FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

COMO ESTAMOS EXPUESTOS AL FRAUDE ELECTRÓNICO Y COMO PODRÍAMOS SOLUCIONARLOS

SUSTENTADO POR:

CARLOS ARTURO MEZA ANDINO

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, F.M. **HONDURAS, C.A.**

ENERO 2017

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

LUIS ORLANDO ZELAYA MEDRANO

SECRETARIO GENERAL
ROGER MARTÍNEZ MIRALDA

VICERRECTOR ACADÉMICO
MARLON BREVÉ REYES

DECANO DE LA FACULTAD DE POSTGRADO

JOSÉ ARNOLDO SERMEÑO LIMA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

CARLOS ROBERTO ARIAS

MIEMBROS DE LA TERNA O COMISIÓN EVALUADORA:

Ing. Oscar Zocon Alba

Ing. Rodolfo Z. Velazquez

Ing. Pablo Moya

FACULTAD DE POSTGRADO

COMO ESTAMOS EXPUESTOS AL FRAUDE ELECTRÓNICO Y COMO PODRÍAMOS SOLUCIONARLO.

AUTOR

CARLOS ARTURO MEZA ANDINO

RESUMEN

En el siguiente estudio se hizo una investigación desde diferentes puntos de vista del fraude electrónico y las herramientas más comunes que se utilizan para llevarlo a cabo, esto frente a la problemática que afecta a todas las personas que poseen una tarjeta de crédito y como los entes financieros que las proveen lidian con esta temática además de proponer qué soluciones se pueden concluir y que soluciones se están implementando actualmente. El método es una investigación sistemática de todos los ambientes relacionados con el fraude electrónico y encuestas a personas expertas y no expertas en el tema de estafa y clonación de tarjetas, también se incluye las experiencias del autor que durante la investigación tomo la filosofía que la mejor forma de prevenir y

combatir el fraude electrónico es conociendo de primera mano las principales herramientas y métodos para realizarlo y por ende experimenta diferentes métodos con el objetivo de conocer cómo actúan los hackers en Internet y mediante ingeniería social para lograr entender y proponer las soluciones y resultados precisos.

Palabras clave: clonación de tarjeta, fraude electrónico, gusano informático, hacker, ingeniería social.

GRADUATE SCHOOL

HOW WE ARE EXPOSED TO ONLINE FRAUD AND HOW WE CAN SOLVE THAT

AUTHORS:

CARLOS ARTURO MEZA ANDINO

ABSTRACT

In the following research an investigation is shown from different points of view on electronic frauds and tools that are most commonly used for them, these because of the problems that affects people who possess a credit card and how financial organizations that provides the credit cards takes care of this problems, in addition to propose what kind of solutions are viable and what solutions are actually being implemented. The method used for this research is a systematic investigation of all the environments related to electronic frauds and surveys done to experts and no experts in the subject of fraud and card cloning, it also includes the author's experience during the investigation taking into consideration the philosophy that the best way to prevent and fight electronic frauds is knowing the main tools and methods used for it, therefore experimenting different methods with the objective of knowing how hackers act in the

Internet to understand and propose solutions as well as accurate results through social engineering.

Clear words: card cloning, computer worm, electronic fraud, hackers, social engineering.

TABLA DE CONTENIDO

TABLA DE FIGURAS

Código de campo cambiado

Código de campo cambiado

Código de campo cambiado

Código de campo cambiado

Código de campo cambiado

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 Introducción:

Este trabajo final se hace con la motivación de proponer algunas posibles soluciones de seguridad informática que sufren las empresas y los usuarios de tarjetas de crédito. En este trabajo se hace enfoque no solo en las empresas financieras y bancos sino además en los tarjeta habientes y usuarios de las empresas con información sensible además en las diferentes situaciones que experimentan en el proceso de ser víctima de una estafa electrónica hasta obtener una respuesta satisfactoria o no, se evalúa y analizan diferentes tipos de métodos de estafa como aplicaciones, ingeniería social, páginas web, correos electrónicos, skimmers (aparato pequeño que se utiliza para clonar tarjetas de crédito) etc.

El siguiente estudio es una recopilación de diferentes textos de expertos, revistas científicas, encuestas, experiencias y experimentación del autor con el objetivo de recaudar la información más reciente con la finalidad de que las soluciones que se pueden llegar a plantear resulten en verdaderos obstáculos para estas prácticas que poco a poco se han convertido en las amenazas de casi cualquier persona con tarjetas de crédito y empresas en el mundo actual.

Por tanto en el siguiente estudio se define qué importancia están dando los usuarios a su información sensible, qué medidas están tomando las instituciones, métodos actuales de recolección de información ilegal y que se hace con esta información, como se trafica en los medios de Internet y como son utilizados.

Este trabajo está estructurado en cinco capítulos donde cada uno se resume de la siguiente manera:

Capítulo uno plantea cual es el problema a tratar desde diferentes puntos de vista y se introduce diferentes herramientas y métodos que se utilizan como parte del problema y un breve resumen de cómo se recolecto esta información. Además se definen los objetivos generales y específicos del trabajo de investigación.

Capítulo dos se plantea toda la información recolectada por medio de investigaciones científicas y estudio profundo de los principales subtemas, se definen los términos importantes que sirven como definición para toda la investigación, además de explicar cada una de las herramientas a profundidad su uso y medios más comunes para la implementación siendo a tratar solo las herramientas que se están utilizando actualmente.

Capitulo tres, se explica la metodología utilizada durante esta investigación, cómo se obtuvo la información, las fuentes y los procesos que se debieron hacer para llegar a la información más actual sobre el tema de investigación. Se define las preguntas clave que se van a utilizar en las entrevistas y los objetivos de las mismas.

En el capítulo cuatro se hacen los análisis de los resultados de las encuestas y de la recolección de información aplicada a 72 personas que representan a los usuarios comunes que poseen una tarjeta de crédito mientras en contraste se entrevistaron 22 personas que son expertas en el tema a tratar o trabajan en entes financieros que tienen información importante para poder llegar a hacer las conclusiones, además en el capítulo cuatro se muestran los resultados de la investigación y experimentación de diferentes herramientas para hacer fraude electrónico y conocer cómo está expuesta esta información al usuario común en otras palabras qué tan fácil es para un usuario común y corriente llegar a esta información y si necesita conocimientos de informática para poder trabajar con el conocimiento que pueda obtener.

En el capítulo cinco finalmente se plantean las conclusiones que se lograron obtener de la investigación y las posibles soluciones que los usuarios y entes financieros pueden aplicar para combatir el fraude electrónico y las estafas mediante ingeniería social.

1.2 Problema:

Actualmente vivimos en un mundo controlado en gran parte por la tecnología, un mundo globalizado donde la información está al alcance de todas las personas esto con lleva muchas ventajas y desventajas de tener la tecnología que se comunica entre

sí y la información a nuestro alcance todo el tiempo. Hoy en día la privacidad se convierte en un lujo que las personas poco a poco van perdiendo. Esto conlleva que las empresas que tienen usuarios y servicios con información que no se puede compartir se enfrenten a un mundo que constantemente está compartiendo información de manera masiva y les obliga a estar un paso adelante siempre ante los diferentes métodos de estafa que utilizan los ladrones informáticos y la falta de información de sus propios usuarios.

1.3 Objetivos

1.3.1 Objetivo General

- Investigar y entender por medio de estudios, pruebas y encuestas la facilidad con la que se dan los diferentes tipos de crímenes y fraudes informáticos para proponer soluciones a esta como una oportunidad de negocio.

1.3.2 Objetivos específicos

- Realizar un estudio de cómo manejar mejor las tarjetas de crédito para evitar ser estafados.
- Dar posibles soluciones que ayuden a aumentar la seguridad del tarjeta habiente y sus datos sensibles.
- Definir si los tarjeta habientes en Honduras están realmente protegidos con leyes contra estafas.
- Conocer y entender los métodos de estafa y fraude electrónico que afectan a los países latinoamericanos.

CAPÍTULO II. MARCO TEÓRICO

2.1 Diccionario de términos

- Skimmer: aparato diminuto utilizado por cibercriminales que copia la información que contiene la banda magnética de una tarjeta de crédito y suelen estar en las boquillas de los cajeros automáticos.

- Bug: es un error del sistema ya sea en software o hardware que hace que este funcione incorrectamente o un error que puede dejar huecos de seguridad.

- Carding o cardeo: es el acto de clonar tarjetas de crédito o robar información de las mismas acto seguido utilizar estos datos ilegalmente para hacer compras.

- Bitcoin**:** es una tecnología basada en criptomoneda virtual o intangible que no está regulada por ningún ente bancario, no existe en ningún lugar y no es de nadie además puede ser generado por cualquiera que esté en capacidad de hacerlo.

- Hacking/ hacker: Es una persona que se caracteriza por ser curiosa y penetra los sistemas informáticos para probar sus habilidades como simple reto**.**

- Cracking/Cracker: Es un derivado del hacker pero con el objetivo de realizar transacciones ilícitas, robar información o impedir el correcto funcionamiento de redes o sistemas informáticos.

- Warez: Grupo de hackers donde su meta es hacer cracking, obtener y compartir datos que usualmente son delitos contra la propiedad intelectual o derechos de autor

- Ciber delincuencia: grupo de hackers que su objetivo es planear y cometer delitos con objetivo de expresar ideas xenofóbicas, racistas o discriminatorias de alguna manera.

- Software: Son programas informáticos que hacen posible el manejo de recursos, datos almacenados y tareas específicas dentro de un computador.

- Parches: Es un programa que se utiliza en el software para modificarlo con el objetivo de actualizar la aplicación para darle nuevas funciones o corregir errores.

- Ingeniería social: Es una práctica para obtener información, accesos privilegiados y datos confidenciales mediante el eslabón más débil que son los usuarios además se aprovechan de estas personas para que les brinden información que les ayude a penetrar sistemas informáticos y obtener datos sensibles.

- Robo de identidad: se utilizan datos personales para hacerse pasar por otra persona para cometer delitos informáticos u obtener beneficios económicos.

- Deep web: Internet profunda es aquella información sitios web donde su principal característica es que no están indexadas a los buscadores tradicionales como google.

(Angelucho, 2013; s. f.; Mitnick & Simon, 2007; «Parche (informática)», 2016).

2.2 Seguridad Informática:

El incremento vertiginoso de las operaciones a través del correo electrónico y del uso de los servicios bancarios a través de Internet han facilitado el acceso al usuario informático de numerosos bienes y servicios que de otra manera resultaría más complicado de contratar, pero inevitablemente, ha propiciado la aparición de nuevas formas de delincuencia y defraudación.

La inseguridad electrónica está presente en todo nuestro entorno social incluyendo las redes sociales, medios de comunicación y el Internet, de tal manera que las empresas como ser bancos, universidades y organizaciones buscan la manera de obtener la mayor protección y seguridad al momento de manejar diversos protocolos y en gran diversidad datos y archivos buscando obtener una gran protección y previniendo accesos no autorizados, ataques cibernéticos robo de información o alteración de los mismos datos, todo esto asegurándose de que la información es accesible a las personas autorizadas, la implementación de normas de seguridad deben ser prioridad en una empresa ya que de esta forma se protege la integridad de los datos, se evita y se previene el robo de información y se protege la divulgación no autorizada.

> Los agujeros de seguridad se han multiplicado con la llegada de dispositivos nuevos como los drones o con la robótica. Un estudio de Allianz Global Corporate & Specialty cuantifica en cuatrocientos mil millones de dólares al año es el gasto mundial causado por la ciberdelincuencia en la economía mundial. La vulnerabilidad corporativa se ha multiplicado también como consecuencia del uso intensivo del big data en las grandes empresas. Esta tecnología permite explotar el conocimiento de los clientes a través del tratamiento de millones de datos. (LÁNDER, 2016, p. 1).

Hoy en día se generan cada vez más expertos en seguridad informática y las universidades se ven en la disposición de tener carreras y maestrías en temas de seguridad de la información sin embargo el usuario común puede ver la seguridad informática como una serie de barreras que le impiden realizar muchas cosas que él piensa que no impiden el correcto funcionamiento de la empresa y que considera correctas es por esto que se debe concientizar sobre la seguridad informática para que deje de ser un tema aparte sobre todo en muchas empresas donde la prioridad es invertir en mercadeo y ventas.

> Un estudio conjunto de HP y del Instituto Ponemon señala que una empresa tarda aproximadamente 46 días de promedio en tapar un agujero de seguridad provocado por un delito de esta índole. En 2014, Sony Pictures perdió 100 millones de dólares por un ataque informático que incluyó la fuga de información de películas sin estrenar, guiones inéditos y datos privados de actores y empleados. Fue el mayor incidente sufrido hasta entonces por una empresa americana. Paralizó los sistemas informáticos de la compañía y provocó grandes filtraciones de datos, de registros financieros y de correos electrónicos privados de ejecutivos de Hollywood. (LÁNDER, 2016, p. 2).

2.3 Herramientas para explotar fallas de seguridad informática.

En el artículo de revista científica llamado fraude online, (Garay, 2008) nos explica algunos conceptos básicos de herramientas y fallas de seguridad.

- Malware: Es un software que ha sido creado para dañar un ordenador o infiltrarse en un sistema sin previo conocimiento del dueño con el objetivo de cometer fraude y realizar tareas maliciosas a través de Internet, cabe destacar que muchos de los fraudes en Internet se relacionan con el malware y todos los derivados del mismo.

- Gusanos informáticos: es un programa que se puede llegar a reproducir o copiar a sí mismo, además puede viajar por las redes informáticas y no necesita ninguna otra difusión y tienen instrucciones de recaudar datos de la víctima.

- Spyware: Es un tipo de malware donde su característica principal es que permiten a un tercero tener acceso a el ordenador incluso a la red de cualquier empresa o entidad pública o privada, estos spyware están clasificados en gusanos y troyanos.

- Troyano: Es un derivado del spyware, es un gusano muy difícil de detectar y consiste en un programa informático que se aloja dentro de los sistemas informáticos y permiten accesos de usuarios externos a través de Internet o de una red local. Los troyanos pueden recolectar información o llegar incluso a controlar remotamente la computadora pero a diferencia del virus este no provoca daños al sistema necesariamente.

- Exploit: Es un software que se aprovecha de las debilidades particulares de un sistema operativo estos se hacen no necesariamente para dañar sino también para probar que existe una brecha de seguridad en el sistema pero también son objetivos de los programas que suelen ser maliciosos.

- Hijacker: es un software que cambia la página de inicio del navegador para dirigirlo a otras páginas con contenido indeseable como ser pornografía o publicidad basura, el hijacker suele ir asociado con otro software que se llama keylogger y sirve para guardar datos confidenciales cuando accedamos a nuestras cuentas.

- Phishing: es la acción de obtener datos confidenciales a través de correos electrónicos o sitios web, para esto se utiliza malware diseñado con el fin de que los usuarios con cuentas bancarias contesten o entren a páginas por ejemplo sitios web que se ven exactamente igual a las de un banco en específico para que ingresen sus datos. En su mayoría el phishing es empleado por un hacker que envía un correo electrónico supuestamente con el nombre de una empresa respetable, la victima da click que lleva a una página web falsa que ha sido diseñada previamente por el estafador coloca sus datos y de esta manera el atacante obtiene información personal.

Existe un software, llamado exploit kit, con el propósito de hacer phishing. Se puede comprar o alquilar por un valor de 2 o más bitcoins, la moneda digital mejor cotizada en el

mercado ilegal de los hackers, ya que no es rastreable. Actualmente cada bitcoin tiene un valor aproximado a los US$ 450(Argentina, 2016).

El exploit kit es una herramienta que se utiliza para aprovechar una vulnerabilidad no conocida, estas provienen de países como Rusia donde la ley contra delitos informáticos y la ingeniería social juega un papel importante ya que entre más específico sea el kit más barato se vuelve comprarlo(Argentina, 2016).

2.4 Tipos de fraudes electrónicos.

Existen diferentes tipos de fraudes electrónicos en Internet donde actualmente se subasta y se vende prácticamente de todo en diferentes sitios y redes sociales y esto abre puertas para que la delincuencia asociada con este tipo de actividades siga en aumento. Lo común es que por parte del vendedor donde este cobre el producto y no lo envíe es la forma más fácil y básica de fraude sobre todo hoy en día donde es común las ventas online internacionales entre portales web donde es bien difícil al comprador perseguir al defraudador extranjero, siendo menos frecuente lo contrario donde el comprador reciba el producto pero que no lo pague además de que es costumbre en todo tipo de ventas online que el dinero se pague por adelantado antes de enviar el producto.

Carding: Otro tipo de fraude electrónico es al momento de hacer el pago efectuarlo con datos de una tarjeta de crédito robada, para evitar este tipo de fraude conviene utilizar los servicios de protección de pago que se ofrecen a los sitios web aunque la compra sea un poco más costosa, muestra que el sitio es seguro para comprar, más adelante en el texto se explica a detalle sobre este tipo de fraude y cómo se obtienen estos datos.

Ventas Bajo publicidad falsa: el Internet facilita mucho este tipo de fraude aunque se puede dar sin el uso del Internet ya que consiste en la venta de artículos con características mucho mejores o muy diferentes a las que realmente son. En casos como estos dependiendo de qué tan exageradas o diferentes son las características del producto original con el que se ve en la publicidad puede ser catalogado como delito o incluso estafa.

Cuentas escrow: también son conocidas como depósito de garantía se origina por algunas empresas que sirven de intermediario en las compras realizadas en Internet. Estas empresas reciben el dinero de la compraventa por medio de una transferencia del comprador y

lo debe transferir al vendedor una vez este entrega el producto al comprador donde este último confía en la empresa que ofrece la cuenta escrow para dicha transacción, sin embargo esta empresa solo es una tapadera del estafador y nunca entrega el dinero al vendedor y simplemente desaparece perdiendo el comprador su dinero sin obtener ningún producto a cambio.

Paquetería falsa: Otro tipo de fraude que se relaciona con este tipo de compra y venta de artículos por Internet son los servicios de paquetería donde el estafador se hace pasar por un servicio de mensajería que va a llevar al comprador el articulo hasta su casa pidiendo todos los datos de la víctima luego este recibe el producto pero nunca lo envía al comprador además de que el estafador pide por adelantado el pago por él envió. (Garay, 2008, p. 318,322).

Skimmer: Este aparato es comúnmente usado en gasolineras y hoteles para clonar la información contenida en las tarjetas de crédito el estafador generalmente paga a las personas que están en los hoteles o en las gasolineras cierta cantidad de dinero por cada tarjeta que este pase por el skimmer, este guarda la copia de la información contenida en la banda magnética de la tarjeta de crédito luego esta información se utiliza para consumar hechos delictivos o vendiendo esta información para que otros puedan hacer uso y comprar en línea o retirar dinero directamente de cuentas bancarias. Estos skimmers se pueden conseguir fácilmente en sitios de venta online como por ejemplo sitios de ventas en línea como eBay.

Figura 1 skimmer aparato que se usa para clonar tarjetas de crédito
Fuente: (e-crime, s. f.)

“El skimming, como se conoce en inglés es la manipulación de los cajeros electrónicos, fue un dolor de cabeza para los bancos latinoamericanos en la década de los 90, pero no llegó a EE.UU. hasta ahora”. («Fraude electrónico crece y cambia de cara tan rápido como la tecnología», 2015)

2.5 ¿Existe un sistema seguro?

La respuesta es sencilla y es no. Existen varias razones por lo cual un sistema de seguridad no puede ser completamente seguro:

- Los humanos cometemos fallos muchas veces no son intencionales
- Errores de los sistemas que no son detectados hasta que se violenta el mismo
- Reciclar software hace que se generen varios errores
- Desarrollar software malicioso es un negocio lucrativo y por eso el software es constantemente atacado.

Generalmente para reparar estas fallas se usan parches y para detectarlas es común que las empresas que pretenden ser las más seguras contraten hackers para probar si puede violar la seguridad de sistema, estas empresas suelen dar una recompensa al hacker o grupo de hackers que logren penetrar en la seguridad del sistema de la compañia, compañías alrededor del mundo usan este método algunas veces como alternativa a contratar empleados comunes para mejorar sus sistemas de seguridad un ejemplo de algunas empresas que han empleado este método en el pasado son Uber, Microsoft, Apple y el F.B.I. (Leonardo ballado, s. f.).

> La tecnológica estadounidense Apple pagará a los hackers (piratas informáticos) que detecten fallos y vulnerabilidades en su sistema operativo iOS y en el resto de sus productos. El objetivo de la compañía dirigida por Tim Cook es encontrar posibles agujeros negros que podrían ser utilizados, precisamente, para piratear el iPhone, el Macbook o cualquier otro dispositivo de Apple. (A. Fernández, 2016).

Los sistemas completamente seguros no pueden existir fácilmente ya que al crearse un sistema seguro también se crean las reglas del juego para el hacker o cracker y este puede utilizarlas a su favor para violar la seguridad, esta es la manera más común en que se hace trampa a los sistemas de seguridad primero se analizan las reglas de cómo funcionan y luego se utilizan a favor los huecos de seguridad que puedan tener, el atacante debe buscar las vulnerabilidades en las mismos sistemas, y lograr penetrar para tener acceso de súper usuario y lograr cambiar, destruir información o simplemente para ver los datos o extraerlos.

Si bien es cierto que es muy difícil que se dé un sistema completamente seguro pero es posible un sistema muy difícil de penetrar y la posibilidad de un ataque exitoso es más y más complicado para el atacante o atacantes y puede tomar años o incluso que aparezcan nuevas tecnologías para poder lograrlo, un claro ejemplo es la seguridad de la consola PS Vita de Sony donde todas las otras consolas luego de algunos años su seguridad han sido violada exitosamente, la PS Vita con más de 10 años en el mercado hasta hace un par de meses hay signos de hackers que han logrado craquearla para poder jugar juegos piratas. Según (Adrián Hernán, s. f.) Es todo gracias a sus tarjetas de memoria que cuentan con un formato único que solo permite utilizarse en un dispositivo que es lo contrario a su predecesor que contaba con las denominadas tarjetas SD y esto permitió el acceso a sus llaves de programación y abrió las puertas a la piratería de esta consola en un par de años de su salida, las nuevas tarjetas de la PS Vita dificulta mucho el acceso y la implementación de software de modificación.

Ayuda llevar un registro de las actividades que se realizan en el sistema ya que de esta manera se puede prevenir los ataques y tener un plan de contingencia rápido si se detecta un ataque en pocas horas se puede arreglar el problema mediante un parche.

> Las innovaciones que impulsan al sector hacia adelante y presentan a los consumidores métodos nuevos y emocionantes para comprar, también se expanden rápidamente más allá de los límites de nuestros existentes regímenes regulatorios y de protección al consumidor", dice la declaración escrita de James A. Reuter, quien se pronunció en nombre de la Asociación Estadounidense de Banqueros. "Y, como ha sido históricamente el caso, es frecuente que los delincuentes vayan un paso adelante, mientras el mercado busca consensos. (JAIVIA, 2014).

En Colombia existe una empresa multinacional llamada Easy solutions que se dedica a la detección y prevención de fraude electrónico, en una entrevista con el director ejecutivo de dicha compañía Ricardo Villadiego, hace énfasis que ningún ámbito conectado a la Internet esta salvo de la acción de los hackers.

Las cifras de Easy solutions aumentaron un 187% solo en el año 2014 con un crecimiento tan espectacular solo se compara con el de los delitos online, Ricardo Villadiego subraya que adoptar leyes contra la delincuencia electrónica no siempre es la solución "Legislar lleva tiempo y los ataques evolucionan más rápidamente que las regulaciones" afirmó («Fraude electrónico crece y cambia de cara tan rápido como la tecnología», 2015).

2.6 Amenaza humana

Básicamente de las principales amenazas que tiene las empresas en este caso bancos y empresas financieras son las amenazas humanas desde personas en altos cargos con conocimiento de información sensible, que pueden llegar a ser imprudentes en lo que dicen y en la información donde la suelen manejar, o el hacker que mediante ingeniería social o por medio de herramientas informáticas obtiene acceso a la información valiosa que es privada.

Una de las amenazas más comunes que enfrentan algunas empresas son los mismos empleados o ex empleados de la misma empresa ya que son ellos los que saben las fallas y debilidades de la empresa.

En algunos casos los actuales y ex empleados de una empresa pueden participar en delitos contra la misma empresa donde trabajaron porque ya conocen las formas en que esta funciona y saben dónde están los huecos de seguridad, estos pueden ser motivados por diferentes razones ejemplo venganza ya sea por un despido injusto, problemas dentro de la empresa con otros empleados o jefes o simplemente enriquecerse económicamente, por esto se debe tener tacto al momento de prescindir de un empleado dentro de una empresa de este rubro sobre todo si este tenía acceso a información sensible además es necesario cambiar la contraseñas de acceso a la información y procesos pero sobre todo las personas que desempeñan estos cargos, deben enfocarse a personas con una madurez y experiencia en materia de seguridad.

2.7 Personalidad del hacker

El hacker es una persona que está continuamente en busca de información para aprender, además de luchar siempre por la difusión libre de la información y la distribución de software libre.

Para el hacker todo es un reto y no hay límites por estas razones el concepto del hacker ha sido mal interpretado y es tratado como un tema tabú alrededor de varios mitos como ser que es un pirata informático lo que es falso ya que el pirata comercia con la información mientras que el hacker obtiene la información para uso personal o compartir gratis, otro mito que rodea al hacker es que es una persona que se dedica a entrar a los sistemas ajenos para robar y destruir la información pero no es el hacker quien destruye la información sino el cracker.

El verdadero hacker es curioso y paciente sino terminaría hartándose en los intentos de entrar a un sistema ya que requiere de bastantes pruebas con fallo y error.

La persona que se considera un hacker no entra a un sistema para destruir la información o venderla él solo quiere aprender entrar a sistemas donde pocas personas pueden estar esa es la finalidad del hacker tomar retos y superarlos.

El hacker disfruta de manera entusiasta explorar todos los rincones de los sistemas programables además de aprovechar todas sus capacidades.

En la actualidad han surgido grupos de hackers que comparten ideas y trabajan por una misma causa con el objetivo de aprovechar sus habilidades. Existen empresas que se conforman de hackers que surgieron de estos grupos, como por ejemplo la empresa italiana llamada “the hacker team” que son contratados por países y empresas para mejorar sus sistemas de comunicaciones o interceptar comunicaciones de los demás, también venden herramientas de vigilancia e intrusión a los gobiernos. A estos grupos y empresas se le llama que practican el hacktivismo y cada vez está tomando más relevancia en el mundo actual.

El hacker tiene su propia ética debe cuidar no convertirse en piratas informáticos su primera regla es que el acceso a la información es sin límites y gratis, otro de los preceptos de un hacker es que este es juzgado por su habilidad no por edad, sexo o religión. Un hacker debe obtener respeto de otros hackers destacándose mediante sus habilidades, un hacker no es uno solo porque él se autoproclama hacker, debe ser reconocido por los demás y para esto último llaman la atención entrando a sistemas muy difíciles y dejando su firma para que otros hackers los vean.

En este trabajo de investigación el objetivo a tratar es el cracker, piratas informáticos y el carder que se entrenan para vender la información o usarla para sus propios fines económicos además de estafar a la demás personas mediante ingeniería social o herramientas informáticas de robo de identidad o datos sensibles pero para fines de facilidad todos esos conceptos en este texto de investigación serán para el llamado hacker.

2.8 Deep web.

La Deep web o Internet profunda son los sitios de Internet que no están indexados y no se puede tener acceso mediante los buscadores tradicionales y tampoco mediante los navegadores comunes, la herramienta adecuada para acceder a la Internet profunda es “Tor”.

> La red Tor fue creada en 2003 por el laboratorio de investigación naval de los Estados Unidos, ahora el proyecto se encuentra en manos de Tor proyect una organización sin fines de lucro orientada a la investigación y la educación.(Argentina, 2015).

<LA NACIÓN- Argentina> en esta revista científica se afirma que el estimado del contenido de la web profunda es de 400 a 500 veces más grande que la web que todos conocemos ya que está lleno de documentos y bases de datos de las empresas temas técnicos y científicos foros y lugares de intercambio de información libres acerca de temas de todo tipo ver figura 2.(Argentina, 2015).

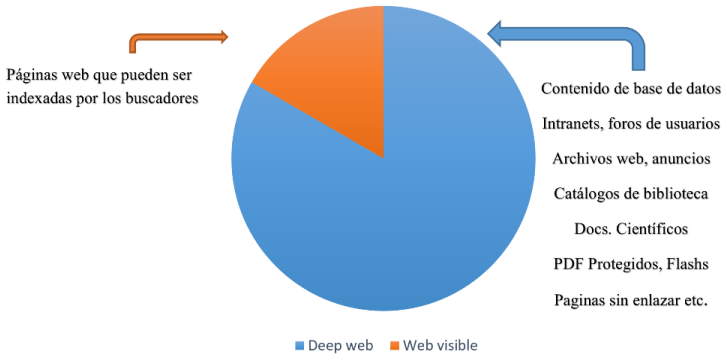

Figura 2 Representación gráfica del Internet que conocemos contra la web profunda.
Fuente:*(*Angelucho, *2013).*

El dinero que se maneja en la Deep web no es otro que el bitcoin que es una moneda que no se puede rastrear tampoco está físicamente en alguna parte y no es regulada por ningún banco y por esto mismo es la mejor opción para hacer ventas y compras ilegales y sobretodo en la Deep web.

El sitio Silk Road dedicado a la venta de drogas, armas y comercio ilícito en el año 2012 genero ingresos de 1.2 millones de dólares mensuales, dejando ganancias de al menos noventa y dos mil dólares en comisiones a los operadores de la página, según el informe "Travelin the silk road" («Deep Web», 2014).

2.9 Carder y carding

Además de los tipos de hackers que se reúnen para buscar información eventualmente surgió aquellos que se dedicaban a obtener números de tarjeta de crédito con intenciones de usar esta información de manera ilegal para lucrarse económicamente de esto nació el denominado carding.

El carding es el uso y generación ilegitimo de números y datos que se encuentran en las tarjetas de crédito para aprovecharse de los mismos y lucrarse económicamente de las mismas aunque pertenecen a otras personas que en ese momento no tienen idea de que fueron víctimas de estafa, esto último es tan fácil como poner en una página web los primeros 6 números de una tarjeta de crédito conocida, en el siguiente ejemplo esta página web genera a partir de patrones de los ya conocidos algoritmos que rigen las combinaciones de tarjetas de crédito, esto además de generar códigos tiene un comprobador de tarjetas de crédito para ver si funcionan o no los códigos que se generan a esto último se le llama checker y si la tarjeta funciona o no se le dice cc viva o cc muerta (ver figura 3).

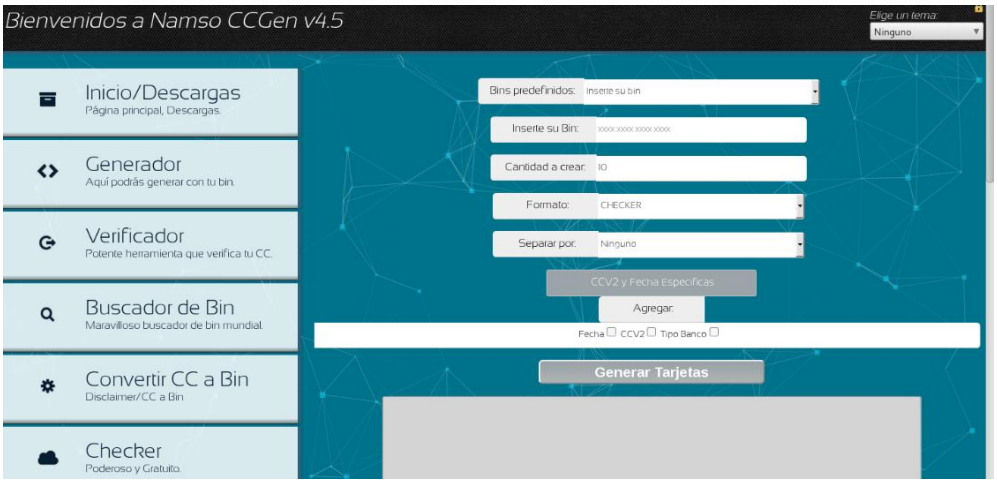

Figura 3 Página web de generador de tarjetas de crédito ilegitimas.
Fuente http://www.namsoccgen.com/

Por ultimo cabe mencionar que existen grupos de estas personas que se dedican a no solo cardear sino enseñar a otras personas de una manera relativamente fácil para recibir a cambio parte de lo que estos a su vez generan de manera ilegal, una parte considerable de estos carders son menores de edad y jóvenes que solo empezaron tratando de crackear servicios en línea de pago por ejemplo Netflix o Spotify.

> Para el 47 por ciento de los usuarios, el principal responsable de la seguridad de las transacciones electrónicas es el banco o el proveedor de tarjetas de crédito, indica un estudio hecho en Colombia entre usuarios de la banca de américa latina realizada por Easy Solutions. Además revela que "que el 95 por ciento de los clientes consultados conoce la amenaza de los virus informáticos, pero sólo el 36 por ciento sabe del phishing y apenas un 26 por ciento del pharming. (Arcila, 2010).

Dentro del estudio el 95 % de los consultados cree que son los bancos los que deben de implementar formas de autenticación más fuerte que velen por la seguridad de los usuarios mientras que el 90 % cree que su entidad financiera ya detecta actividades sospechosas y las contrarresta con alarmas en transacciones.(Arcila, 2010).

2.10 Ingeniería social

La Ingeniería social consiste en atacar las debilidades no del sistema informático sino del ser humano que puede proporcionar datos confidenciales y de esta manera conseguir algún tipo de beneficio.

2.10.1 El eslabón más débil:

No importa la inversión de cualquier sistema de seguridad si el usuario no está capacitado para mantener y ejecutar las políticas de seguridad aunque el software sea el correcto y este correctamente actualizado siempre estará en riesgo la seguridad. (Goldberger, 2006)

> La ingeniería social no es un mal en sí mismo. Un vendedor hace uso muy frecuentemente de una forma de de ingeniería social para vendernos algo que, a priori, nunca hubiésemos comprado igualmente la publicidad cuando crea una necesidad de consumir allí donde no existe (Goldberger, 2006)

La ingeniería social en manos de un cracker se convierte en una herramienta poderosa para extraer información por medio de correos, teléfonos o redes sociales donde tomar un usuario desprevenido se traduce en información confidencial en riesgo ya que puede entregar contraseñas, números de cuentas o dar información clave acerca de la empresa donde trabaja.

La tecnología solo ocupa un lugar que aunque si es destacado solo es un rol que debe cumplir, la verdadera seguridad en una empresa viene de la política en general y esto incluye protocolos y buenas prácticas de seguridad.

2.10.2 ¿Cómo piensa un estafador en ingeniería social?

Luego del éxito de la ingeniería social es importante en algunos casos no quemar la fuente ya que se requiere bastante esfuerzo para establecer una relación de confianza entre el atacante y la victima si la víctima se da cuenta de inmediato que ha sido objetivo de una estafa

puede llamar al banco por ejemplo y advertir y el atacante quizás habrá tenido tiempo de consumar su primera estafa pero no podrá seguirlo haciendo en el futuro con la misma víctima además si la victima desconoce el ataque puede significar utilizar su cuenta robada durante más tiempo.

Para evitar ser víctimas de ingeniería social el usuario nunca debe contestar con datos confidenciales correos electrónicos provenientes del banco ni hacer click en cualquier enlace que se encuentre en el correo siempre se aconseja trabajar en la página principal y oficial de la identidad bancaria, ya que estos pueden resultar enlaces falsos la información de números de cuentas y contraseñas privadas solo deben suministrarse en la sucursal bancaria de lo contrario estaremos dando toda la información necesaria para consumar el fraude. (Garay, 2008, p. 319).

2.11 Seguridad de los datos y detección de fraude.

Existen diferentes modelos de detección de fraude y estos a su vez se pueden clasificar en 3 enfoques principales:

- Detección de anomalías con alertas identifican diferentes patrones que ya antes fueron determinados como amenazas en las transacciones porque son inusuales con el resto de información en las transacciones.
- Protocolos donde el auditor tenga completo conocimiento para poder actuar paso a paso en caso de detección de fraudes.
- La elaboración de listas positivas y negativas mediante métodos supervisados y datos ya clasificados en minería de datos, análisis de patrones y estadísticas.

La implementación de estos modelos le da al auditor un mayor control, sobre los procesos de auditoría que es de vital importancia identificar un fraude tan pronto como es cometido y los modelos de detección de fraude mejoran su capacidad de análisis en las transacciones de comercio electrónico además de proveer medios de recuperación de datos con esto el experto ya está en condiciones de realizar las auditorías muy cercanas a lo óptimo.(Arias & Cerpa, 2008).

La compañía Datapro Research Corp en un reciente estudio se revela que los problemas de los usuarios que relacionan a la seguridad de una empresa se distribuyen de la siguiente manera:

- Errores de los empleados 50 %.
- Empleados deshonestos 15%.
- Empleados descuidados 15%.
- Otros 20%.

La mayoría de problemas de seguridad son relacionados con los empleados de una organización y se pueden subdividir en tres grandes grupos:

- Problemas de ignorancia.
- Problemas por haraganería.
- Problemas por malicia.

(«Manual de Seguridad V1.0 - Manual-de-Seguridad-de-Redes.pdf», s. f.).

Entre estas razones, la ignorancia es la más fácil de poner como excusa pero pueden ser combatidas con implementación de entrenamiento y protocolos, el desconocimiento de buenas prácticas de seguridad puede ocasionar incidentes que ponen en riesgo la confidencialidad e integridad de Información sensible.

Analizando todos estos datos es fácil concluir que el tema más importante para proteger la información dentro de una empresa es el tema humano y sobretodo de los empleados de la misma empresa ya que la fuga de la información está dada en un 80% de los empleados y ex empleados de la empresa sobretodo en bancos los ataques son en una proporción bastante amplia por personas que ya están o estuvieron o están dentro de la empresa.

2.12 Inyección SQL

Es una vulnerabilidad que los crackers aprovechan en las consultas de las bases de datos donde la mayoría de programadores se confían y ponen poca seguridad a veces ninguna, esta vulnerabilidad puede estar en todo tipo de lenguajes de programación.

El procedimiento es inyectar código SQL al lenguaje de programación predeterminado para cambiar su contenido y funcionabilidad de esta manera se ejecuta un código malicioso en las tablas de bases de datos esto generalmente se produce por la ignorancia de los programadores de estos posibles errores aunque se corrigen fácilmente luego que un programador con bastante experiencia en estos errores lo repare mediante los denominados parches.

Una de las formas comunes de hacer esta práctica es donde el atacante crea un súper usuario en las bases de datos usando trampa para autenticarse ya que muchos programadores no hacen la validación de la falta de datos al momento de autenticarse, esto se hace introduciendo comandos en donde debería ir la contraseña pero que cuando se hace la validación este lo ve un comando de programación y deja entrar al atacante (uno de los más comunes en PHP es "--") es por esto que se recomienda encarecidamente encriptar muy bien los campos de las contraseñas.

El atacante debe tener al menos algún conocimiento de arquitectura de bases de datos para poder realizar el ataque con éxito, la obtención de esta información es fácil ya que existen tutoriales en Internet.

El programador nunca debe confiar en ningún tipo de entrada especialmente si es del usuario ya que estos ataques se basan en explotar el código que no ha sido escrito teniendo en cuenta la seguridad.

Las técnicas de fraude en base a inyección SQL últimamente han tenido mucha más importancia que antes ya que cada vez existen más diseñadores web sin experiencia o con poca conciencia en la seguridad al momento de diseñar páginas debido a que cada vez existen más herramientas para diseñar web y la información para aprender a hacerlo está al alcance de la mayoría de usuarios de Internet.

Los crackers que penetran la base de datos son capaces de sacar información valiosa como por ejemplo nombres y números de tarjetas de crédito de usuarios y se logra con facilidad en un sitio popular pero con una pobre programación en seguridad al violar esta línea de defensa inicial se obtienen los datos de las tarjetas de crédito de los tarjeta habientes de manera masiva.

Estos datos en su mayoría los números de las tarjetas de crédito fecha de vencimiento y códigos de seguridad se venden a un precio aproximado de 14 dólares en la Deep web, grupos de Facebook y varios otros en la Internet.

Es responsabilidad del comprador dar un buen uso a esos datos ya que de dar un uso sin conocimiento alguno o erróneo saltarán las alarmas de los bancos emisores y se bloquea la tarjeta por ejemplo es cuando la tarjeta es pertenece a el país de Estados Unidos y la usa desde

un país latino o europeo sin usar un buen proxy (computadora que sirve de intermediario) automáticamente la tarjeta se bloquea y el estafador ya le dio un mal uso a tarjeta de crédito y esta se bloqueó.

Existe una variante de esta técnica que se denomina Pharming pero esta no ataca a las páginas de los vendedores sino que de los compradores, primero insertan un troyano en la computadora de la víctima que hace cambios en la computadora de manera que cuando el comprador quiere realizar una compra online este ve una copia exacta de la página original pero no se da cuenta y al poner sus datos en esta página que copia la original y así estos datos pasan directamente al atacante, tener un antivirus actualizado en general resuelve este tipo de problemas.

2.13 Puerta de enlace o proxy.

El proxy contribuye a la seguridad con la que navegamos en Internet ya que este sirve como ordenador entre el usuario y la Internet de esta manera no se puede rastrear al usuario original sino que a los proxys que por supuesto tiene una IP diferente al usuario de esta manera el usuario puede estar en cualquier país o en cualquier otro lado del mundo donde se requiera. Ver figura 3.

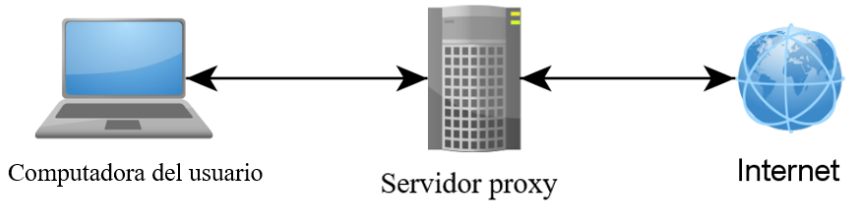

Figura 4 Interpretación del funcionamiento de un proxy.
Fuente: (Fuentes, 2016).

> Lo que hace es enmascarar tu auténtica IP, dando otras direcciones de cualquier parte del mundo para confundir a los servidores. (Además) utiliza los proxy, que ayudan a hacer un puente y traspasar filtros para que la página que visitas no sepa tu verdadera identidad.(«Deep Web», 2014).

Una ventaja de los servidores proxy es que la seguridad informática es beneficiada ya que estos mejoran el acceso a las páginas web y al mismo tiempo filtran contenido y malware, usuarios que desean visitar paginas prohibidas o con contenido no disponible en su país

pueden utilizar el proxy que se conectan a una computadora que si tiene todos los derechos para conectarse a cualquier clase de sitio web o que tiene más privilegios que el país del usuario por ejemplo mucha gente en el país de china usa proxys para conectarse a Facebook otro ejemplo es Netflix donde muchas películas no son transmitidas en América Central un usuario con un Proxy de América del Norte puede acceder al contenido que previamente estaba prohibido.

También puede ser usado en viceversa por los gerentes en tecnologías de la información de una empresa que necesitan monitorear que la empresa tiene o no permisos para acceder a ciertas páginas web con la red local de la misma entonces usan proxy para probar la intranet de la empresa.

Para el tema que se propone en esta investigación el proxy se usa frecuentemente para fraudes y procesos ilegales ya que evita ser rastreado. La mayoría de buenos hackers además de usar el proxy utilizan una máquina virtual y luego dentro de la misma instalan un proxy esto les da una seguridad extra de no ser rastreados.

2.13.1 Instalación de un proxy

Para el proxy más básico simplemente son 2 pasos para instalar el proxy para esconder la IP física de usuario donde el paso uno es buscar en Internet el proxy de preferencia la mayoría cumplen el mismo objetivo y tienen IP en su mayoría de Norteamérica y Europa, el paso dos es definir a qué velocidad navegar, los proxys se pueden descargar para Windows y Linux la mayoría son de pago pero ofrece un periodo de prueba. Dentro de las ventajas de utilizar proxy tenemos sobre todo el anonimato luego le siguen filtros más eficientes mayor seguridad y muchas veces mayores velocidades. Dentro de las desventajas tenemos que si el proxy está demasiado sobrecargado puede verse lento si tiene muchos ordenadores de manera simultánea algunos proxys sobre todo los gratis además guardan copias de transferencias y comunicaciones que causa violación a los propios datos del usuario, si no se paga por el servicio los proxys pueden resultar en conexiones más lentas.

2.14 Leyes vigentes en Honduras ante fraude electrónico.

En Honduras no existe una Ley contra el ciberterrorismo en sí, cuando se trata de judicializar estos casos se apegan al artículo 241 y 242 del código penal Hondureño en donde se hace referencia a los delitos de estafa y fraude utilizando sistemas informáticos («CÓDIGO PENAL DE HONDURAS », s. f.).

Desde el año 2015 hasta la actualidad el Congreso Nacional de Honduras está trabajando en la nueva propuesta de ley para incluir nuevos incisos en el código penal hondureño donde se hacen referencia a la ciberdelincuencia, estos contemplarían robo de identidad, clonación de tarjetas, atentados contra la identidad de datos entre otros.

> Actualmente en el Congreso Nacional se discute una ley especial de delitos cibernéticos, pero sin el concurso de expertos en esta temática por lo que se presume que se hará un "copy paste" de legislaciones de otros países, dijo al periódico Hondureño "Criterio.hn" la experta en derecho informático (Alicia Paz, 2016).

Actualmente la Agencia Técnica de Investigación Criminal (ATIC) que es un organismo dedicado a la investigación de los delitos graves y de fuerte impacto social en Honduras es pionera en sus resultados contra el ciberterrorismo en honduras.(«ATIC», s. f.) El nuevo proyecto de ley estaba destinado a completarse para finales del año 2016 pero actualmente no se ha implementado aun.(«CÓDIGO PENAL DE HONDURAS, s. f.).

CAPÍTULO III. METODOLOGÍA

3.1 Investigación

El primer paso es leer todo lo relacionado con el tema de seguridad informática y reunir todas las raíces y sub temas de estos luego de leer libros, revistas, artículos esto lleva a la realización de que el tema es bastante amplio y lleva la necesidad de resumirlo para poder contemplar sus diferentes sub ramas de una manera más específica para luego conectarlos entre sí a través del presente trabajo de investigación

3.2 Concretar definiciones.

Importante aterrizar el verdadero tema de investigación que es fraudes a el tarjeta habiente con sub ramas en los diferentes tipos de fraudes que se pueden realizar a los usuarios de banca.

En esto permite determinar que existan 2 grandes personalidades en juego uno es el banco y el otro es el usuario, son los dos objetivos en los que se centra el presente tema de investigación y con este conocimiento permite enfocar la investigación en cómo estas 2 grandes personalidades se ven afectadas por los ataques de crackers.

Se determina que entra en juego otra gran personalidad que es el carder y de este trabajo de investigación podemos concretar los objetivos y el propósito de esto que queremos y en lo que queremos lograr, pero además de que observamos las capacidades que tiene el banco para defenderse de estos fraudes y determinar si el usuario tiene conocimiento o no en cómo protegerse del robo de sus datos.

3.3 Definir preguntas de entrevista a los tarjeta habientes y expertos en la materia

Tanto como para personas con alto conocimiento de temas de seguridad como también para usuarios de los bancos que poseen una tarjeta.
Las preguntas para usuarios comunes de la banca son:

- ¿Cuántas tarjetas de crédito y débito tiene actualmente?
- ¿Tiene seguros antifraude en sus tarjetas de crédito?
- ¿Ha sido objetivo de fraude o conoce alguna persona que ha sido estafada en sus tarjetas de crédito?
- ¿Tiene alguna educación financiera de cómo prevenir fraudes a sus tarjetas de crédito? (¿De ser afirmativa la respuesta donde obtuvo ese conocimiento?)

El objetivo de estas preguntas es medir si las personas que tienen tarjeta de crédito, en promedio han sufrido un fraude o conocen a alguien que sí, además de saber si se solucionó el problema y si tiene algún conocimiento que le ayude a prevenir un fraude electrónico.

Las preguntas de entrevistas a expertos en fraude electrónico son:

- ¿Qué estamos haciendo en Honduras para prevenir el Fraude?
- En general, de cada 100 casos de fraude electrónico, ¿Cuántos cree usted que no se da una solución satisfactoria al tarjeta habiente afectado?
- ¿Cuál cree que son los principales lugares donde hay facilidad para que se cometa fraude electrónico?
- ¿En cuánto tiempo normalmente se da una resolución de problemas con relación al fraude para el tarjeta habiente?
- ¿Cuáles son las medidas que deben tomar las instituciones para reducir los fraudes a los tarjeta habientes?

Con estas preguntas se busca conocer cómo está la situación actual en Honduras y el tiempo de resolución de problemas que es lo más importante además de saber si los expertos coinciden en las formas de prever el fraude electrónico que se expondrán en las conclusiones de este material de investigación, estas personas a entrevistar son clave en diferentes puntos de seguridad de sus mismas empresas donde laboran, tienen acceso a datos que aunque los nombres permanecen en secreto y no se pueden divulgar, si podemos estudiar los números que nos proporcionan para sacar estadísticas y tener una idea clara de cómo está el fraude electrónico a nivel nacional.

Segundo objetivo de estas preguntas es medir el calibre con el que los usuarios normales son estafados y saber qué nivel de necesidad de una educación financiera y de seguridad necesitan los usuarios normales en nuestro país con estas preguntas podremos sacar estadísticas y comparaciones y dará una clara idea de cómo es la realidad a nivel nacional.

3.4 ¿Cómo es un hacker?

Dentro de toda la investigación llevada a cabo poco a poco se piensa adquirir el conocimiento y práctica y por último se requiere ir a las profundidades de la Internet donde nacen los tutoriales de inyección SQL, la raíz del carding, donde los ciberdelincuentes o piratas informáticos se reúnen para hablar de estos temas sin ningún tabú, donde la información es libre de censura y donde un paso en falso y se cometerían muchos actos que se consideran delitos en algunos países, este lugar se le conoce como Deep web o web profunda. Lo mejor es ampliar y adentrarse dentro de la oportunidad no solo de aprender cómo se hacen los negocios en este lugar sino además intentar interactuar con los hackers de la Deep web, consultar precios y métodos como ellos adquieren sus productos.

El primer paso es instalar un nuevo navegador llamado Tor este navegador se diferencia los que todos conocen porque nos permite navegar sin ser detectados ya que cambia sus IP cada 10 minutos y por eso se hace lento algunas veces pero nos garantiza que no estamos siendo rastreados es muy importante esto sobre todo si se navega en las profundidades de la Deep web o web profunda.

Una vez estando en la, Deep web el objetivo es investigar en la wiki o diccionario los sitios que podían ser de interés todos esos que se centran en la venta y compra de CC (credit cards por sus siglas en inglés) una vez dentro de estos, es encontrar los sitios de discusión donde todo es como cualquier otro foro de Internet común, personas intercambiando sus opiniones y haciendo ofertas, anunciándose etc. El objetivo es aprender mediante el contacto directo con un hacker los procesos que se manejan allí.

Se tiene como objetivo aprender diferentes tipos de fraude y entre estos el de las tarjetas de crédito, conocer varios conceptos como qué significa CC, bins, páginas vírgenes etc. Se busca aprender qué páginas normalmente son vulnerables y que características comparten entre sí, que paginas son más seguras y que caracteriza estas páginas para que sean más difíciles de hackear.

En este trabajo de investigación se va a buscar identificar que tan fácil puede llegar a ser para un usuario común y corriente aprender técnicas de hackeo, cracks, robo de información, ingeniería social y además de encontrar tutoriales sobre el paso a paso sobre temas de carding en la Deep web.

Se pretende investigar si existen grupos delictivos que se dedican al fraude electrónico en grupos comunes de Facebook, conocer con que nombres normalmente aparecen, cotizar la venta de tarjetas de crédito o si estos solo se limitan a la venta de los dígitos parcialmente correctos de una tarjeta de crédito, qué países son los más comunes de donde se roban estas tarjetas de crédito y conocer qué tipo de pagos aceptan.

Se planea realizar un estudio exhaustivo en el ambiente de los hackers a nivel internacional y nacional investigando en medios habituales como sitios web, búsquedas en google, redes sociales como Facebook y también en medios más complicados como ser la Deep web con el objetivo de determinar cómo un usuario común puede encontrar este tipo de

información con un poco de búsqueda o cuánto requiere de conocimientos técnicos para ser un hacker.

Si es posible ponerse en contacto con alguno de los hackers que moran en estos lugares conocer las formas en que aceptan pagos, intercambios, ventas de artículos, servicios que no se podrían obtener fácilmente de otra forma y descubrir el mundo de transacciones del que nadie se da cuenta pero en el que todos pueden estar involucrados indirectamente.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

El presente capítulo muestra los resultados que como parte de la investigación se hizo 2 tipos de encuestas, una a usuarios comunes de tarjetas de crédito y otra se hizo a personas con conocimiento en fraudes electrónicos,

El tamaño de la muestra de usuarios comunes fue de 72 personas pertenecientes a la zona central de Honduras que incluyen estudiantes universitarios y trabajadores de clase social media y alta, esto porque estas personas están propensas a sufrir este tipo de fraudes ya qué interactúan más con las compras en línea y en establecimientos físicos.

El tamaño de la muestra para la entrevista a personas que son expertos en materia de fraude es de 22 personas en los cuales son distribuidos entre empleados en posiciones donde se manejan estos datos de los 6 bancos más importantes del país, trabajadores en puestos de

fraude en financieras y aseguradoras de autos, y del ente regulador (Comisión Nacional de Bancos y Seguros) además de profesores en materia de seguridad informática.

Se aplicara las encuestas a personas con acceso a Internet mediante cuestionarios en línea. Con el objetivo de evaluar la situación en nuestro país con respecto al fraude electrónico y como las personas que están directamente relacionadas con este tema pueden aclarar sobre la situación actual y ayudarán con el plan actual de propuesta de mejora.

En el presente capítulo se hará una breve descripción y resumen de los resultados y análisis de las investigaciones realizadas en diferentes ámbitos del fraude electrónico esto incluye redes sociales, sitios web y finalmente resultados de sitios de la web profunda o Deep web.

4.1 Análisis de investigaciones realizadas.

Como parte del estudio se realizó una búsqueda en diferentes foros de Internet para conocer cuál es la primera información que un usuario puede encontrar durante sus primeros 5 minutos en una búsqueda en Internet ver figura 9.

Además en las redes sociales también se puede encontrar diferentes páginas dedicadas a el fraude electrónico ver figura 5 y pueden ser difíciles de encontrar si no se sabe que palabras clave buscar y como es de esperar una vez dentro de ellas existen diferentes ofertas de los hackers para vender los productos que ilegalmente han obtenido mediante el método carding ver figura 6.

Figura 5. **Página de grupo de intercambios y pagos ilícitos en Facebook.**
Fuente: Red social Facebook.com

Los diferentes grupos de la red social Facebook tienen diferentes objetivos como pago de servicios, compartir datos de tarjetas de crédito de personas víctimas de diferentes métodos de estafa electrónica, aprender a hacer fraude electrónico y compartir tutoriales de cómo hacer hacking. La mayoría de los perfiles que se encuentran en estos grupos son perfiles secundarios o falsos para que el hacker no revele su identidad sin embargo muchos de los hackers que venden a otros hackers datos de tarjeta de crédito tienen perfiles verdaderos en orden de mostrar credibilidad a sus futuros compradores.

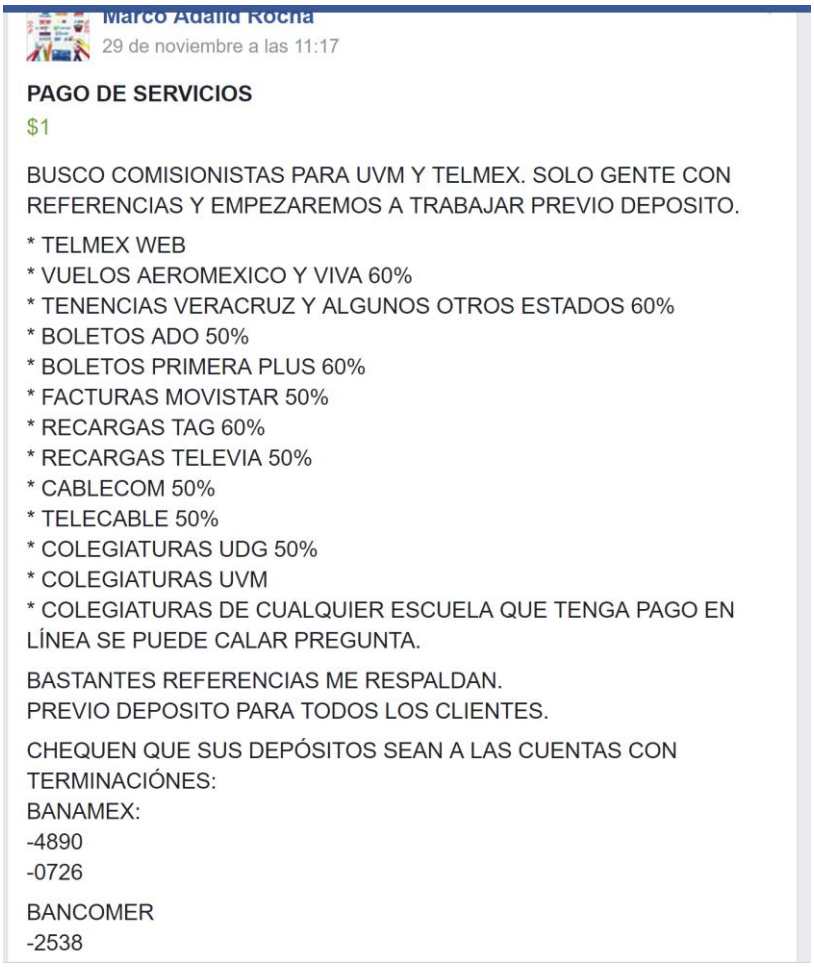

Figura 6. Captura tomada de un grupo de intercambios de datos de tarjetas en Facebook
Fuente: Red Social Facebook grupo de "carding Latinoamérica"

El término conocido dentro de los foros de Internet y redes sociales para las tarjetas de crédito es el denominado "CC" y para los dígitos parcialmente correctos de una tarjeta de crédito el termino es "*bins"* que son los al menos 6 números de una tarjeta de crédito que luego son extrapolados en páginas de Internet para conseguir los datos de una tarjeta auténtica.

En la Deep web o en los grupos de Facebook se intercambian y se venden bins, estos luego de pasarse por un checker (ver figura 1) da como resultado varias tarjetas de crédito.

Las tarjetas de crédito pueden estar vivas o muertas los dígitos generados por el cheker que estén vivos automáticamente harán el cobro de 1 dólar, para saber que esos dígitos verdaderamente funcionan, una vez comprobado esto sirven para comprar desde cosas

sencillas como cuentas en sitios de música o películas de streaming, por ejemplo “Netflix” o “Spotify”, hasta transacciones más grandes como compras en línea de más de 200 dólares. Para saber esto es necesario saber qué tipo de tarjeta es la que “salió viva” y pueden existir diferentes clasificaciones como por ejemplo clásica, dorada o platinum esto depende del ente que provee la tarjeta, esta información también la provee el sitio web o cheker donde se hacen las pruebas.

Existen páginas web no muy seguras a estas páginas se le llaman sitios web vírgenes y son páginas que no han sido explotadas por los carders es decir no han mejorado aun sus métodos de seguridad anti hack , una vez una página ha sido estafada muchas veces estas mejoran sus sistemas de seguridad y dejan de aceptar cualquier tipo de tarjeta de crédito además de actualizar la IP con la quiso hacer la compra ilícita en lista negra para que futuras compras desde esa ip estén bloqueadas automáticamente, como el caso de Amazon que tiene unas reglas exigentes de rastreo de IP y verificación de identidad y cada vez que un usuario nuevo hace una compra, se tarda más tiempo de lo normal en ser aprobada dicha compra ya que se somete a diferentes investigaciones para verificar la legitimidad del dinero aunque aun así tampoco Amazon se salva del fraude electrónico de los hackers más experimentados ver figura 7.

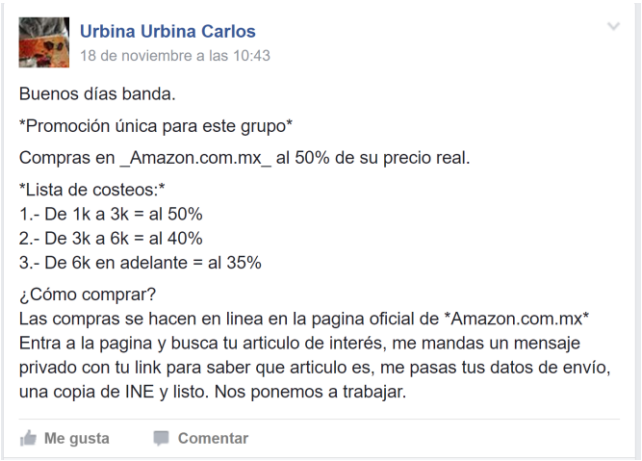

Figura 7. Ejemplo de rango de precios para pagar por artículos a un precio de hasta el 65% menos del valor original
Fuente: Red Social Facebook grupo de “carding Latinoamérica”

En Internet y las redes sociales los trueques que se llevan a cabo dependen mucho de la confianza que los denominados “proveedores” que son hackers a los cuales las personas comunes les pagan para que compren artículos al 50 % o más baratos que lo normal, además

estas personas también pueden pagar de manera ilegítima servicios como por ejemplo Internet, planes telefónicos o hasta vuelos internacionales.

Para asegurar a los futuros clientes la confianza, es muy importante que el hacker guarde conversaciones de clientes satisfechos y debe tener referencias de otras personas que den fe de que no es estafador de estafadores ya que la mayoría de estos piden el pago por adelantado ver figura 8. El pago es realizado mediante Western Union que es ideal para hacer transferencias internacionales y nacionales sin dejar muchos datos o directamente desde bitcoins a través de Internet.

Figura 8. Carder busca demostrar que tiene clientes satisfechos con múltiples artículos que otras personas han comprado mediante CC que el vende ilícitamente.
Fuente: Red Social Facebook grupo de "carding Latinoamérica"

En Honduras se observa que en muchos grupos de ventas de en Facebook se pueden encontrar personas vendiendo cuentas de Spotify y Netflix incluso boletos de cines nacionales como Cinemark y Cinepolis a precios muy bajos que según los vendedores solo pueden ser en lugares que se compre en línea por montos pequeños. En Honduras no se pudo encontrar un

grupo de hackers fuerte en comparación con los de otros países de Latinoamérica como por ejemplo México y Colombia pero sí se identificaron en los diferentes grupos de venta que son páginas donde las personas pueden vender diferentes artículos que van desde celulares hasta refrigeradoras, carros, electrodomésticos etc.

En la Deep web se encontró que a diferentes límites de tarjeta se venden a diferentes precios depende de la cantidad de dinero que pueden tener disponible, las tarjetas con límite de 500 dólares o menos se venden a un precio de aproximadamente 15 dólares cada una mientras que las límite de 3 mil dólares se logran vender entre 45 a 95 dólares. En la mayoría de los casos es responsabilidad del comprador saber usar los datos de una tarjeta de crédito pero en ocasiones los mismos vendedores pueden enseñar si se trata de compras en línea o comparten tutoriales para hacer el cardeo, el siguiente ejemplo es la primera página en el buscador de Google al poner la frase "compra de CC". Ver figura 9.

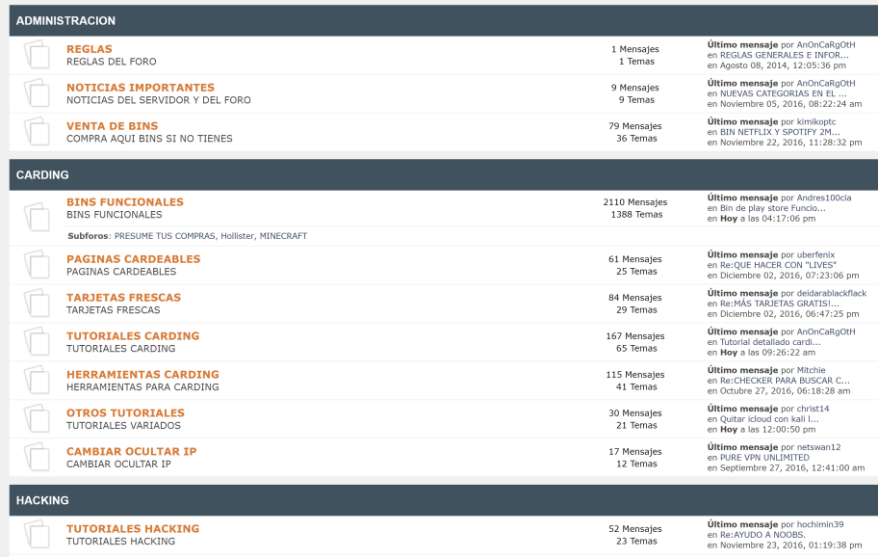

Figura 9 Captura tomada del primer sitio web en búsqueda con la frase "venta de cc" Fuente: http://binerosunidos.org/

En la figura 9 se observa que se comparten diferentes temas útiles para cualquier usuario en Internet que desee aprender a hacer carder ya que como temas principales están tutoriales de carding, herramientas para carding y páginas para hacer carding. Estos temas son similares a los que se encuentran en la Deep web si el usuario sabe buscar pero en la wiki de la Deep web solo se selecciona el tema de interés para buscar todos los sitios web que tengan una relación con el tema seleccionado en la página principal de la Wiki de la Deep web es

posible encontrar todo tipo de temas desde compra de armas y drogas hasta teléfonos robados y falsas identificaciones pero además existen muchos temas relacionados con el carding y hasta es posible contratar un hacker para realizar ingeniería social o un ataque DDOS que consiste en hacer que un servicio en Internet sea inaccesible temporalmente ver figura 10.

En la investigación que se llevó a cabo fue posible entablar conversaciones con algunos hackers donde su principal área de especialidad es el carding a gran escala donde se logran vender datos de hasta 25 personas por día o incluso se venden paquetes de 10 a 20 datos de tarjetas de crédito diferentes en una sola transacción.

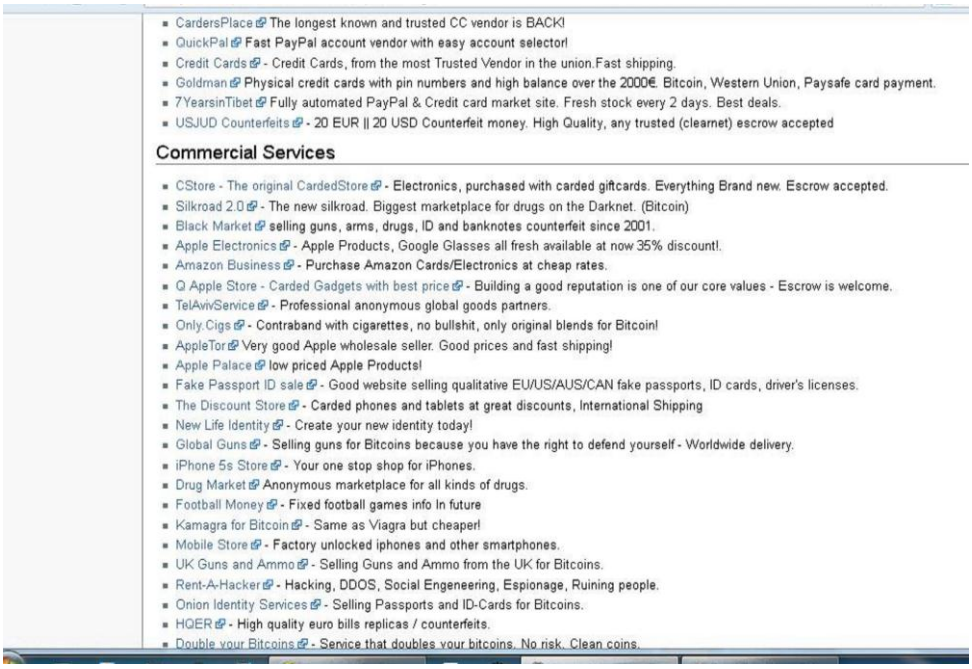

Figura 10 Captura de la "hiden wiki" que sirve como índice de la Deep web.

4.2 Análisis de resultados de encuesta a usuarios comunes de tarjetas de crédito

Las encuestas que fueron aplicadas a usuarios comunes de tarjetas de crédito serán denominadas como encuesta uno, en total la muestra de la encuesta la encuesta 1 es de 72 personas que poseen tarjeta de crédito y encuesta 2 se denominara para la encuesta que se aplicó a las personas que tienen conocimiento en fraudes electrónicos.

Figura 11 Número de tarjetas que una persona promedio entre 18 y 35 años tiene en Honduras

En la siguiente grafica referente a la pregunta número uno y dos comparadas entre sí. La línea roja representa las personas que no tienen un seguro antifraude y su nivel en la gráfica el número de tarjetas de crédito que tienen con un máximo de cuatro o más. La línea azul representa las personas que si tienen un seguro antifraude y su nivel en la gráfica, el número de tarjetas de crédito que poseen,

Observamos que el 55 % tiene más de 3 tarjetas de crédito y si tienen seguro antifraude deberán pagar 3 seguros antifraude diferentes en caso de tener uno en cada tarjeta para esto estas personas al menos deben ser conscientes del peligro a ser víctimas de una clonación de tarjeta y recibir de algún modo un cierto nivel de educación financiera y cómo protegerse ante el fraude electrónico.

De los usuarios que tienen tres o más tarjetas de crédito en su mayoría poseen cierto conocimiento para protegerse del fraude electrónico, estos son representados en color azul en comparación a los color rojo que no tienen ningún conocimiento de protección antifraude sin embargo el 65 % de estos usuarios tienen 3 o más tarjetas de crédito,

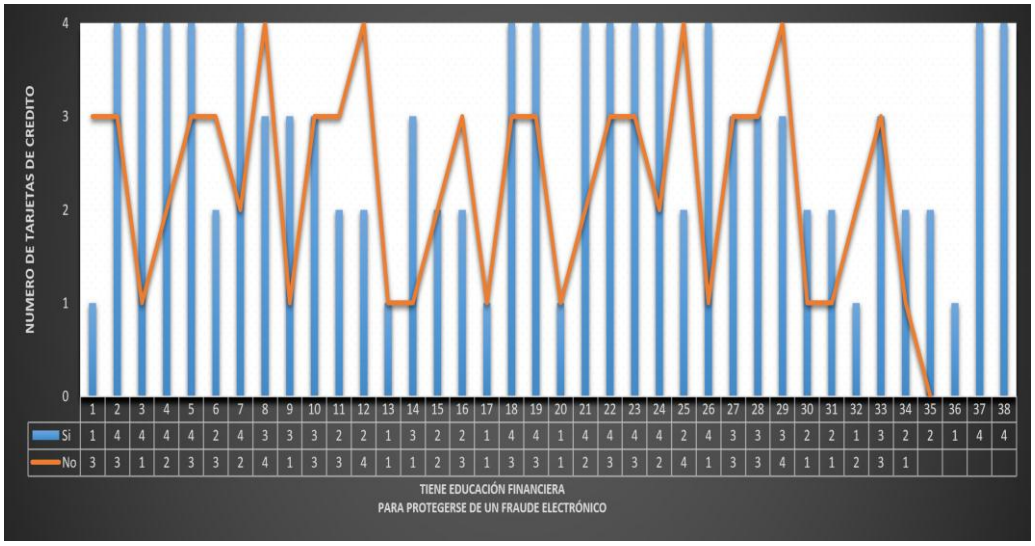

Figura 12 Personas que tienen educación financiera en comparación a número de tarjetas que tienen.

Se observa que son cifras son muchos los usuarios que reciben al menos un poco de conocimiento anti robo como indica la pregunta número cinco que dice que tipo de conocimiento antifraude ha recibido; la mayoría manifiesta haberlo adquirido en el mismo banco emisor a través de la persona que le entrego la tarjeta y las otras partes se dividen en personas que investigaron por su propia cuenta, que tienen amistades en la banca o trabajan allí.

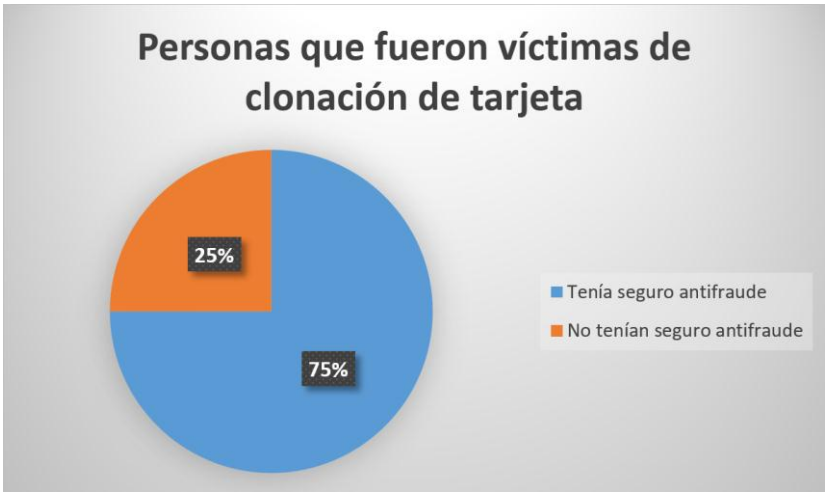

Figura 13. ¿Cuántas de las víctimas de clonación de tarjeta tenían seguro de antifraude?

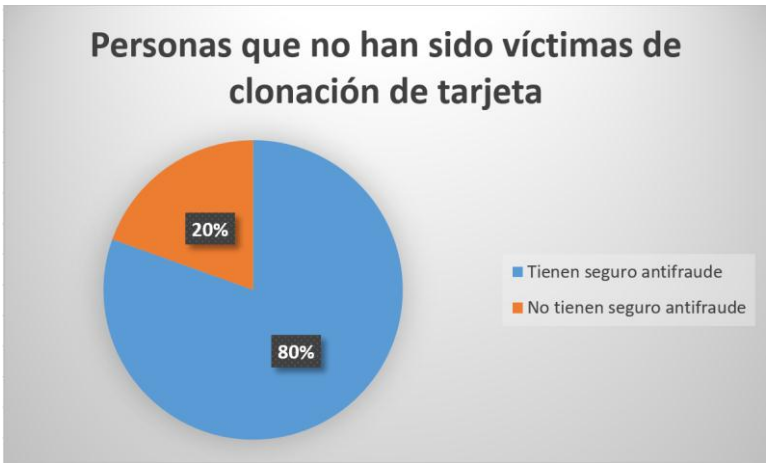

Figura 14. ¿Cuántas de las personas que no nunca han sido víctimas de clonación de tarjeta no tienen aún seguro de antifraude?

La pregunta número dos y tres se les preguntó si han sido víctimas de fraude electrónico alguna vez y si tenían o tienen seguro antifraude, se observa en los datos que se relaciona el 25% de las personas que si han sido víctimas de estafa no tenían seguro de antifraude en sus tarjetas de crédito por tanto tuvieron que asumir la pérdida aunque también existieron casos dentro de la muestra donde el banco a pesar de que algunos usuarios no tenían el seguro igual pudieron demostrar su inocencia ya que las tarjetas habían sido clonadas y usadas en países como Brasil y Colombia y estos usuarios no habían hecho viajes fuera del país. De las personas que nunca han sido víctimas de estada electrónica de ningún tipo el 20% aun no tienen ningún seguro antifraude.

4.2.1 Análisis de encuesta número dos.

Como parte de la investigación para conocer la situación en Honduras es necesario aplicar encuestas a personas que tienen un panorama más amplio desde el lado de los entes financieros y aseguradores, con el objetivo de saber qué están haciendo para protegerse y cómo están protegiendo al usuario de tarjetas de crédito en el país.

Figura 15. Tiempo de resolución de problema para la víctima de una clonación de tarjeta.

Con relación a la pregunta número uno de la encuesta aplicada a personas expertas y con experiencia en el tema indican que en el 50% de los casos el usuario debe esperar más de una semana para obtener una respuesta satisfactoria al problema que presenta y esto depende si paga un seguro antifraude o no cuando el usuario no paga ningún seguro depende mucho del banco emisor y de las pruebas que el usuario pueda sustentar para no asumir la pérdida, producto de lo más probable una clonación de tarjeta de crédito.

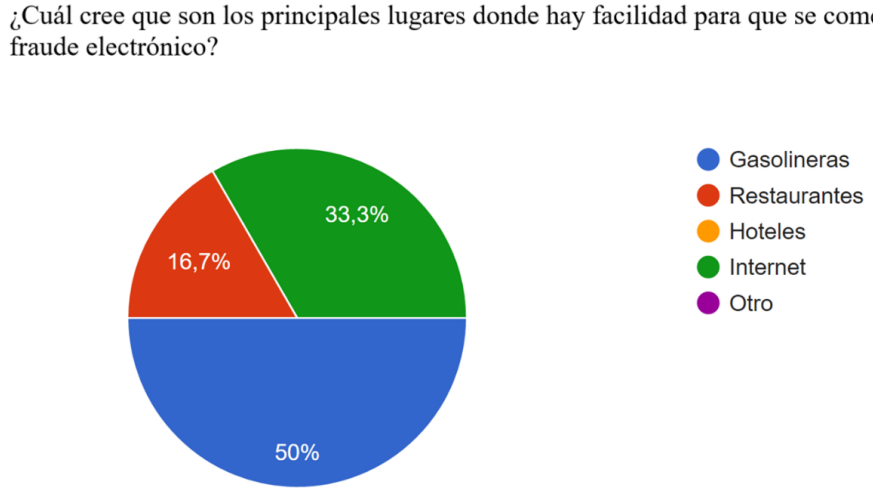

Figura 16. Lugares donde comúnmente se propician la clonación de tarjeta.

Sobre los sitios donde más se producen los robos de los datos es en lugares como gasolineras donde es fácil tomar una foto de los datos de tarjeta de crédito o utilizar un skimmer ya que el usuario a veces no se da cuenta donde está la tarjeta de crédito en todo momento durante el pago del servicio, mientras otro 33% indica que el fraude electrónico se produce en Internet al realizar pagos con tarjetas de crédito, los virus informáticos guardan los datos co n los que se realizó el pago o mediante ingeniería social por medio de un correo electrónico disfrazado del banco pidiendo datos sensibles del usuario con alguna excusa como por ejemplo para mejorar el rendimiento del servicio.

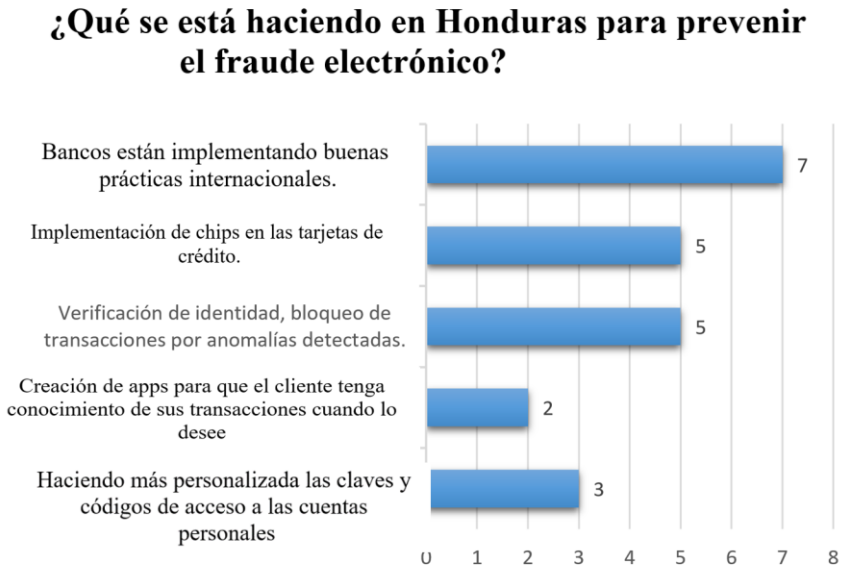

Figura 17. Soluciones que se están implementando en Honduras actualmente.

El 32 % de los expertos entrevistados opinan que en Honduras se está imitando buenas prácticas de bancos internacionales donde las medidas de seguridad son mejores es posible concluir que en países subdesarrollados no son proveedores de nuevos estándares de seguridad y se limita a implementar los protocolos de seguridad que mejor se acondicionen de los bancos que se encuentran en otros países más desarrollados.

El 23% opina que la interpretación y monitoreo de anomalías en las transacciones de los clientes de tarjetas de crédito son una herramienta útil que se implementa en el país además

otro 23% opina que la implementación de chips en las tarjetas de crédito está ayudando para la protección del tarjeta habiente en sus transacciones.

El 9% de los 22 encuestados opinan que la creación de apps para que el usuario siempre éste en entero conocimiento de cada transacción que se realiza, es una buena forma de que él pueda reportar cualquier anomalía que detecte mientras que el 13% restante expresa que haciendo las claves de acceso más personalizadas y los códigos de verificación de identidad con mejor tecnología es la primera línea de seguridad que se implementa en Honduras.

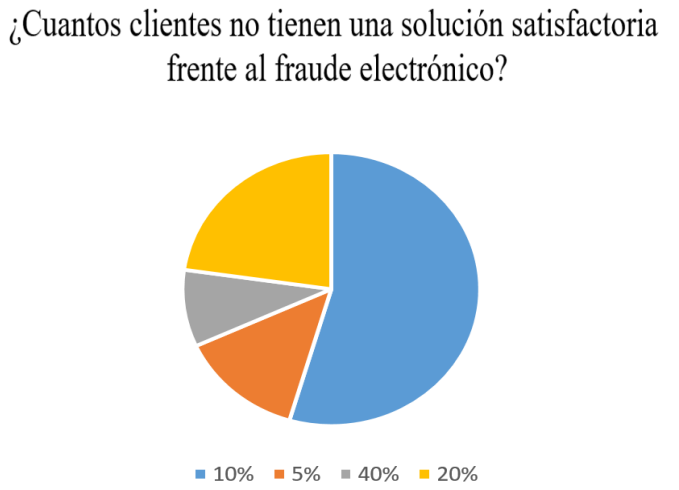

Figura 18. El 68% de los encuestados concuerdan que menos del 10% de los usuarios no obtienen una respuesta satisfactoria.

El 68% de los expertos encuestados expresan que menos del 10% de los casos que se reportan de fraude electrónico no se da una respuesta que ayude a solucionar el problema al cliente y aunque antes describieron que la respuesta no es en menos de una semana se observa que si el cliente denuncia el fraude tiene buenas posibilidades de recibir una solución a la estafa de fraude electrónico y no asumir la pérdida que resulto de esto, los datos recabados en esta pregunta complementan la respuesta dada por los usuarios en la encuesta número uno ya que solo dos de los 72 encuestados tuvieron que asumir las pérdidas producto del fraude electrónico, además con estos datos podemos concluir que los entes financieros absorben la mayoría de las pérdidas que se presentan en casos de estafa a sus clientes.

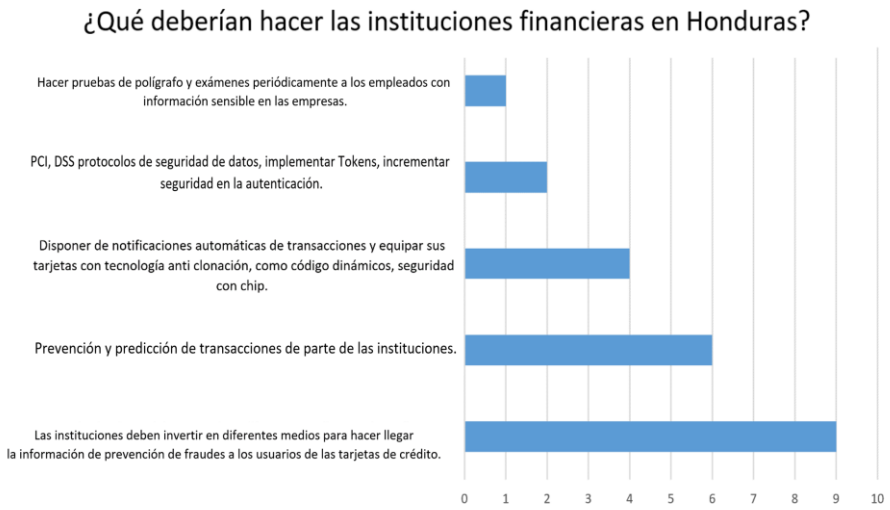

Figura 19. Posibles soluciones que las instituciones y bancos pueden implementar que para combatir el fraude electrónico.

Referente a la pregunta numero 5 los encuestados propusieron ideas de qué deberían hacer los entes financieros en Honduras para combatir el fraude electrónico y proteger no solo a sus clientes sino también a sí mismos. De los 22 encuestados 9 indican que la mejor forma de prevenir el fraude electrónico es hacer llegar información útil a sus clientes ya sea mediante correos electrónicos, panfletos o charlas al momento de ser atendidos o al serles entregada las tarjetas de crédito.

De los encuestados seis proponen que la mejor forma de combatir el fraude electrónico es mediante la predicción de las transacciones mediante monitoreo de cada compra en comparación a ubicaciones del usuario, la generación temprana de alertas de fraude permite el bloqueo automático de la tarjeta de crédito hasta validar la identidad del usuario.

6 de los 22 encuestados más comparten opiniones sobre la tecnología que se utiliza en la autenticación del usuario es muy importante pero además los protocolos de seguridad son la solución que debe nacer desde dentro de la empresa o ente financiero.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se logró identificar las herramientas de carding y fraude electrónico gracias a las investigaciones y experimentos de los métodos de estafa que afecta no solo a Honduras sino a los países latinoamericanos logrando entender cómo se desarrolla y perpetra un ciberdelito paso a paso y cómo diferentes ámbitos de la sociedad que tienen que ver con el tema directa o indirectamente reaccionan ante la situación actual que vive el país.

- Con los datos recaudados se pueden proponer posibles soluciones para los usuarios de tarjeta de crédito que ayuden a evitar ser estafados como por ejemplo no perder de vista sus tarjetas de crédito al momento de pagar en un establecimiento y realizar compras en línea en sitios seguros, además se tienen datos concluyentes sobre cómo aumentar la seguridad de los entes financieros y cómo estos deben cuidar la seguridad informática y priorizar en primer lugar sus empleados con información sensible y en segundo lugar la tecnología que solo cumple su rol que si bien es muy importante el factor decisivo lo tienen las personas que trabajan en organización.

- Se logró conocer qué entes Hondureños buscan proteger al usuario con tarjeta de crédito y tienen herramientas que son eficaces para la detección y prevención de fraude electrónico, mientras que no existe una ley en específico para lidiar con el ciberterrorismo sí que se está trabajando en este tema actualmente en el Congreso Nacional de Honduras, es cuestión de poco tiempo para que la ley entre en vigencia pero también se identificó que se necesita equipo especial y personas especializadas para confrontar este tipo de casos con lo que se encuentra en escasos recursos para demostrar un ciberdelito en la realidad el país mantiene actualmente.

- Se concluye que actualmente la información para perpetrar un cibercrimen está al alcance de cualquier usuario de Internet y que no requiere ser un especialista en informática para aprender a usar las herramientas de hacking y carding, además se identificó que existe mucha información disponible que enseña paso a paso como un

usuario común y corriente obtiene la información necesaria para convertirse en un cibercriminal.

5.2 Recomendaciones y posibles soluciones.

5.2.1 Soluciones para los usuarios tarjeta habiente:

- Se recomienda a los usuarios que tengan tarjeta de crédito que utilicen el seguro que su banco les proporcione y que no pierdan de vista su tarjeta de crédito al momento de pagar con ella.
- Es muy importante que la población tenga educación financiera, utilizar medios de difusión y capacitación en universidades y bancos para que las personas en general aprendan el método correcto de utilizar una tarjeta de crédito y cómo protegerse y evitar fraudes electrónicos. La falta de ignorancia con este tema puede llegar a ser la solución más importante y definitiva para combatir el fraude electrónico y la estafa mediante ingeniería social.

5.2.2 Posibles soluciones para las empresas y organizaciones financieras:

- Se recomienda a las organizaciones financieras y bancos crear una cultura empresarial que tenga como factor importante la seguridad de los datos y hardware que pueda poner en peligro los datos sensibles de la empresa.

- Es importante enfatizar que las empresas deben tener protocolos de seguridad al prescindir de empleados que ya no son parte de la empresa cambiando las contraseñas y accesos además de informar a toda la empresa que dicho empleado ya no forma parte de la misma sobre todo en las empresas donde constantemente hacen rotación de personal.

REFERENCIAS BIBLIOGRÁFICAS

Mitnick, K. (2009). En *ingenieria social* (pág. 18).

Rello, C. A. (13 de agosto de 2014). *Monografias.com*. Obtenido de http://www.monografias.com/trabajos89/crimen-y-fraude-informatico/crimen-y-fraude-informatico.shtml

Sebastián, S. A. (1 de junio de 2011). ingenieria social.

Segu-info. (sin fecha).

ADDIN ZOTERO_BIBL {"custom":[]} CSL_BIBLIOGRAPHY A. Fernandez. (2016, agosto 6). Apple paga a «hackers» para encontrar fallos. Recuperado 25 de septiembre de 2016, a partir de http://www.expansion.com/empresas/tecnologia/2016/08/06/57a60b5c468aeb294c8b465c.html

Adrian Hernan. (s. f.). Hackear PS Vita es más dificil gracias a su tarjeta de memoria – PS Vita. Recuperado 25 de septiembre de 2016, a partir de http://www.juegosdb.com/hackear-ps-vita-es-mas-dificil-gracias-a-su-tarjeta-de-memoria-ps-vita/

Alicia Paz. (2016, julio 6). Estado hondureño improvisará al incluir delitos cibernéticos en Código Penal. Recuperado a partir de http://criterio.hn/estado-hondureno-improvisara-al-incluir-delitos-ciberneticos-codigo-penal/

Angelucho. (2013, agosto 25). Las profundidades de Internet: LA DEEP WEB. Recuperado a partir de http://elblogdeangelucho.com/elblogdeangelucho/blog/2013/08/25/las-profundidades-de-Internet-la-deep-web/

Arcila, N. D. (2010). Crece inquietud por fraude electrónico a la banca. *Portafolio*. Recuperado a partir de http://search.proquest.com/docview/757796297/abstract/3E4BA67A31404690PQ/1

Argentina, L. N.-. (2015). Deep web: el universo paralelo de Internet. *La Nación*. Buenos Aires, United States. Recuperado a partir de http://search.proquest.com/docview/1657262781/abstract/9276D467207840F1PQ/1

Argentina, L. N.-. (2016). Tarjetas de crédito: las 5 formas de estafas que más preocupan a todos. *La Nación*. Buenos Aires, United States. Recuperado a partir de http://search.proquest.com/docview/1757509886/abstract/CEEF6AC3A1E44FF4PQ/2

Arias, F., & Cerpa, N. (2008). EXTENDIENDO EL MODELO e-SCARF DE DETECCION DE FRAUDE EN SISTEMAS DE COMERCIO ELECTRONICO/EXTENDING THE e-SCARF MODEL FOR FRAUD DETECTION ON ELECTRONIC COMMERCE SYSTEMS. *Ingeniare : Revista Chilena de Ingenieria*, *16*(3), 282-294.

ATIC. (s. f.). Recuperado 26 de septiembre de 2016, a partir de https://www.mp.hn/index.php/direcciones/atic

Bitcoin - Wikipedia, la enciclopedia libre. (s. f.). Recuperado 5 de diciembre de 2016, a partir de https://es.wikipedia.org/wiki/Bitcoin

CODIGO PENAL DE HONDURAS - Codigo-Pena-Honduras.pdf. (s. f.). Recuperado a partir de https://www.ccit.hn/wp-content/uploads/2013/12/Codigo-Pena-Honduras.pdf

Deep Web: el lado oscuro de Internet. (2014). *Expansión*. Mexico City, United States. Recuperado a partir de http://search.proquest.com/docview/1541472245/citation/9276D467207840F1PQ/14

e-crime, P. por S. (s. f.). Bancos contra carders. Recuperado a partir de http://blog.s21sec.com/2010/03/bancos-contra-carders.html

Fraude electrónico crece y cambia de cara tan rápido como la tecnología: TECNOLOGÍA FRAUDE (Entrevista). (2015). *EFE News Service*. Madrid, United States. Recuperado a partir de http://search.proquest.com/docview/1645918562/abstract/6A2252790C814115PQ/1

Fuentes, F. J. S. (2016, febrero 7). Lo basico sobre los proxy. Recuperado a partir de http://www.fsanchez.cl/index.php/2016/02/07/lo-basico-sobre-los-proxy/

Garay, J. B. (2008). El Fraude on-Line: Nuevo Escenario, Vieja Picaresca. *Boletín de Estudios Económicos*, *63*(194), 311-332.

Goldberger, R. (2006, abril 10). Opinion-Las amenazas a la privacidad mas importantes de la actualidad; [Source: El Reporte Delta]. *NoticiasFinancieras*, p. 1. Miami, United States.

JAIVIA. (2014). Riesgo en el uso de tarjetas El crédito y el débito, en la mira. *Portafolio*. Recuperado a partir de http://search.proquest.com/docview/1501635492/abstract/BEB4C478490C4009PQ/1

LÁNDER, R. (2016). 5. Pólizas Contra La Amenaza De Los Ciberdelitos. *Actualidad Economica*. Recuperado a partir de http://search.proquest.com/docview/1805374760/citation/4621C168B21A4049PQ/3

leonardo ballado. (s. f.). ¡Uber le paga a Hackers! – MarcianoTech. Recuperado 25 de septiembre de 2016, a partir de http://www.marcianotech.net/2016/03/26/uber-le-paga-a-hackers/

Manual de Seguridad V1.0 - Manual-de-Seguridad-de-Redes.pdf. (s. f.). Recuperado a partir de http://instituciones.sld.cu/dnspminsap/files/2013/10/Manual-de-Seguridad-de-Redes.pdf

Mitnick, K. D., & Simon, W. L. (2007). *El arte de la intrusion: la verdadera historia de las hazañas de hackers, intrusos e impostores*. México D.F.: Alfaomega : RA-MA.

Parche (informática). (2016, septiembre 30). En *Wikipedia, la enciclopedia libre*. Recuperado a partir de https://es.wikipedia.org/w/index.php?title=Parche_(inform%C3%A1tica)&oldid=93999404

ANEXOS

6.1 Preguntas de encuesta a usuarios de tarjetas de crédito.

¿Cuantas tarjetas de crédito y débito tiene actualmente? *

- 1
- 2
- 3
- 4 o mas

¿Tiene algún tipo de seguro anti fraude en sus tarjetas de crédito? *

- Si
- No

¿Ha sido objetivo de fraude o Conoce alguna persona que ha sido estafada en sus tarjetas de crédito? en caso de ser una respuesta afirmativa de un breve resumen sobre lo sucedido *

Texto de respuesta larga

¿Tiene alguna educación financiera de cómo prevenir fraudes a su tarjetas de crédito? *

- Si
- No

En caso de ser afirmativa la respuesta anterior como obtuvo ese conocimiento?

Texto de respuesta larga

Edad

- Entre 18 y 25 años
- 26 y 35 años
- mas de 36 años

6.2 Preguntas de encuesta a expertos en materia de fraude electrónico.

¿Que estamos haciendo en Honduras para prevenir el Fraude? *

Texto de respuesta larga

En general, de cada 100 casos de fraude electrónico, ¿cuantos cree usted que no se da una solución satisfactoria al tarjeta habiente afectado? *

Texto de respuesta corta

¿Cual cree que son los principales lugares donde hay facilidad para que se cometa fraude electrónico? *

- Gasolineras
- Restaurantes
- Hoteles
- Internet
- Otro...

¿En cuanto tiempo normalmente se da una resolución de problemas con relación al fraude para el tarjeta habiente? *

- Menos de 24 Horas
- Entre 24 y 48 horas
- Menos de una semana
- Mas de una semana.
- Otro...

Cuales son las medidas que deben tomar las instituciones para reducir los fraudes al tarjeta habiente. *

Texto de respuesta larga