridad, tales como colocar claves de acceso, de lo contrario, el usuario estará dentro de las probabilidades de que se comentan infracciones utilizando el IP de su servicio, con la desventaja de que lo convertirá en sospechoso de las acciones delictivas cometidas.

Según la entrevista sostenida con el Ing. Hiddekkel Morrison, nos da un ejemplo de un Hacker que identifica a una posible victima que está compartiendo su WIFI y el ciberdelincuente consiente de esa vulnerabilidad utiliza la IP ajena para fines delictivos, en este caso aunque la persecución va en contra del dueño

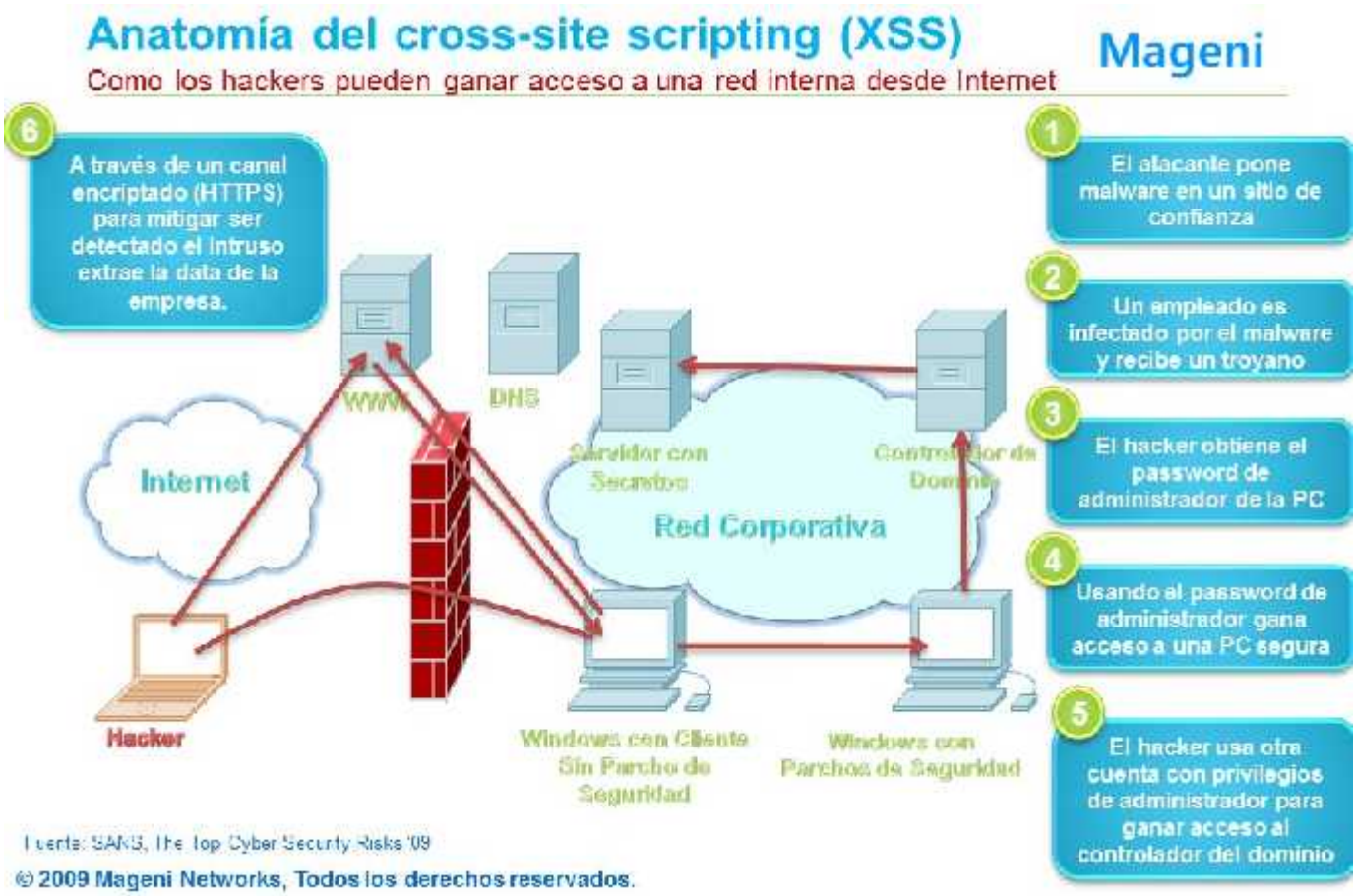
de la IP, la ley de delitos de altas tecnología da lugar a que se pueda investigar de manera más a fondo quien es el verdadero culpable del delito electrónico. Es importante que los usuarios estén informados ya que en lo que se investiga puede ir preso o detenido por la ley. Otra vertiente desde el mismo ejemplo, si es una Institución financiera la afectada puede hacer la demanda a la policía y entonces al detectar que se utilizó la IP de una víctima, dicho inocente por el grado de compromiso será que tenga que ser detenido mientras se investiga el caso.

El Ing., Morrison también nos explica como los delincuentes ejecutan el pishing a los usuarios de internet, en la Figura No.12 se ilustra el proceso de un phishing, el atacante crea el correo electrónico y la página digital falsa, luego utilizando tanto el correo como la página falsa los envía a los usuarios, los cibernautas victimas reciben el correo falso, acceden a la página falsa que se envía en el correo falso, los usuarios son estafados en la página digital falsa al completar los datos que les solicitan, estos a creer que están en un dominio conocido son engañados.

Figura No.12
Proceso de un Phishing

Según la Figura No.13, los Hackers de igual forma para entrar a una red corporativa utilizan los siguientes parámetros, el delincuente coloca el malware en un sitio de confianza, luego un empleado es infectado por un malware y recibe un troyano, el hacker obtiene el password como administrador de la PC, haciendo uso del acceso administrador gana acceso como usuario a una PC segura, así gana los acceso como administrador controlador del dominio habilitándose a su vez todos privilegios y a través de un canal encriptado extrae toda la data de la empresa.

Figura No.13
Proceso del Cross-Site Striping



4.2. Mitigación de Riesgos para Fraudes Electrónicos

Mitigación de Cross Site Scripting en las Empresas

- Implementar la modelación de intimidaciones.
- Validar todas las entradas de datos a las herramientas.
- Implementar listas negras que filtren los caracteres: < # > ‘ “
- Auditar cada año el código de sus aplicaciones.
- Capacitación continua en los programadores sobre seguridad.
- Realizar pruebas de penetración es un buen ejercicio.
- Aplicar políticas y normas de seguridad web exhaustiva.

Mitigar el Riesgo Del Phishing en las Empresas

- Implementar programas de educación Anti Fraude/Phishing para clientes, además esto impulsara la confianza de los servicios.

Auditoria Forense

Ejecutar Auditoria Forense en el proceso de estudio y compilación de evidencias post-incidentes de un procedimiento ha sido comprometido con el con el propósito realizar acciones legales contra los ciberdelicuentes o hackers. Esto produce las siguientes ventajas: minimiza el impacto de una incidencia de seguridad, minimiza costos, provee confianza a los clientes y usuarios, facilita la aplicación de medidas legales contra los hackers.

Mitigar los Troyanos en las Empresas

- Concientizar y educar los clientes usuarios y empleados en información de seguridad.
- Realizar intentos de penetración comprensivas.

Mitigar las URL zone en las empresas:

Es complejo detectar estos fraudes y peor aún detenerlos, la mejor opción es prevenirlos. Una educación proactiva a clientes y empleados puede ser más favorable que invertir en costosos recursos tecnológicos que no mitigaran este riesgo. Cabe destacar que el factor humano siempre es el más débil cuando hablamos de seguridad.

Algunos ejemplos de las acciones que el usuario debe tener en cuenta para evitar convertirse en una víctima.

- No descargar cracks, casi todos (o todos) son troyanos
- Google Chrome registrada tiene medidas de seguridad para mitigar este riesgo
- No visitar páginas de dudosa reputación
- Revisar los balances desde otra computadora si se algo anormal
- Mantener actualizados los softwares (PDF, Flash, Office, Zip, WMP, etc)
- No ejecutar programas que sean enviados para solucionar virus

4.3. Medidas de Prevención para minimizar los riesgos en la red del usuario

Passwords / Contraseñas

- Mantener en secreto la contraseña es la primera garantía de individualidad y privacidad.
- No compartir el password.
- Evitar que sea fácilmente deducible. Ej. Número de tarjeta, de cédula, nombre o apellidos relacionados, lugares, empresas, etc…

- Usar palabras o frases sin sentido como password, mientras tenga mayor cantidad de caracteres será mejor.
- El grupo de soporte técnico nunca tendrá necesidad de saber el password del usuario.

¿Cómo protegerse de ser hackeado?

- Evitar hacer clic en enlaces sospechosos recibidos por correo, aun sea el remitente una persona conocida.
- Ninguna institución financiera solicita actualización de datos por correo.
- No escribir ni compartir número de tarjetas ni contraseñas por correo, chat o redes sociales, pues podrían ser fácilmente obtenidos por terceros.
- Evitar en lo posible usar cybercafes para entrar al correo o cuenta del banco.
- Tampoco entrar a las cuentas en otras computadoras que se encuentren en casas de amigos u otros sitios.
- No poner preguntas muy personales para fines de recuperación de contraseña.
- Tener antivirus actualizado y hacer análisis periódicos.
- Instalar programas de dudoso origen, son propensos a riesgo corrupto o virus.
- Mantener siempre activo el cortafuego para que evite el ingreso de programas sospechosos.
- Utilizar contraseñas largas, alfanuméricas y que contengan mayúsculas y minúsculas; ya que existen programas que obtienen las contraseñas débiles.
- Evitar el envío de correos masivos o cadenas.
- No aceptar personas desconocidas en las redes sociales. Podrían ser identidades falsas y con malas intenciones

- Ver y percatarse siempre al hacer compras en línea, fijarse en la parte superior de la página, que contenga el protocolo HTTPS, porque la S significa que es una página verificada y por lo tanto segura.
- No revelar datos como nombre completo, número de documento, direcciones o teléfonos en las cuentas de correo o redes sociales.
- Nunca hacer click en páginas que digan que se ha ganado algo. En la mayoría de los casos es una trampa.

¿Cómo protegerse al navegar?

Comprobando la configuración de los perfiles: es importante revisar el grado de privacidad que has elegido para tu perfil en las redes sociales y foros en los que participas. Confirma que tienes bien configurada la privacidad de tu información y fotos, y en las que te han etiquetado. Al navegar desde una PC compartida, recuerda cerrar la sesión de todas tus cuentas de email o páginas en las que estés registrado cada vez que te conectas.

No reenviar cadenas: Nunca reenvíes a todos tus contactos las famosas ‘cadenas’, con decenas de destinatarios y piden una respuesta inmediata y multitudinaria, ya que con frecuencia contienen virus, incluso cuando es un contacto propio y de confianza quien lo envía. Son correos falsos, también conocidos como ‘hoax’, y sirven para recopilar miles de direcciones de mails.

Internet no olvida ni perdona: Recuerda que "internet no olvida" fácilmente la información, expresiones o imágenes que tú, gente de tu entorno, empresas y páginas de todo tipo cuelgan en la web sobre ti.

Sólo amigos verdaderos: Antes de aceptar una petición de amistad o de agregar tú a alguien en cualquiera de las redes sociales, piensa si en verdad le conoces, no agregues personas desconocidas.

CONCLUSIONES

De acuerdo a la información de la Procuraduría de la República Dominicana, refleja que el ochenta por ciento de los clientes de las instituciones bancarias han sido afectados por el ciberdelito, siendo las consecuencias principales la clonación de tarjetas, transferencia de dinero, y phishing. Asimismo, la Dirección Central de Investigaciones Criminales (Dicrim), revelo que en enero de 2014 desmantelaron dos laboratorios clandestinos utilizados para clonar tarjetas de crédito y débito, procediendo a estafar bancos, comercios y usuarios.

A través de este estudio de investigación abordamos los elementos que inciden en los fraudes cibernéticos dentro del Sistema Bancario Dominicano, hemos determinado por medio de los datos facilitados por el Departamento de Investigaciones de Crímenes de Alta Tecnología (DICAT) y la Superintendencia de Bancos como el órgano regulador del sistema financiero, que el phishing es sin lugar a dudas una de las estrategias más utilizadas por los ciberdelincuentes, los cuales desarrollan correos electrónicos, enlaces y páginas web pareciendo confiables para los usuarios y así extraer sus datos personales con los cuales logran realizar el fraude.

Los resultados que hemos podido determinar inclinados a once entidades de Republica Dominicana en el servicio intermediación financiera desde 2007 al 2014, tienen al momento 432 casos resueltos, esto representa una recuperación alrededor de RD$ 53.5 MM, en USD$ 1.7 MM, y en EUR$ 43.1 M, esta es una muestra de que los órganos reguladores están esforzándose por cumplir con su propósito pero es necesario fortalecer e innovar en todo lo que compromete la protección y seguridad de la información. Hemos identificado que durante el periodo 2007 al 2014, existen 299 denuncias por clonación de tarjetas de crédito y 697 de casos resueltos además de que los delitos fueron accionados por 312 personas nacionales las cuales fueron sometidas a un proceso penal, mientras que 17 casos sometidos corresponde a extranjeros.

El veintidós por ciento de los usuarios de Kaspersky Lab, han sido víctimas de fraudes en la red de Facebook, cada día hay más de 200,000 casos donde los usuarios por desconocimiento y engaño hacen intento de clic en enlaces que dirigen a páginas web de Facebook falsas. Así mismo, le empresa de seguridad de la información AVAST, reportó que tan solo en la penúltima semana de abril 2015 detuvieron en todo el mundo más de 11.5 millones de intentos de hackers. Basado en el análisis realizado en esta investigación, desde 2007 al 2014 hemos podido determinar que la red social que posee mayor cantidad de delitos es Facebook, con un 77% de casos por difamación, el 11% por robo de identidad, el 10% a través de hacking, el 1% de acoso y finalmente 1% por chantaje.

En otra modalidad de fraude electrónico, empresas telefónicas importantes del país fueron afectadas en 2014 por más de RD$10 MM a través de la estrategia delictiva Bypass la cual consiste en un enlace internacional que requiere de la instalación de equipos de telecomunicaciones y líneas telefónicas cuya interconexión le permite establecer una ruta del tráfico telefónico internacional sin contar con la autorización debida según demanda la Ley. El bypass realiza la estafa a una operadora telefónica establecida legalmente, la cual genera evasión de impuestos y explota el servicio que por concesión le corresponde a compañías que están autorizadas para prestar ese tipo de servicios. Esta Banda fue interceptada por el Departamento de Investigaciones de Crímenes y Delitos de Alta Tecnología (DICAT) en diciembre 2014, donde allanaron simultáneamente a los integrantes en diferentes provincias del país.

Así mismo, los fraudes a través de las tarjetas de crédito no tan solo amenazan a los usuarios sino también a las empresas. Un factor decepcionante es que la clonación de tarjetas la cual se lleva a cabo a través de un instrumento llamado skimmer o beeper, este dispositivo no fue creado para tal propósito, pero los delincuentes aprovechan la herramienta para tales fines delictivos.

RECOMENDACIONES

Según los resultados abordados en la presente investigación, recomendamos lo siguiente para evitar fraudes electrónicos:

A las Entidades de Intermediación Financiera:

- Cada entidad financiera debe orientar a sus clientes de todos los detalles más actualizados sobre delitos cibernéticos de manera interactiva en su plataforma virtual.

- Toda entidad financiera podría facilitar softwares de seguridad en sus dominios virtuales para proteger la información financiera de sus clientes. Por lo general, los usuarios tienden a depender de antivirus gratuitos con poca capacidad de protección virtual.

- Realice pruebas de penetración a un sistema después de cada actualización y a su organización de forma continua.

- Aplicar Auditoria Forense para el proceso de análisis y recolección de evidencias post-incidente.

- El mayor logro que puede alcanzar una entidad que preste servicios electrónicos es convencer al mercado que garantiza la seguridad electrónica que se merece.

- Implementar tecnología de chip y token a productos de tarjetas de crédito, débito y el acceso a internet banking. (cabe destacar que algunas empresas están ya han incursionado esta optima estrategia).

Al Usuario:

- Al recibir un correo electrónico que no le parezca legítimo, no debe acceder al mismo, lo más recomendable es borrarlo o guardarlo hasta identificar la procedencia de origen.

- Para acceder a un sitio web, es importante digitar por uno mismo la dirección en el navegador y tomar en cuenta el icono del candado cerrado en la barra de direcciones justo en la parte superior a la izquierda, de esta manera el dominio será reconocido con una certificación de lugar seguro.

- Es importante tener en precisa confidencialidad los datos personales al igual que las claves de seguridad y PIN, es riesgoso enviar dichas informaciones a otros sin excepción alguna de la vía.

- No enviar datos personales o financieros a través de mensajes electrónicos a ningún amigo o relacionado. Estos medios no prometen seguridad.

- Hacer cambios de contraseñas constantemente.

- Borrar periódicamente los registros de cookies e históricos de navegación.

- Tener un antivirus actualizado y con licencia, no gratuito.

- Muy importante no utilizar nuestros datos personales en dispositivos públicos o de poca seguridad de igual forma no hacer ningún tipo de transacción bancaria.

- Utilizar herramientas anti phishing que se puedan adherir al navegador virtual, al igual que el correo, tener software anti-spam, firewall personal manteniendo al día las actualizaciones.

- Los usuarios de servicios telefónicos ya sea residencial o móvil, no deben suministrar datos por esa vía y mucho menos si le solicitan desde números desconocidos.

A la Administración Pública:

- Actualizar la ley 53-07 y la ley No.153-98, de manera exhaustiva en la diversidad de fraudes que se comenten y las sanciones que se le impongan a estos delitos.

- Impulsar un plan de seguridad de la información en la red.

- Emprender campañas de concientización de fraude cibernético que ayuden a elevar la confianza en los servicios de internet.

- Crear proyectos incentivando jóvenes al aprendizaje de la seguridad de información así logrando desarrollo personal y aporte a la sociedad.

- Proponer a los fabricantes de computadoras que el ensamblaje del equipo contenga un código serial de fábrica capaz de accionar el desahucio del computador. Ejemplo: la víctima de un computador robado agota un protocolo obligatorio desde una página web del fabricante, haciendo la denuncia, el equipo electrónico al conectarse a internet es detectado y automáticamente se inhabilita hasta quedar inservible, ubicando al delincuente desde la IP y protegiendo la información lo cual aportaría el desinterés de los delincuentes por robar equipos ya que no podrán sacar ningún beneficio del computador.

BIBLIOGRAFIA

Audiencia Electrónica (2010). Citado por Hiddekel Morrison en su artículo titulado: "Afirman que la banca electrónica de la Republica Dominicana es segura". Disponible en: http://www.audienciaelectronica.net/2010/11/19/afirman-que-la-banca-electronica-de-la-republica-dominicana-es-segura/

Audiencia Electrónica (2010). Reportaje televisivo transmitido en el programa "Nuria en el 9″ disponible en el sitio Web: http://www.audienciaelectronica.net/2010/04/28/reportaje-de-nuria-internet-en-republica-dominicana/

Banco Popular Dominicano (2014). Pistas de Seguridad, Disponible en: https://www.bpd.com.do/sites/bpdpublico/SP/Informacion_Corporativa/Paginas/pistas-de-seguridad.aspx

Boletín Informativo Lacnic News (2014). Encuesta e Impacto del ciberdelito en America Latina y el Caribe. Disponible en: http://prensa.lacnic.net/news/edition/febrero2013_es

Casasnovas, Angelán E. 2011 "Ciberdelincuencia y política criminal. Internet: nuevo reto jurídico-penal", Editora Premium, Santiago de los Caballeros.

Dacanet (2008). "Procuraduría solicita ingreso de Rep. Dom. a convenio contra el cibercrimen" Disponible en: http://www.dacanet.com/?p=36

Diario Libre (2014). Fraudes Bancarios son los Ciberdelitos, Disponible en: http://www.diariolibre.com/destacada/2014/02/11/i477561_fraudes-bancarios-son-los-ciberdelitos.html

Diario Libre (2014). Ataques Pishing desviaron RD$120 Millones en Bancos. Disponible en: http://www.diariolibre.com/destacada/2014/02/12/i478961_ataques phishing-desviaron-rd120-millones-bancos.html

Evidencias Digital (2014). Extorsiones telefónicas a la orden del día en República Dominicana. Disponible en: http://evidenciasdigital.com/?p=890#sthash.0OvlfRMT.dpuf

Funglode (2014) Los Fraudes Cibernéticos ¿Una batalla pérdida? Disponible en: http://cdri.funglode.org.do/index.php?option=com_content&view=article&id=480:los-fraudes-ciberneticos-iuna-batalla-perdida&catid=229:novedades&Itemid=86

García. T. (2010) Diccionario el Pequeño Larousse Ilustrado. México.

Gits informática. (2014). Ciber seguridad informática y delitos telemáticos. Disponible en: http://www.gitsinformatica.com/vishing.html

Hoy (2007). Respondiéndote que es la Banca Electrónica. Disponible en: http://hoy.com.do/respondiendoteque-es-la-banca-electronica

Hoy (2014). A un “clic del peligro” Con clonación de tarjetas de crédito y otros ciberdelitos. Disponible en: http://hoy.com.do/a-un-clic-del-peligro-con-clonacion-de-tarjetas-de-credito-y-otros-ciberdelitos/

Kaspersky (2014). Para los adictos a las redes sociales: Facebook es el portal principal de phishing. Disponible en: http://blog.kaspersky.es/1-de-cada-5-fraudes-de-phishing-afecta-a-facebook/3694/

Listín Diario (2014).Comercio Electrónico. Ventas por Internet se estiman en RD$4,500 MM. Disponible en: http://www.listindiario.com/economia-and-negocios/2014/1/5/305737/Ventas-por-Internet-se-estiman-en-RD4500-MM

Mariscos Locos. El Origen y Evolución Histórica de las Tarjetas de Crédito (2007). Disponible en: http://edrismilgrullon.blogspot.com/2007/01/sabia-usted-acerca-de.html

Medina, P. (2009). El Delito Informático Realidad Procesal en República Dominicana. Disponible en: http://visionlegal-analisisjuridico.blogspot.com/2009/08/el-delito-informatico-realidad-procesal.html

Morrison, Hiddekel. (2009), libro titulado: “La República Dominicana en la Sociedad de la Información” p.43 OMNIMEDIA 2009.

OMG (2014). Noticias y Publicaciones. Disponible en: http://www.omg.com.do/guia_de_negocios/Telecomunicaciones/

Proyecto Amparo (2013). Ciberdelito en América Latina y el Caribe. Disponible en: http://www.proyectoamparo.net/

Ramírez, M. (2011). La Banca en República Dominicana. La Banca en República Dominicana.

Sibci. (2013). Estudio revela el aumento de ataques cibernéticos a usuarios de redes sociales en 2013. Disponible en: http://www.sibci.gob.ve/2013/10/estudio-revela-el-aumento-de-ataques-ciberneticos-a-usuarios-de-redes-sociales-en-2013/

Symantec. (2014) El mercado negro del crimen cibernético.Disponible en: http://www.symantec.com/region/mx/avcenter/cybercrime/index_page5.html

Sfmnews (2014). Fraudes Bancarios. Disponible en: http://www.sfmnews.com/2014/02/fraudes-bancarios-son-el-80-de-los.html

Taiguey (2009). Presidente de Indotel llama a atacar ciberdelincuencia. Disponible en: http://taiguey.org/cact-dom/prensa.php?msg=prensa_tics_dom-1923&lang=es

ANEXOS

Entrevista a: Ing. Hidekkel Morrison

Noviembre: 2014 (CD anexo)

HM Consulting

Autores: Personal del departamento de monitoreo, reguladores, responsables de custodiar a través de herramientas informáticas, las transacciones realizadas por los clientes de diferentes instituciones bancarias, en los diferentes dispositivos existentes en el mercado.

Somos estudiantes de la Maestría Gerencia y Productividad de la Universidad APEC y estamos realizando una investigación sobre las causas del incremento de los fraudes en los Sistemas Financieros Bancarios en los últimos dos años. Para lograr la realización de nuestro trabajo investigativo solicitamos responda a la siguiente entrevista.

¿Cuál es el marco legal que penaliza los delitos de transacciones fraudulentas en los servicios financieros y cuáles son las sanciones más significativas que estipula esta ley?

Primero es bueno entender que hay una diversidad de disposiciones legales y de leyes podríamos decir, bien antiguas pero que tienen presencia dependiendo el tipo de delito que se lleve a cabo. Por ejemplo están las estafas, fraudes y así existen las disposiciones legales que no importa el medio que el delincuente utilice para hacer la estafa, así está penalizado por la ley, luego ante el avance de los medios electrónicos, se han ido identificando leyes puntuales para poder tipificar y poder perseguir de forma más efectiva este tipo de delitos a través del sistema financiero a través de nuestro territorio.

Tenemos una ley de delitos y crímenes de alta tecnología (Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología) es la que agrupa y desenvuelve la mayor cantidad y cuasi totalidad de delitos que se puedan llevar a cabo por sistemas electrónicos y por supuesto todo el tema de los fraudes en el sistema financiero nacional.

Luego encontraríamos una ley en telecomunicaciones (La Ley General de Telecomunicaciones número 153-98) que tiene unos aspectos vinculados a llevar a cabo hechos delictivos utilizando medios te telecomunicaciones.

Entonces de manera puntual podríamos decir que esas son las dos leyes básicas y luego existen leyes más antiguas que pueden ser referidas al momento de imputar a alguien en un tipo de fraude de ciberdelitos.

¿Quién emite dichas leyes en telecomunicaciones?

La Ley General de Telecomunicaciones número 153-98, es promulgada por el poder Ejecutivo y aprobada por el Congreso Nacional, una vez está vigente ya cualquier transgresión a la Ley, puede la persona que transgrede ser objeto de acción penal o una demanda. En el concepto de las telecomunicaciones hay un órgano regulador que es el Indotel que es un órgano que surge por mandato de esa ley pero la misma no se limita solo a eso sino que también se vincula y tiene aspecto al delito electrónico en el tema bancario.

¿Podría darnos un ejemplo de un delito que atribuya la disposición de cumplimiento de esta ley?

Claro, una persona hace uso de una IP de alguien que está compartiendo su WIFI y la persona delincuente consiente de esa vulnerabilidad utiliza la IP ajena para fines delictivos, en este caso aunque la persecución va en contra del dueño de la IP, la ley de delitos de altas tecnología da lugar a que se pueda investigar de manera más a fondo quien es el verdadero culpable del delito electrónico. Es importante que los usuarios estén informados ya que en lo que se investiga puede ir preso o detenido por la ley. Otra vertiente desde el mismo ejemplo, si es una Institución financiera la afectada puede hacer la demanda a la policía y entonces al detectar que se utilizó la IP de una víctima, dicho inocente por el grado de compromiso será que tenga que ser detenido mientras se investiga el caso.

¿Considera usted que la cantidad de fraudes electrónicos son provocados mayormente por extranjeros que por dominicanos?

Yo diría que sí, conforme a los datos que he tenido acceso.

¿Cuáles son las modalidades más utilizadas para realizar los fraudes cibernéticos, y cuál es la más predominante?

Pishing y Clonación de tarjetas de créditos.
La que es más común y que parte su origen desde Nigeria un país Africano lo que se llama como el Phishing o la Pesca. Es un procedimiento donde un grupo de especialistas manejando una base de datos envía correos electrónicos con la identidad fantasma de empresas reales para engañar a sus víctimas.

¿A qué se debe que la mayor cantidad de clonación de tarjetas de créditos se realizan en una estación de gasolina o el consumo se refleja en un lugar distante?

En realidad la clonación de tarjeta de crédito es vulnerable a ocurrir en cualquier establecimiento como un restaurante al igual que en un hotel cinco estrellas. A diferencia de una estación de gasolinera la particularidad será que se podrá más fácil en los dos lugares antes dichos para cometer el delito.

Por ejemplo: el delincuente le ofrece al empleado de la estación una paga si utiliza un dispositivo llamado Skimmer para el pago de las tarjetas, si el individuo acepta, se hace cómplice y el delincuente al final posee en su disco duro los códigos de la tarjetas, agota el proceso de clonación del plástico y crea un duplicado que le permitirá hacer consumo sin importar el lugar del país.

¿Cómo se hace el delincuente para obtener un Skimmer, no existe un regulador y requisitos que deba agotar la persona que desee adquirirlos?

Bueno, el Skimmer es fácil de obtenerlo ya que se puede comprar a través del internet, y no existe un regulador que limite al comprador de dicho dispositivo.

¿Si el Skimmer es tan fácil de utiliza para fines delictivos porque se vende de esa manera?

Un ejemplo consumidor legal son los hoteles, cada vez que las llaves de las habitaciones se pierden, la única forma de solucionar el problema es creando un duplicado, ósea, este es el objetivo de este dispositivo.

A modo de empresa, mencione algunos factores internos y externos que han podido incidir en el incremento de los fraudes bancarios, en los últimos dos años.

El riesgo mayor se encuentra en el usuario interno de la empresa. Por ejemplo, en una USB puede sustraer toda la información que pueda usarse para fines de delito.

Luego podemos citar ejemplos como accesos a páginas de internet maliciosas desde la empresa o con el recibo y envió de mailing maliciosa, entre otros.

¿Cuál es la diferencia entre un virus y un Malware?

El virus tiene el objetivo de dañar lentamente el equipo infectado afectando progresivamente el software, sin embargado el Malware no tan solo afecta la computadora sino que vulnera los datos para fines delictivos.

¿Existe algún antivirus que considere perfecto o infalible ante esta modalidad de riesgo?

No existe una seguridad perfecta, existen niveles de dificultad ya que diariamente se generan más de tres mil virus diarios.

¿Qué sugiere a aquellos usuarios que por desconocimientos o por falta de presupuesto no tienen un antivirus que asegure su información?

Es una pregunta muy importante, y es una falta de orientación, como es posible que si pagamos veinte mil pesos por una laptop que no estemos dispuestos a invertir en proteger a costo de una mínima y hasta anual.

Muchos se hacen dependientes de antivirus gratuitos que solo cubren el 30% pero no se percatan de que el riesgo está ahí por falta de conocimiento.

¿Cuándo escuchamos la palabra Hackers, pensamos en lo peor, necesariamente no existirían Hackers para bien?

El concepto de Hackers no es malo, Hack es una expresión muy técnica que quiere decir: manipular o alterar. En una época para desarrollar sistemas, los expertos manipulaban para prueba pero el problema es que en el presente el ejercicio ha crecido para fines delictivo.

Cabe destacar que grandes Hackers han terminado siendo contratados por Importantes empresas.

¿Podría mencionarnos algunos de los sistemas de controles más comunes utilizados en las instituciones bancarias para la previsión de los fraudes electrónicos financieros?

Si, existen empresas que utilizan el chip para tarjetas de bandas magnéticas, token o mecanismos de revalidación de información. De modo general están los controles de accesos, a la red, al sistema, a la empresa, deshabilitar puertos USB. Luego podemos citar una gama Fireworks, porta fuego, encriptados de datos, algoritmo combinado con el control de los usuarios y los elementos antes dicho.

En el aspecto de los clientes como usuarios, tener cierto grado al menos de conocimiento básico acerca de los riesgos al acceso de información desconocida.
Las capsulas informativas que eduquen al acceso de la información de la manera más segura.

¿Cómo considera usted que tan impactante han sido los delitos cibernéticos a la economía Dominicana?

Es proporcional al nivel de digitalización del país. Ósea, no todo el mundo tiene acceso a los medios electrónicos, solo el 70% de la población utiliza estos medios y por esta realidad no es que sea un impacto para alarmarse. Ahora bien, no es que no sea significativo o no tiene su valor, lo que sucede es que comparamos las cifras económicas y comparamos lo afectado con el nivel de los negocios podremos ver el peso del impacto.

¿Qué recomendación sugiere a los usuarios para evitar riesgos electrónicos?

La gran recomendación es la educación en cuanto al riesgo de la información.

Modelo de Encuesta.

Somos estudiantes de la Maestría Gerencia y Productividad de la Universidad APEC, la siguiente encuesta tiene como objetivo: “Análisis de los Fraudes en los Sistemas Electrónicos de la Banca de la República Dominicana año 2010 - 2014”. Su opinión es importante para nosotros.

Instrucciones: A continuación se presentara una serie de preguntas, por lo que le solicitamos que conteste de la manera más sincera, seleccione la respuesta que más se adecue a usted, Muchas Gracias.

1. **Sexo:**

   F □ M □

2. **Edad:**

   18-25 □ 26-35 □ 36-45 □ 46 o más □

3. **¿Posee usted negocio propio?**

   Sí □ No □

4. **¿Actualmente se encuentra laborando?**

   Sí □ No □

5. **¿Utiliza medios electrónicos como computadoras, cajeros automáticos, tarjetas de créditos, internet, etc…, para hacer sus operaciones?**

   Si □ No □

6. **¿Alguna vez ha sido víctima de un fraude cibernético o conoce de alguna persona afectada por el mismo?**

   Si □ No □

7. **¿Entonces, de haber ocurrido, cuál fue el medio del fraude?**

   Correo Electrónico □ Tarjeta de Crédito □ Vía Telefónica □

   Virus Informático □ Phishing □ Smart Phones □

   Maleware □ Redes Sociales □
   Otro_____

8. **¿A pesar de los fraudes existentes en el país, dejaría usted de utilizar los medios electrónicos para realizar sus transacciones personales?**

Si □ No □

9. **¿Es responsabilidad de los bancos eliminar los fraudes Cibernéticos?**

Sí □ No □ Bancos y personas □

10. **¿Cómo entiende usted que podemos combatir el Ciberdélito?**

No entrando páginas web desconocidas □
No dar datos personales en internet □
No descargar archivos desconocidos en la web □
No utilizar la tarjeta de crédito en lugares sospechosos □
No tener comunicaciones con extraños vía web □
No compartir Contraseñas de accesos □
No tener seguridad en la PC □
No utilizar Redes Wi-Fi públicas o computadoras de otras personas □
Utilizar sentido común □
Otros □_____

11. **¿Con cuál técnica fraudulenta has sido afectado?**

a) Retiro en cajero automático □
b) Fraude en comercios con la tarjeta □
c) Vía llamada de teléfono □

12. **¿Cómo le gustaría ser informado, sobre cómo prevenir el fraude?**

a) Brochure □
b) Internet □
c) Campaña de tv □
d) Otros medios □

13. **¿Considera usted que a pesar de los fuertes ataques cibernéticos, los sistemas financieros electrónicos son la clave al avance del futuro?**

Sí □ No □

Ranking de las páginas web más visitadas en la República Dominicana a modo general como local (2014)

Most visited Websites in DR

Top 10 General

Position	Website
1	Google.com.do
2	Facebook.com
3	Google.com
4	Youtube.com
5	Live.com
6	Yahoo.com
7	Blogspot.com
8	Twitter.com
9	Amazon.com
10	ListinDiario.com

Top 10 Local

Position	Website
10	ListinDiario.com
14	DiarioLibre.com
15	Bpd.com.do
17	ElCaribe.com.do
19	Remolacha.net
25	Gob.do
32	eMarket.com.do
35	Hoy.com.do
36	Eldia.com.do
37	Noticiassin.com

Amazon and Listin Diario reached the Top 10 General sites.

Source: Alexa.com – June 2014

Cantidad de Casos Sometidos de Fraudes Electrónicos tarjetas de crédito y phishing
2014

POLICIA NACIONAL

DIRECCION CENTRAL DE INVESTIGACIONES CRIMINALES

DEPARTAMENTO DE INVESTIGACION DE CRIMENES Y DELITOS DE ALTA TECNOLOGIA

SECCIÓN DE FRAUDES ELECTRÓNICOS

CLONACION TARJETAS DE CREDITO

AÑO		DENUNCIAS	RESUELTOS
2007		0	0
2008		0	0
2009		6	22
2010		4	3
2011		1	3
2012		91	276
2013		175	359
2014		22	34
Total	∑	299	697

PHISHING

AÑO		DENUNCIAS	RESUELTOS
2007		0	0
2008		97	192
2009		364	96
2010		195	195
2011		110	114
2012		94	95
2013		29	43
2014		17	41
Total	∑	906	776

SOMETIDOS

AÑO		NACIONALES	EXTRANJEROS
2007		0	0
2008		0	0
2009		4	0
2010		0	0
2011		1	1
2012		131	5
2013		143	10
2014		33	1
Total	∑	312	17

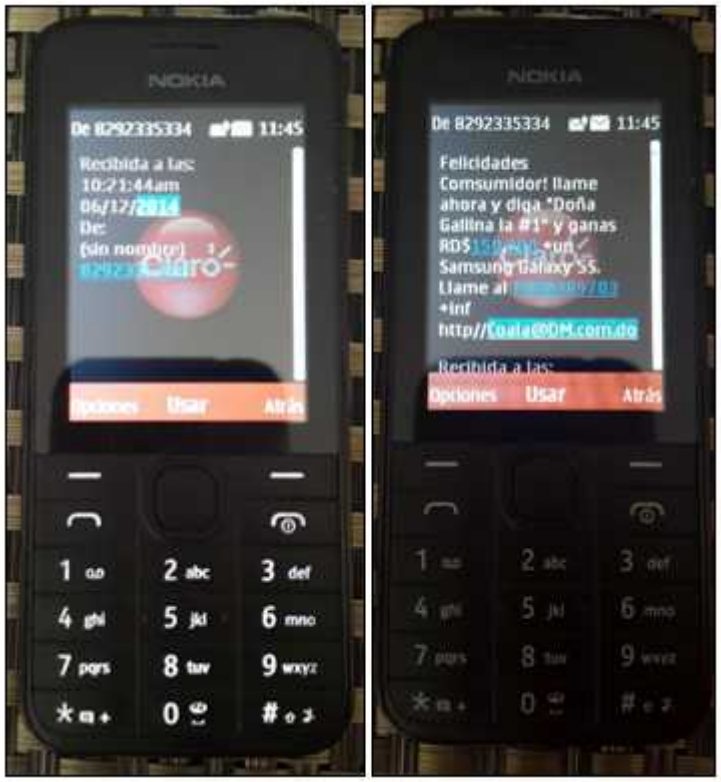
SOMETIDOS

AÑO		NACIONALES	EXTRANJEROS
2007		0	0
2008		28	1
2009		54	0
2010		305	1
2011		147	0
2012		132	0
2013		31	0
2014		37	0
Total	∑	734	2

Ejemplo empírico de intento de fraude a usuario de móvil

En diciembre 2014 un usuario recibe el siguiente mensaje, felicidades consumidor llame ahora y diga Doña Gallina la #1 y ganaras RD$150,000.00 y un Samsung Galaxy 5s, etc. El usuario se percató de los siguientes errores de la comunicación:

No es consumidor de Doña Gallina, solicitaban llamar a un teléfono celular, el dominio virtual que presentaba el mensaje no era correcto, no existen 5s de Samsung sino S5 y por ultimo al usuario confirmar llamando, a conciencia con ciertas preguntas capciosas, los delincuentes se declararon ladrones y cerraron.



Ejemplo empírico de intento de fraude a usuario de móvil

Richie Diaz ▸ **Luis Manuel Aguilo**
19 de octubre de 2013 ·

hermano aguilo,alguien se esta asiendo pasar por y por tu concurso de doña gallina y tambien por por los empresarios de antena latina,para robar dinero y tarjetas de celulares,atu nombre,yo tambien soy de un canal de tv local,,me gustaria darte todos los detalles por favor llamame al 829 717 0619,,yo tengo asta el numero del cual ellos yaman para haser la estafas diciendo k eres tu junto a orange y antena latina

Me gusta · Comentar · Compartir

A 10 personas les gusta esto. Lo más relevante

Escribe un comentario...

Betty Segura Yo tambien acabo de recibir un mensaje y me imagino es una falsa, el telefono que publican es 829 712 6050 y cicen llamar 829 661 4392 OJO CON ESO
Me gusta · Responder · 29 de octubre de 2013 a la(s) 10:48

Richie Diaz enviame tu denuncia al programa la tarde con richie de lunes a viernes
Me gusta · 29 de octubre de 2013 a la(s) 19:30

Luis Manuel Aguilo Hola! Eso es una estafa, deben hacer su denuncia al 809-682-2151.
Me gusta · 31 de octubre de 2013 a la(s) 10:00

Escribir una respuesta...

Luis Manuel Aguilo Hola! Eso es una estafa, por favor hagan su denuncia al 809-682-2151. Gracias
Me gusta · Responder · 4 · 5 de noviembre de 2013 a la(s) 9:43

Luis Manuel Aguilo Es una estafa.
Lo hacen para recargar celulares, esperaremos que con el control de los celulares "Macs" esto termine
Me gusta · Responder · 1 · 20 de junio de 2014 a la(s) 22:44

Edermina Serrano Croussett a mi me llamaron de los numeros 809-666-1726 y 809-749-3774, conmigo no le fue nada bien, son unos estafadores, sin principios.
Me gusta · Responder · 1 · 30 de enero de 2014 a la(s) 15:06

Ejemplo empírico crimen organizado utilizando Bypass y afectando empresas de telecomunicaciones en República Dominicana. 2014.

Apresan mujer que estafaba con llamadas telefónicas

12/11/2014 11:37 AM REDACCIÓN

Junto a otras dos, que están prófugas, formaba parte de una banda

Mujer apresada. (Fuente Externa)

COMPARTIR ESTA NOTICIA

Compartir por e-mail

Imprimir este artículo.

226 Me gusta | 55 Tweet | 0 Comentar

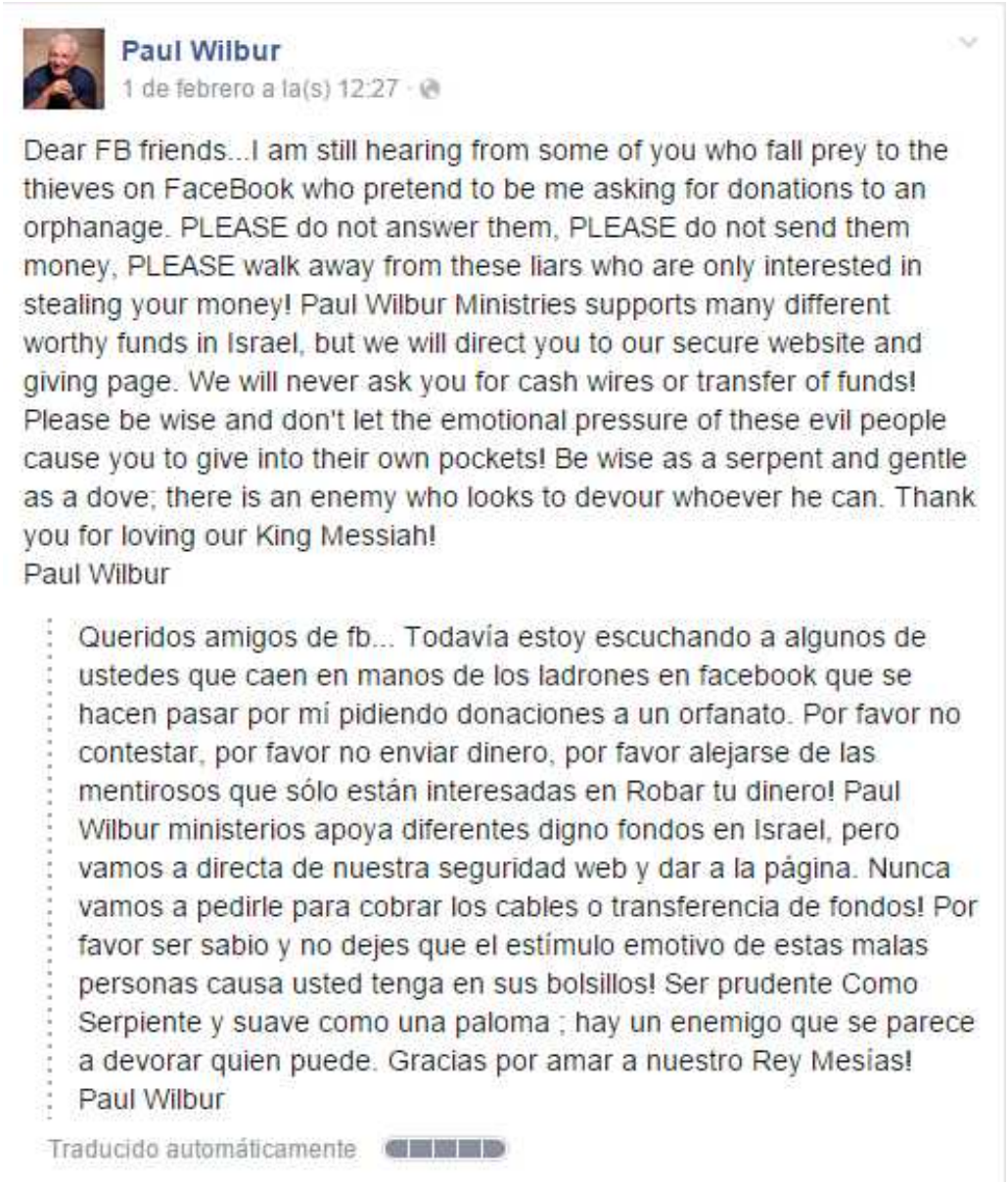
Santiago.- La Policía apresó a una mujer que integraba una banda de estafadoras integrada por otras dos damas, que lograron estafar a varias personas mediante llamadas telefónicas.

La apresada es Wendy Rivera Sánchez, mientras continúan prófugas Yajaira Lebrón Valdez, y Ana Miguelina Basilio, supuestas autoras de robo de dinero mediante estafa y asociación de malhechores, en perjuicio de Mireya García Polanco.

Un informe policial establece que mediante llamadas telefónicas del número 809-765-2721, García Polanco depositó distintas cantidades de dinero a la cuenta 785069352, a nombre de la detenida.

Luego a la cuenta 788013746 de una entidad bancaria por tres ocasiones, depositaron la suma de 57 mil 142.86 pesos y 474 mil pesos con la falsa promesa de que se había ganado un premio de un millón en Doña Gallina y un celular Galaxy S4.

Denuncia de usuario de Facebook por usurpación de identidad a través de phishing 2014



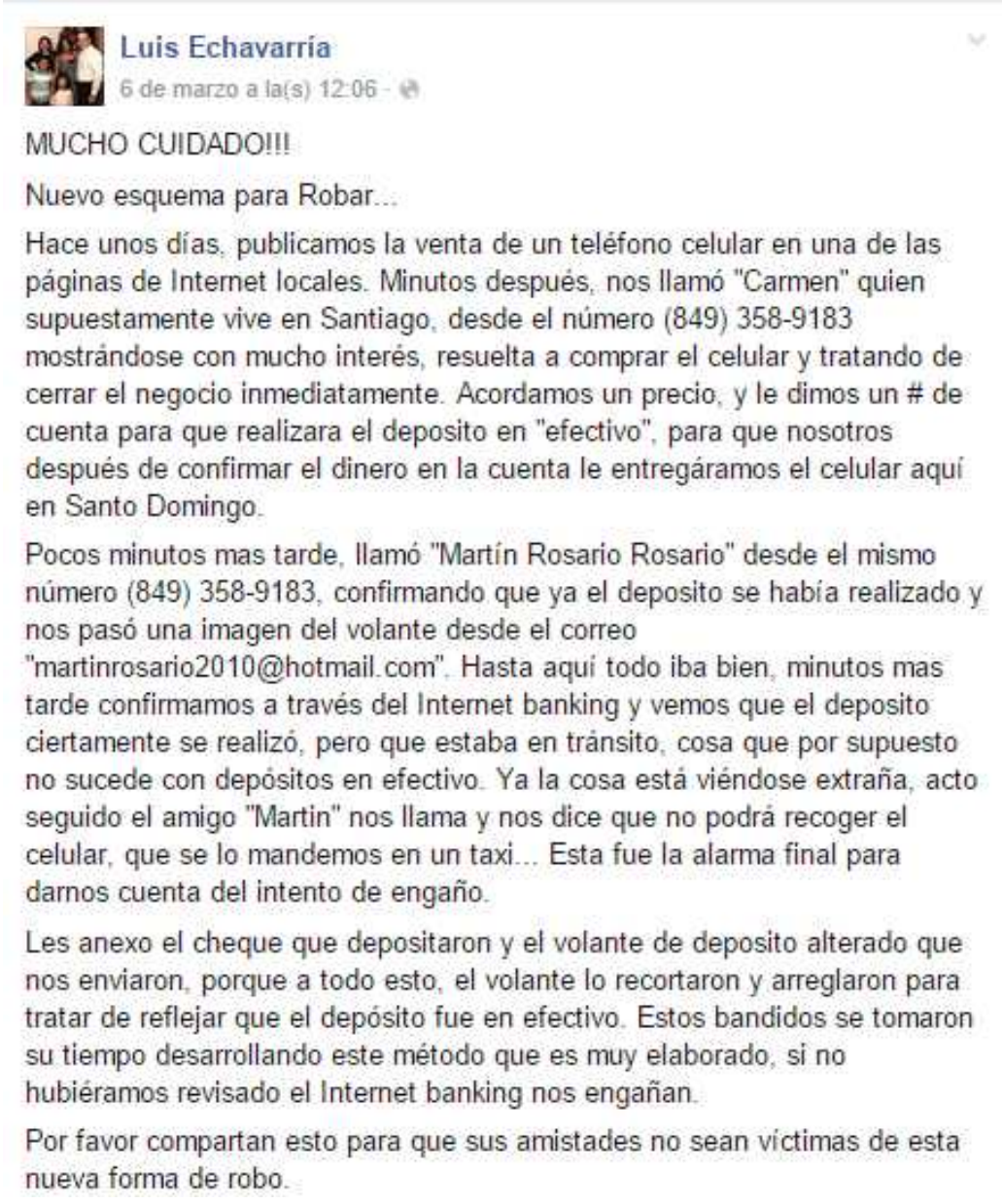
Paul Wilbur
1 de febrero a la(s) 12:27 ·

Dear FB friends...I am still hearing from some of you who fall prey to the thieves on FaceBook who pretend to be me asking for donations to an orphanage. PLEASE do not answer them, PLEASE do not send them money, PLEASE walk away from these liars who are only interested in stealing your money! Paul Wilbur Ministries supports many different worthy funds in Israel, but we will direct you to our secure website and giving page. We will never ask you for cash wires or transfer of funds! Please be wise and don't let the emotional pressure of these evil people cause you to give into their own pockets! Be wise as a serpent and gentle as a dove; there is an enemy who looks to devour whoever he can. Thank you for loving our King Messiah!
Paul Wilbur

> Queridos amigos de fb... Todavía estoy escuchando a algunos de ustedes que caen en manos de los ladrones en facebook que se hacen pasar por mí pidiendo donaciones a un orfanato. Por favor no contestar, por favor no enviar dinero, por favor alejarse de las mentirosos que sólo están interesadas en Robar tu dinero! Paul Wilbur ministerios apoya diferentes digno fondos en Israel, pero vamos a directa de nuestra seguridad web y dar a la página. Nunca vamos a pedirle para cobrar los cables o transferencia de fondos! Por favor ser sabio y no dejes que el estímulo emotivo de estas malas personas causa usted tenga en sus bolsillos! Ser prudente Como Serpiente y suave como una paloma ; hay un enemigo que se parece a devorar quien puede. Gracias por amar a nuestro Rey Mesías!
> Paul Wilbur

Traducido automáticamente

Usuario informa a través de las redes sociales, intento de fraude vía telefonía móvil (2015), donde después de hacer una supuesta venta el delincuente le promete enviar el comprobante de depósito el cual fue alterado.



Luis Echavarría
6 de marzo a la(s) 12:06 -

MUCHO CUIDADO!!!

Nuevo esquema para Robar...

Hace unos días, publicamos la venta de un teléfono celular en una de las páginas de Internet locales. Minutos después, nos llamó "Carmen" quien supuestamente vive en Santiago, desde el número (849) 358-9183 mostrándose con mucho interés, resuelta a comprar el celular y tratando de cerrar el negocio inmediatamente. Acordamos un precio, y le dimos un # de cuenta para que realizara el deposito en "efectivo", para que nosotros después de confirmar el dinero en la cuenta le entregáramos el celular aquí en Santo Domingo.

Pocos minutos mas tarde, llamó "Martín Rosario Rosario" desde el mismo número (849) 358-9183, confirmando que ya el deposito se había realizado y nos pasó una imagen del volante desde el correo "martinrosario2010@hotmail.com". Hasta aquí todo iba bien, minutos mas tarde confirmamos a través del Internet banking y vemos que el deposito ciertamente se realizó, pero que estaba en tránsito, cosa que por supuesto no sucede con depósitos en efectivo. Ya la cosa está viéndose extraña, acto seguido el amigo "Martin" nos llama y nos dice que no podrá recoger el celular, que se lo mandemos en un taxi... Esta fue la alarma final para darnos cuenta del intento de engaño.

Les anexo el cheque que depositaron y el volante de deposito alterado que nos enviaron, porque a todo esto, el volante lo recortaron y arreglaron para tratar de reflejar que el depósito fue en efectivo. Estos bandidos se tomaron su tiempo desarrollando este método que es muy elaborado, si no hubiéramos revisado el Internet banking nos engañan.

Por favor compartan esto para que sus amistades no sean víctimas de esta nueva forma de robo.

JOSE DENCIL MERA JIMENEZ
DO17SCRZ00000011041010001805

No. 0485

DIA MES AÑO
24 02 2015

25 FEB 2015

Pagaron contra este cheque a la orden de: Rosa Acosta

RD$ 17,000.00

diesisiete mil

BANCO SANTA CRUZ

Concepto: inicial

21428122735⑆04010001805⑈048517

Banco BHD León

RNC 1-01-13679-2

DEPOSITOS CUENTA CORRIENTE

103 AGENCIA

CAJERO	FECHA	HORA	NO. LOTE
3758	24/02/2015	17:00:33	3457488

CUENTA RD$: [redacted]
NOMBRE: [redacted]

TOTAL DE EFECTIVO: 17,000.00
TOTAL DE CHEQUES : 0.00
TOTAL DEPOSITADO : 17,000.00

REFERENCIA :
DESCRIPCION:

⑆555501000⑆

Aviso de extorsión a través de redes sociales. 2015.

Intento de fraude a través de phishing, encontraremos el ejemplo real una comunicación falsa y más adelante el siguiente paso de la pesca de información.

Enviado por: **SERVICIO TECNICO.**

Asunto: **Error: BCE001547-56**

Su cuenta muestra segun nuestro sistema un mensaje de error: **Error: BCE001547-56**, mismo que se define como: **CUENTA TEMPORALMENTE SUSPENDIDA.** El error se ha generado porque usted no ha realizado el proceso de - **Verificacion de Identidad** - en su cuenta, lo cual es necesario para seguir usando el servicio de Banca por Internet.

Es necesario que ingrese a nuestra web para poder verificar su información en nuestra base de datos o de lo contrario su servicio de banca por internet quedará bloqueada y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.

Para iniciar el proceso de verificacion de identidad de su cuenta a ingrese haciendo clic en el enlace siguiente o haciendo clic AQUI:

https://www2.bhd.com.do/SolBancasaLogin/newLogin/cuensuspen487=id37?

Con esta aplicacion se llavaran a cabo de manera automatica:

- Actualizacion de su información para nuestras Base de Datos

Segtec.net

- Encriptación en 128 bits que es requierida para Bancas@.

- Mensaje de alerta en escritorio en cada inicio de sesion a banca en línea.

- Mensaje de alerta en escritorio de cada transaccion en banca en línea.

Esto le tomará unos minutos y nos permitirá mejorar sustancialmente la seguridad y calidad de nuestro servicio.

Derechos Reservados 2012, Banco BHD S.A., Institución de Banca Múltiple, Grupo Financiero BHD.

Ojo Dirección Falsa!

Skimmer: Instrumento utilizado para fines de clonación magnética en tarjetas de crédito y en cajeros electrónicos. Nota: este dispositivo no fue creado con ese fin.

Hackeo a la empresa Sony Pictures y chantaje (2014). Al momento según los medios se cree que Corea del Norte es el responsable de este ciberataque aunque aun no se tienen las pruebas suficientes, ya que los activistas amenazaron del hecho si Sony Pictures publicaba la pelicula The Interview en todos los cines la cual afecta al maximo lider gubernamental de dicho pais, evidentemente, Sony no hiso caso y grandes perdidas se produjeron al materializar las amezanas por el abuso de la informacion. El FBI expone que este acto puede ocurrirle a cualquier empresa. Esta pelicula fue considerada como un acto de terrorismo e insulta para la afectada nación del oriente.

Avast antivirus, informa que en sus usuarios que tan solo en la penultima semana de Abril 2015, mas de 11.5 MM de ataques hackers fueron detenidos en todo el mundo. Es bueno tomar en conisderación, que esto es tan solo una muestra ya que solo se refiere a los usuarios de esta marca de seguridad cibernetica.

Avast antivirus, informa que en sus usuarios que tan solo en la penúltima semana de Abril 2015, más de 11.5 MM de ataques hackers fueron detenidos en todo el mundo.

Marco Conceptual.[45]

Bancos: Empresa comercial que realiza operaciones financieras con el dinero procedente de los accionistas y los clientes.

Fraude: Acto realizado para eludir una disposición legal en perjuicio del estado o de tercero o para burlar los derechos de una persona o una colectividad.

Fraudes Cibernéticos Bancarios: Utiliza medios electrónicos para hacerse de datos o el control de datos confidenciales que permiten cometer el ilícito y estafar a alguien, por medio de la intercepción de datos, como la obtención de contraseñas, cuentas de tarjetas de crédito o datos confidenciales sobre la identidad de una persona.

Falsificación: Es un acto consistente en la creación o modificación de ciertos documentos, efectos, productos (bienes o servicios), con el fin de hacerlos parecer como verdaderos, o para alterar o simular la verdad.

Phishing: Es el término informático que se traduce como "pesca" y denomina un tipo de delito encuadrado dentro del ámbito de los fraudes, el cual, se comete mediante el uso de herramientas informáticas que permiten adquirir información confidencial de forma fraudulenta (como puede ser la contraseña o información confidencial sobre cuentas bancarias).

Spammers o emisores de spam: Son los responsables de enviar los correos electrónicos de phishing a tantas direcciones de correo electrónico como sea posible.

Software: Son las instrucciones que el ordenador necesita para funcionar, no existen físicamente, o lo que es igual, no se pueden ver ni tocar.

Malware: Son programas maliciosos (en inglés Malicious Software) o códigos informáticos que pueden destruir nuestro sistema de información.

---

[45] García. t. (2010) diccionario el pequeño larousse ilustrado. méxico. larousse sa.
gits informatica. (2014) [en línea] ciber seguridad informática y delitos telemáticos. disponible en: http://www.gitsinformatica.com/vishing.html

Ciberdelito: es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo robar, destruir y dañar a través de los ordenadores, medios electrónicos y redes de Internet.

Internet: es una red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominado.

Seguridad: herramienta o estrategia que produce la capacidad de confianza en el sistema.

Contingencia: segunda alternativa de seguridad que garantiza el cuidado de la información a pesar de cualquier catástrofe delictiva.

Usuario: ente independiente que registra las ordenes y transacciones en el sistema de información.

Sistemas: es el universo de funciones y operaciones que comprende la informática en un lugar determinado.

Spear phishing: variante del phishing, es un tipo de delito utilizado por los estafadores cibernéticos cuyo objetivo específico son los clientes de empresas. Basado en las técnicas de ingeniería social, este método es utilizado para obtener información confidencial, mediante ataques por correo electrónico muy personalizados.

Vishing, mediante un correo electrónico o llamada, se solicita a la víctima que llame a un número de teléfono con el objetivo de actualizar sus datos o resolver algún supuesto inconveniente. Si la victima concreta el llamado, accede a una grabación de atención al cliente, que parece absolutamente normal, y a través de la misma se le solicitan sus datos personales.

Smishing: Sigue básicamente los mismos patrones del vishing. La diferencia es que, en este caso, el contacto es a través de un SMS.

DNS Spoofing: Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa.

ARP Spoofing: El ataque denominado ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo.

Web Spoofing: Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL.

XSS, del inglés Cross-site scripting: es un tipo de inseguridad informática o agujero de seguridad típico de las aplicaciones Web, que permite a una tercera parte inyectar en páginas web vistas por el usuario código JavaScript o en otro lenguaje script similar (ej: VBScript), evitando medidas de control como la Política del mismo origen. Este tipo de vulnerabilidad se conoce en español con el nombre de Secuencias de comandos en sitios cruzados.

URLZone: Es un bot (troyano) bancario que es implantado en las PC's comprometidas por LuckySploit o por otro Crimeware.

Skimmer: es un dispositivo del corpulencia de un "beeper", y permite duplicar los datos con sólo deslizar la tarjeta.

Cracker: Persona que posee basto conocimientos informáticos que desprotege, roba programas, efectúa daños delictivos ya sea en sistemas o redes.

Hacker: es la persona capaz de infiltrarse en un sistema o red ajeno para conocer la información sin tocarla ni abusarla.

Carder: individuo utiliza las tarjetas de crédito de sus víctimas para realizar pagos a sistemas de compra a distancia (principalmente).