DECANATO DE CIENCIAS ECONÓMICAS Y EMPRESARIALES
ESCUELA DE MERCADOTECNIA

Trabajo de Grado para Optar por el Título de Licenciatura en Mercadotecnia

Estrategias de Marketing, fraudes y publicidad engañosa en las redes sociales y páginas web en el sector de telecomunicaciones en República Dominicana desde el año 2014 hasta el 2015.

SUSTENTADO POR:

Charlie Enrique Pérez Acosta
2009-1582

ASESOR (A):

María Luisa Montás

Santo Domingo Distrito Nacional, República Dominicana
2016

Los conceptos expuestos en esta investigación, son de exclusiva responsabilidad del autor.

ESTRATEGIAS DE MARKETING, FRAUDES Y PUBLICIDAD ENGAÑOSA EN LAS REDES SOCIALES Y PAGINAS WEB EN EL SECTOR DE TELECOMUNICACIONES EN REPÚBLICA DOMINICANA DESDE EL AÑO 2014 HASTA EL 2015

ÍNDICE GENERAL

INDICE DE TABLAS E ILUSTRACIONES

TABLAS:

ILUSTRACIONES:

DEDICATORIA

A mis padres, Modesta Bienvenida Acosta Matos y Kilvio Francisco Pérez Borbón, por ser mis modelos a seguir y por haberme enseñado e inculcado valores morales y espirituales. Doy gracias a Dios por tenerlos, este logro no lo hubiese hecho sin el apoyo incondicional de ambos. ¡Los amo!

También se lo dedico a Dios, que siempre ha estado conmigo en las buenas y en las malas. Eres quien me guía en todo sendero, eres mi fortaleza, el que hace que cada día de lo mejor de mí. ¡Te doy gracias por todo mi Dios!

AGRADECIMIENTOS

A Jehová

Gracias a ti, mi Dios, por ser mí guía en cada momento y circunstancia. Eres la fuente que me da fortaleza para seguir adelante en busca de mis objetivos y metas. Tú eres el altísimo sobre todas las cosas y con tu ayuda, las cargas se hacen más ligeras.

A mis padres

Modesta Bienvenida Acosta Matos y Kilvio Francisco Pérez Borbón, por ser los responsables de mi formación como persona a lo largo de toda mi vida. Gracias por forjar en mí, una persona de bien para la sociedad y por inculcarme buenos valores. Les agradezco de corazón, todo lo que han hecho por mí, por cada consejo en los momentos más difíciles y por servir como fuente de inspiración para lograr lo que me propongo. También por esforzarse en ayudarme a seguir adelante, para desarrollarme en el ámbito personal y profesional. Sin ustedes no lo hubiese logrado. Los amo, ¡gracias por todo!

A mis hermanos

Por recibir un apoyo incondicional de todos ustedes. Mis logros los comparto con cada uno. ¡Gracias por todo su apoyo!

A mi novia

Gracias a ti Wilendy Rosario, por ser partícipe de esta meta. Agradezco tu colaboración y apoyo incondicional en cada momento. Con Dios por delante, juntos forjaremos muchos éxitos.

A mi prima Elizabeth Castro

Gracias por ofrecerme tu apoyo desde el principio, te agradezco los consejos y sugerencias que me has dado. Gracias a Dios, lo logramos.

A mis familiares

Gracias a Dios por tener una hermosa familia que me ha apoyado en cada momento, por ser personas ejemplos de superación y dedicación en todo contexto en el que cada uno de ustedes se desarrolla. Este logro lo comparto con todos ustedes.

Charlie Enrique Perez Acosta

INTRODUCCIÓN

Las actividades de comercialización de productos, bienes y servicios han desarrollado y dinamizado el comercio en todos los ámbitos. Actualmente las empresas están implementando estrategias para ingresar a nuevos segmentos de públicos a los que quieren hacer llegar sus bienes y servicios.

Los medios digitales están a la vanguardia en los últimos años. El marketing ha logrado introducirse en los medios digitales creando estrategias de promoción de ventas y captación de clientes potenciales que utilizan dichos medios para comunicarse con otras personas, buscar información, comprar productos, etc.
Esto es de provecho para las empresas ya que pueden lograr introducir publicidad en los laterales de las páginas web y redes sociales según las necesidades de los clientes. De manera que puede ser atractiva para lograr vender y distribuir bienes y servicios.

Esta investigación tiene como objetivo estudiar las distintas estrategias de marketing, fraudes y publicidad engañosa en los medios digitales en el sector de telecomunicaciones con el fin de identificar las los métodos utilizados para realizar este tipo de acciones.

En el primer capítulo se hablara del inicio, origen y aspectos generales de las telecomunicaciones. Esto es como fin de mencionar los primeros instrumentos utilizados en el mundo de las telecomunicaciones.

En el segundo capítulo se abordan los aspectos generales de las páginas web y las redes sociales en el sector de las telecomunicaciones en República Dominicana. Veremos el inicio de las páginas web y las redes sociales y sus tipos.

El tercer capítulo habla del origen del fraude electrónico y la publicidad engañosa. Veremos los softwares más utilizados para el robo de información y las diferentes estrategias utilizadas para persuadir a los usuarios.

Y por último, el cuarto capítulo que es el análisis de las estrategias de marketing, fraudes y publicidad engañosa en las páginas web y redes sociales en el sector de las telecomunicaciones. Se describirá la tendencia en que los usuarios suelen ser defraudados y a través de qué medios electrónicos.

CAPÍTULO I

LAS TELECOMUNICACIONES

1.1 Origen de las Telecomunicaciones

Desde los inicios de las civilizaciones, la comunicación entre los individuos ha logrado evolucionar a través de búsqueda de nuevos métodos y técnicas utilizadas en distintos contextos, que de tal forma, se han originado diferentes maneras de comunicarse a corta y larga distancia para enviar y recibir mensajes.

El hombre ha buscado la forma de comunicarse por medio de situaciones que ameritan remitir un mensaje a larga distancia como es el caso de las guerras, el comercio, tratados diplomáticos entre gobiernos o civilizaciones, entre otros casos. De esta forma, el mensaje se ha desarrollado y ha logrado jugar un papel importante en la historia de la humanidad.

Las primeras civilizaciones como la romana, persa y la egipcia utilizaban mensajeros que se trasladaban a grandes distancias para enviar y recibir informaciones a través de escritos en papiro. Esto agilizaba la recepción de mensajes y a la vez podían lograr tener mejor control de todos sus territorios.

Hacia el año de 1200 a.C. ya el hombre se valió de señales con fuegos para transmitir mensajes a distancia. En la Ilíana se alude al uso de hogueras en las costas griegas, para anunciar la llegada de la flota amiga en ayuda de los sitiados. Se hicieron señales de fuego de montaña a montaña y desde torre a torre. (Szymanczyk, 2013, pág. 17)

Más adelante, surgieron otras formas de comunicación a larga distancia que se practicaban en lugares altos para transmitir informaciones a través de movimientos con los brazos y señales con humo y fuego. Luego en América y África se utilizaban tambores e instrumentos para emitir sonidos desde lugares altos como montañas y árboles.

Para el siglo IV a.C. se desarrolló el telégrafo hidráulico por el señor Eneas el Táctico. Este consistía en un sistema que estaba compuesto por dos contenedores llenos de agua y una varilla dentro del mismo. Para emitir el mensaje se alertaba al receptor con una antorcha para indicar que se quería realizar un llamado. Ambos abrían o tapaban los envases según las distintas señales de fuegos emitidas.

Al año de 150 a.C. había cerca de 3,000 telégrafos de agua, sistema dispuesto alrededor del vasto Imperio Romano. El historiador griego Polybios (200-118 a.C. señalo que este sistema fue utilizado de Silicia hasta Cartago, durante la primera Guerra Púnica, 264-241 AC. (Szymanczyk, 2013, pág. 20)

Por consiguiente, luego de la etapa anterior se diseñó el telégrafo óptico, el cual fue el primer sistema moderno de telecomunicación. A través de este, se podía transmitir mensajes cortos. Su estructura constaba de brazos móviles, con poleas que lograban tener distintas posiciones y de esta forma se lograba emitir un mensaje hacia un destinatario especifico. Este sistema se tomaba en transmitir la información de 2 a 6 minutos, pero para decodificar el mensaje se

tomaba tiempo. Sin embargo, durante la Revolución francesa el ingeniero Claude Chappe instaló 556 telégrafos ópticos junto a sus hermanos. Este fue un gran hecho mediante el cual Francia tuvo la oportunidad de emitir mensajes que cubrían más de 4000 kilómetros. Como consecuencia, se logró transmitir la victoria francesa de la reconquista de la región Condé-sur-I´Escaut.

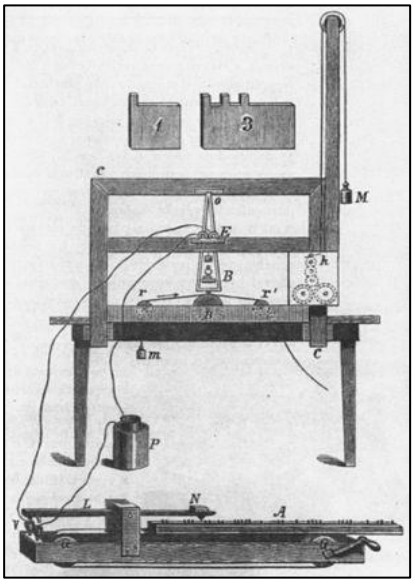
Este instrumento fue propagándose en toda Europa, cada país realizaba modificaciones de acuerdo a sus necesidades y fines de uso. Fueron utilizados en torres, en lugares altos, en las guerras, el comercio, entre otras actividades. Fue un instrumento que revolucionó las telecomunicaciones y que fue el impulso para desarrollar y utilizar nuevas tecnologías con el fin de que la comunicación sea más eficiente.

Un sistema más avanzado, utilizado en el siglo XIX, fue el **telégrafo eléctrico** que fue desarrollado posteriormente al descubrimiento de la electricidad por el científico Stephen Gray en el 1729. Este sistema dio un giro a las telecomunicaciones ya que dicho telégrafo emitía señales eléctricas que se transmitían a través de cables metálicos. Reemplazó los anteriores sistemas de transmisión de mensajes ópticos, por lo tanto, se convirtió en una buena opción a la hora de emitir un mensaje a través de este dispositivo eléctrico.

Según expresa (Figueiras, 2002)

El **telégrafo** usaba cinco hilos conductores y uno de vuelta, y la corriente de cada hilo activaba una aguja de modo que, con un código simple de pares y una presentación visual, quedaba identificada la letra o número. Este telégrafo, basado en el de Schilling pero cuyo terminal receptor era más práctico, seguía teniendo un grave inconveniente: el coste de la línea, que era de 165 libras por milla, lo cual retraía a los inversores.

Ilustración 1. El Telégrafo



Fuente: https://es.wikipedia.org/wiki/Tel%C3%A9grafo

Rápidamente simplificaron el número de hilos y de agujas estableciendo un código visual registrado en el aparato receptor y haciendo uso de la desviación a izquierda o a derecha de las agujas según el sentido de la corriente. Así pudieron construir telégrafos de dos agujas y tres hilos, y de una aguja y dos hilos, lo cual reducía el coste drásticamente a costa de un manejo algo más experto para los telegrafistas y permitía la instalación rentable de un servicio telegráfico (p.38).

Un gran avance fue el invento del **teléfono** en el siglo XIX, este medio de comunicación es muy utilizado hoy en día. A través de este medio, se logra escuchar la voz en tiempo real, de modo que las informaciones y los mensajes llegan más rápido al receptor. Por lo tanto, este instrumento es capaz de enlazar

una voz a distancia y permitió mejorar la comunicación, ya que agilizaba los procesos de negociación entre empresas, también muy utilizado en las guerras.

El teléfono apareció en 1876. No cambia profundamente el equilibrio de las comunicaciones, en la medida en que no es posible desarrollar, en los primeros años, más que redes urbanas, y que la tecnología de las líneas de larga distancia es todavía precaria. (Frederic Barbier, 2007, pág. 168)

Otro invento que realizo un aporte a las telecomunicaciones es **la radio**, que es un instrumento de comunicación masiva y a su vez transmite información, música y noticias que tiene una gran cobertura y puede llegar a muchas personas.

La idea de la radio nació, seguramente, en 1837, cuando Samuel F. Morse transmitió su primer telegrama a través de la primera línea telegráfica. Lograr un medio, que sin necesidad de línea –de hilos y postes- permitiera la comunicación, pudo ser una idea, casi mejor, un sueño… Un sueño que se hizo real cuando, en código Morse, los radiogramas cruzaron el espacio. Por eso es que la radio, en sus comienzos, fue conocida como la **telegrafía sin hilos (TSH).** (Gustavo Docampo Otero, 2000, pág. 3)

Por otro lado, la **televisión** es un dispositivo que emite imágenes con sonido y movimiento que se efectúa a través de ondas de radio. Según (Gomez, 2015) La televisión nació después de darse una serie de inventos y fenómenos simultáneos, pero que se desarrollan de forma individual. En siglo XIX varios

investigadores empezaron a experimentar con la transmisión de imágenes por medio de ondas electromagnéticas. Los que hicieron avances más importantes, fueron el ingeniero alemán Paul Nipkow; el escoces John Logie Baird, quien desarrollo y perfecciono el disco de Nipkow en 1923 a base de células de selenio; A los norteamericanos Ives y Jenkis, los que basándose en Nipkow consiguieron avanzar bastante; y al ruso Vladimir Sworykin, quien gestiono el tubo Inoscopio.

1.2 Definición

Según (Isaac Alfonso Devis Granados, 2008) el Decreto 1900 establece un concepto sobre **telecomunicaciones**, y en su artículo 2 lo define como: “Toda emisión, transmisión o recepción de señales, escritura, imágenes, signos, datos o información de cualquier naturaleza, por hilo, radio, u otros sistemas ópticos o electromagnéticos” (p.39).

También (153-98, 1998, pág. 5) la define como la transmisión y recepción de señales por cualquier medio electromagnético.

Además, (Hiddekel Morrison, 2005) muestra un concepto de que las telecomunicaciones son la emisión, transmisión o recepción de toda clase de señal, signos, imágenes, sonido o información por alambre, el aire, por medios ópticos, etc.

Sin embargo, (Constantino Perez Vega, 2007) dice que la Ingeniera de telecomunicación o ingeniería de comunicaciones es la rama de la ingeniería que se ocupa de la generación, transmisión, recepción y procesado de señales ya sea por medios eléctricos, electromagnéticos, electroacústicos, ópticos, etc., y los sistemas de telecomunicación son aquellos que mediante el empleo de técnicas y dispositivos adecuados realizan el transporte de información entre una fuente y uno o más destinatarios finales (p.1).

1.3 Características

Las telecomunicaciones se caracterizan por su diversidad, por su influencia e innovación. Por lo tanto, han realizado grandes aportes a la tecnología y al avance de la sociedad. A continuación veremos algunas de las principales características según (Perez, 2004):

Las mejores características de las redes modernas de telecomunicaciones, también permiten la introducción de una serie de novedosos y benéficos servicios que han probado ser de vital importancia para elevar la productividad y disminuir los costos de producción de gran cantidad de negocios relacionados con la actividad económica, social y política de los diferentes países. Esto hace, consecuentemente, que las telecomunicaciones, en su contexto de sistemas moderno, ocupen un lugar preponderante en el desarrollo integral de las naciones (p.9).

Por lo tanto, contribuido a desarrollar distintos sectores económicos, contribuyendo a mejorar los servicios, la producción, interacción con los usuarios de telefónicas e internet. Por consiguiente, las telecomunicaciones son de mucha importancia porque:

- ✓ Tienen una gran influencia y es aceptada por diversos niveles de la sociedad.
- ✓ Está relacionada con la Internet.
- ✓ Forma parte de los medios de comunicación.
- ✓ Realiza aportes a la informática.
- ✓ Mejora los servicios de comunicación a distancia.

Además, cada día surgen nuevas novedades en este sector que al mundo globalizado lo mantiene a la vanguardia creando nuevas estrategias de comunicación e interconectando millones de personas.

1.4 Origen de las Telecomunicaciones en República Dominicana

El sector de las telecomunicaciones en República Dominicana ha logrado convertirse en un sector muy importante, ya que es una fuente que ha generado muchos ingresos y a la vez aumentado la empleomanía. Por lo tanto, existen distintas compañías que en los últimos años se han instalado Rep. Dom. Para ofrecer una variedad de servicios que diversifica la interacción de los usuarios con personas a nivel local e internacional.

De esta forma, dicho sector ha aumentado la capacidad de comunicación a través de distintos canales de información como la televisión, el Internet, la comunicación telefónica, los celulares, entre otros medios que son utilizados como vía de comunicación y a la vez ofrecen oportunidades de inversión en proyectos empresariales, con el fin de garantizar el dinamismo de la economía.

Para los años 1884, empezó a surgir los primeros pasos para el ingreso de las telecomunicaciones en República Dominicana. Todo se originó cuando el Poder Ejecutivo lanzó un Decreto para ingresar el Sistema Perfeccionado de centrales telefónicas de Nason.

El 17 de Mayo de 1884 durante el mandato presidencia del general Ulises Heureaux es que el Congreso Nacional aprueba una concesión que se convirtió en realidad el **telégrafo** en la República Dominicana. (Hiddekel Morrison, Las Telecomunicaciones en Republica Dominicana, 2005, pág. 37)

Más adelante, se publicó el primer Directorio Telefónico en el año 1907, con el fin de que los usuarios puedan tener libre acceso a los directorios telefónicos para lograr establecer comunicación con terceros.

En el 1902 se empezó a instalar la primera línea telefónica, que logró comunicar Santo Domingo con San Pedro de Macorís, Guerra, entre otros. Luego el 11 de

Noviembre del 1930 se fundó la Compañía Dominicana de Teléfonos (CODETEL). Su primera instalación e inicio de sus operaciones fue en San Pedro de Macorís. Esta compañía dio inicio a una amplia red de servicios telefónicos logrando posicionarse como la número uno de las compañías que más adelante se establecieron en Rep. Dom.

Según expresa (INDOTEL, 2015) en su página web:

"En Enero de 1931, la Compañía Dominicana de Teléfonos (CODETEL) había comprado a los señores Manuel de Jesús Troncoso T. y a Eduardo Winter la Empresa Telefónica de San Pedro de Macorís.

El 27 de marzo de 1931 el Presidente de la República, Rafael L. Trujillo, promulgo la ley Núm. 104, mediante el cual el Congreso Nacional autoriza al Poder Ejecutivo a vender pura y simplemente o bajo condición y grado a grado como lo estime necesario el sistema de teléfonos automáticos de la ciudad de Santo Domingo y el sistema de líneas telefónicas y telegráficas interurbanas actualmente existentes en el país, ambos sistemas bajo la propiedad del Estado, siempre que el Gobierno conserve el control de las comunicaciones telegráficas en la República."

Otro dato importante es la introducción de la **Radio**, que también se popularizó e hizo grandes aportes a las telecomunicaciones. Según expresa (Veras, 2010):

Después de la mitad del decenio de los años 20 (en 1926) inquietos dominicanos incursionaron a manera de afición en la Radio. Fue entonces cuando el ingeniero Frank Hatton Guerrero como Presidente del Radio Club de Santo Domingo, construye un pequeño transmisor de Amplitud Modulada (AM) de pocos vatios para crear lo que sería la primera señal de broadcasting del país. Hatton y sus amigos jamás imaginaron lo que la radio fusión significaría desde ese momento no solo para la Rep. Dom. Sino, para el resto del mundo.

Luego, en el año 1968 se realizó la instalación del cable submarino. Anteriormente se habían iniciado los estudios correspondientes para evaluar cómo realizar la instalación de dicho cable que llegaría a Saint Thomas a una distancia de 648 kilómetros. Más adelante, (Piantini, 2011) dice que el 21 de julio de 1975 se inaugura la Estación Satélite de Cambita – San Cristóbal (105 pies de diámetro o 32 metros) para incorporar a República Dominicana a la Red Mundial de Telecomunicaciones captando los mensajes enviados desde diferentes puntos del mundo al satélite Intersat IV localizado sobre las aguas del Atlántico permitiendo los servicios de voz y televisión.

Se inicia la instalación del teléfono público inalámbrico a finales del 1987, exclusivamente en lugares arcaicos y lejanos, en tal sentido la Rep. Dom. Fue considerado como uno de los países principiantes en desarrollar este sistema. De modo que fue un gran avance, porque este sistema logro conectar distintos puntos del país, garantizando la comunicación a larga distancia. Posteriormente,

en 1988 sale al mercado el servicio de Beeper que consistía en recibir mensajes de textos y de voz entre usuarios.

Más adelante, en el año 1995 se introdujo la **Internet** que contaba con el servicio Dial Up el cual era prestado por las empresas de TRICOM y CODETEL. En efecto, estas empresas emplearon una gran gama de servicios para desarrollar la conectividad entre usuarios y diversificando las velocidades de Internet con el fin de brindar un servicio de calidad y tener mayor participación de mercado.

Dos años después en 1997, comenzó la circulación del Servicio Personal de Comunicación (PCS Digital), que otorgaba un mejor funcionamiento a los teléfonos celulares. Este servicio, fue de mucha importancia porque incursiono en la incorporación del Internet en los celulares, recepción de mensajes de voz, ID de llamadas, entre otros beneficios.

Sobre la Ley General de Telecomunicaciones No. 153 – 98, (INDOTEL, 2015) informa que ha sido redactada acorde a los convenios y tratados internacionales firmados y ratificados por el país, donde se enmarcan los principios de continuidad, generalidad, igualdad y neutralidad que hoy la complementan y se caracteriza por establecer, de forma expresa, el interés del estado de garantizar un servicio de telecomunicaciones eficiente, moderno y de costo razonable, a todos los habitantes de la República Dominicana bajo un esquema de competencia leal, efectiva y sostenible, a ser seguido por aquellos que provean dicho servicio.

Posteriormente, se introdujo la Tecnología Celular de Tercera Generación (3G) y Tecnología de Banda Ancha, que juntas contribuyeron al desarrollo y facilidad de los servicios telefónicos e Internet móvil. Por lo tanto, el desarrollo de las telecomunicaciones en Rep. Dom. Han contribuido al crecimiento de diversos sectores empresariales y en la población, porque a través de estos avances hay más acceso a la información, al desarrollo industrial, mejora de servicios, eficiencia en los procesos y creación de nuevas empresas.

1.5 Marco Legal de las Telecomunicaciones en República Dominicana

Según explica (Heredia, 2010):

La República Dominicana ha tenido una evolución particular en materia de telecomunicaciones. Históricamente las telecomunicaciones en esta nación se han desarrollado en manos del capital privado desde su origen, a diferencia de lo ocurrido en la mayoría de los países, donde originalmente este servicio era ofrecido por el Estado como un servicio público.

Desde 1930 y hasta 1990, la Compañía Dominicana de Teléfonos, C. por A., CODETEL, era la única empresa en ofrecer servicios de telefonía en el país. En ese momento hace presencia en el mercado una segunda empresa, conocida como TRICOM.

Posteriormente, y como fruto de un proyecto auspiciado por el Banco Mundial y la Unión Internacional de las Telecomunicaciones, el 27 de mayo de 1998, se promulga la Ley General de Telecomunicaciones, No. 153-98, que constituye el marco regulatorio básico del sector de las telecomunicaciones en la República Dominicana.

El capítulo II, en el artículo No.2 de la Ley General de Telecomunicaciones, No. 153-98 hace referencia (INDOTEL, Instituto Dominicano de las Telecomunicaciones, 2015) que la presente ley constituye el marco regulatorio básico que se ha de aplicar en todo el territorio nacional, para regular la instalación, mantenimiento y operación de redes, la prestación de servicios y la provisión de equipos de telecomunicaciones. La misma deberá ser interpretada de conformidad con los convenios internacionales ratificados por la Republica Dominicana y se complementara con los reglamentos dictados por las autoridades competentes (p. 6).

Sin embargo, esta ley es de gran alcance y tiene facultad para regular e intervenir en todos los sectores de telecomunicaciones. Es la ley competente que se encarga de depurar a los organismos que ofrecen servicios de telecomunicaciones y de tal forma establece parámetros para la protección de los usuarios.

1.5.1 Ley General de Telecomunicaciones No. 153-98 de la República Dominicana

Según expresa (Herrera, 2012):

Esta legislación liberaliza y moderniza las medidas de regulación del sector, adaptándolas a los parámetros establecidos en el área por organismos internacionales tales como la Organización Mundial de Comercio (OMC) y la Unión Internacional de Telecomunicaciones (UIT), a fin de reforzar el auge que ha estado experimentado este sector en el país desde la década de los ‘80 y de insertar a la nación dominicana dentro del proceso de liberalización del comercio de bienes y servicios de telecomunicaciones que se ha estado produciendo a nivel mundial desde mediados de la década de los ’90 (p.1).

Por otro lado, dentro del ámbito de aplicación (Herrera, 2012) dice que la Ley 153-98 regula en su totalidad el sector de las telecomunicaciones, definidas como “la transmisión y recepción de señales por cualquier medio electromagnético”. Por ende, no se aplica a los demás medios de comunicación, tales como la prensa, sino a la transmisión de palabras, sonidos, imágenes o información por medio de señales o impulsos electromagnéticos, lo cual incluye los servicios de teléfono, radio, televisión, televisión por cable y satélite, facsímil, teléfonos celulares y transmisión digital de información.

Asimismo, la ley se aplica tanto a la prestación de los referidos servicios como a la comercialización de bienes y equipos relacionados con los mismos.

Finalmente, cabe señalar que el Estado tiene interés en regular las telecomunicaciones desde diversos puntos de vista. En primer lugar, en su calidad de servicio público, para garantizar la prestación eficaz e igualitaria del mismo a toda la población; en segundo lugar, en su calidad de actividad económica, para promover el desarrollo del sector y de regular la interactuación de los participantes en el mercado; y finalmente en su calidad de medio de transmisión de información, para proteger y regular en ciertos casos el contenido de la misma y velar por el respeto de los derechos de propiedad intelectual de los creadores de dicha información.

La Ley 153-98 regula principalmente los aspectos públicos, económicos y técnicos del sector, y no aquellos relacionados con la transmisión de información, lo cual es de la competencia de otras leyes que se aplican a los medios de comunicación en general, incluyendo las telecomunicaciones.

1.5.2 Objetivos de la Ley General de Telecomunicaciones No. 153-98

Según explica (Herrera, 2012)

La Ley 153-98 regula el comercio de bienes y servicios en el sector con la finalidad general de fomentar el desarrollo de las telecomunicaciones y de garantizar la prestación de un servicio eficiente, moderno y a costo razonable para contribuir así a la expansión socioeconómica de la nación. Con miras al logro de dicho objetivo general, la ley persigue el logro de los siguientes objetivos específicos (Art. 3):

a) Establecer el principio de la libertad de prestación de servicios de telecomunicaciones, incluida la libertad de construcción y operación de sistemas y facilidades;

b) Regular el sector de las telecomunicaciones y promover la libre competencia en el mismo, a fin de mejorar la oferta de telecomunicaciones en términos de precios, calidad de servicio e innovación tecnológica;

c) Reafirmar el principio del servicio universal y garantizar que los servicios de telecomunicaciones sean accesibles a toda la población, de conformidad con los principios de continuidad, generalidad, igualdad y neutralidad de dichos servicios;

d) Adaptar la industria de telecomunicaciones local a los niveles de apertura y a las normas técnicas adoptadas por los organismos internacionales de los cuales

forma parte la República Dominicana, especialmente a las recomendaciones de la Organización Mundial de Comercio y la Unión Internacional de Telecomunicaciones;

e) Asegurar el ejercicio efectivo e imparcial de la función reguladora del Estado mediante la creación de un organismo regulador independiente y el establecimiento de procedimientos públicos y transparentes; y,

f) Garantizar la administración y el uso eficiente del dominio público del espectro radioeléctrico (p.7).

1.5.3 Organismo que regula la Ley de Telecomunicaciones

La Ley 153-98 dispone la creación del Instituto Dominicano de Telecomunicaciones (INDOTEL), el cual tiene como función la regulación del Estado en el área de las telecomunicaciones, por lo que tiene la misión de regular y supervisar el comercio de bienes y la prestación de servicios en el sector y de velar por la aplicación de las disposiciones de la ley.

Papel de INDOTEL dentro del nuevo marco regulatorio

A partir de la entrada en vigencia de la referida ley, la prestación de servicios de telecomunicaciones está sujeta a las disposiciones de la ley, así como al reglamento de aplicación de la misma que deberá dictar el Poder Ejecutivo y a los reglamentos que dicte INDOTEL en las áreas de su competencia.

La legislación otorga al organismo regulador un papel esencial de regulación, supervisión y arbitrio en el sector, otorgándole amplios poderes y facultades a fin de permitirle cumplir con sus objetivos, los cuales son los siguientes (Art. 77):

a) Promover el desarrollo de las telecomunicaciones, implementando el principio de servicio universal;

b) Promover la existencia de una competencia sostenible, leal y efectiva en la prestación de servicios públicos de telecomunicaciones;

c) Defender y hacer efectivos los derechos de los clientes, usuarios y prestadores de dichos servicios; y

d) Velar por el uso eficiente del dominio público del espectro radioeléctrico.

Poderes y atribuciones

La ley otorga a INDOTEL todos los poderes necesarios para que este organismo pueda cumplir con su función reguladora, facultándolo para establecer, a través reglamentos de carácter general, las normas técnicas que regirán a la industria de telecomunicaciones en todo el territorio nacional, así como para tomar todas las medidas administrativas y las decisiones de alcance particular que sean necesarias para cumplir con las disposiciones de la ley (p.7).

CAPÍTULO II

ASPECTOS GENERALES DE LAS PÁGINAS WEB Y REDES SOCIALES EN EL SECTOR DE TELECOMUNICACIONES

2.1 Antecedentes históricos de las páginas web y redes sociales.

Para hablar del origen de las páginas web y redes sociales, debemos tomar en cuenta algunos datos que dieron origen a la Internet, que son de gran importancia para entender sus orígenes y evolución. A continuación veremos los aspectos generales de ambas.

2.1.1 Origen del Internet

Según (Angel Ibeas Portilla, 2000)

Los orígenes de Internet se remontan a la Guerra Fría, en plena escalada atómica entre los bloques militares de URSS y EE.UU. Los gobernantes estadounidenses decidieron crear una red informática que abarcase toda la nación y que fuese muy segura. El conjunto de la red debía soportar el ataque a cualquiera de sus ordenadores o a cualquiera de sus líneas. Así comenzó a funcionar una red descentralizada, que inicialmente tenía utilidades militares y gubernativas. Luego se fueron añadiendo conexiones con centros de investigación, universidades, empresas…

El embrión de Internet fue una red denominada ARPANET. El ejercito de los EE. UU. Precisaba un sistema de comunicaciones que funcionara en caso de ataque enemigo, aun cuando fuesen destruidos algunos de los ordenadores y líneas que formaban parte de esa red. Frente a aquella necesidad, la Advanced Research

Projects Agency (ARPA) diseño un sistema según el cual los ordenadores no se conectaban por una ruta única, sino que disponían de diversas rutas por las que alternar las comunicaciones en función de los recursos disponibles.

Por otro lado (Mora, 2002, págs. 5 - 6) expresa:

El desarrollo de Internet, como casi todos los avances de la ciencia y tecnología no se debe a una persona o a un grupo pequeño de personas, sino que ha sido fruto de las ideas y del trabajo de miles de personas. Sin embargo, en un repaso de la historia de Internet de unas pocas páginas solo se pueden nombrar a las personas más importantes.

Como reconocimiento al cambio que Internet ha producido en todos los niveles de la sociedad, el 23 de mayo de 2002, Lawrence Roberts, Robert Kahn, Vinton Cerf y Tim Berners-Lee fueron distinguidos con el Premio Príncipe de Asturias de Investigación Científica y Técnica en representación de las “miles de personas y muchas instituciones” que han hecho posible este avance de nuestro tiempo. Según la resolución del jurado, “Se les otorga el premio por haber diseñado y realizado un sistema que está cambiando el mundo al ofrecer posibilidades antes impensables para el progreso científico y social”.

A Lawrence (Larry) Roberts se le puede llamar “el padre de Internet”, porque fue el director del equipo de ingenieros que crearon ARPANET, el precursor de la

actual Internet. A parte de ser el director, también fue el diseñador principal de ARPANET (pag.6).

Así, en 1969 se estableció ARPANET, la primera red sin nodos centrales, de la que formaban parte cuatro universidades estadounidenses: Universidad de California Los Ángeles (UCLA), Universidad de California Santa Bárbara (UCSB), Universidad de Utah y Stanford Research Institute (SRI). La primera transmisión tuvo lugar el 29 de octubre de 1969, entre UCLA y SRI. (Aranda, 2004)

Sin embargo, en el año 1990 desaparece ARPANET y más adelante se crea la **Internet** con un concepto de carácter público y que va dirigido al sector industrial, militar, científico y académico.

Por lo tanto, la Internet es un conjunto de ordenadores o computadoras conectadas entre sí, a través de una red. Con el fin de compartir información a través de correos electrónicos u otros medios desde cualquier parte del mundo.

Este es un medio que ha revolucionado el mundo de las telecomunicaciones, porque a través de este, todos los países están interconectados. Además, compartiendo y enviando informaciones según los intereses de los usuarios que utilizan este servicio.

Además, en 1990 Tim Berners-Lee comienza a desarrollar un editor y navegador grafico de hipertexto para **NeXTStep**, el sistema operativo con entorno grafico de los ordenadores NeXT. Elige **WorldWideWeb** como nombre del programa y "World Wide Web" como nombre del proyecto, después de descartar una serie de nombres: *Information Mesh, Mine of Information e Information Mine.* (Mora, 2002, pág. 17)

Sin ninguna duda, este es el servicio estrella en Internet, y el que ha conseguido la explosión de nuevos usuarios de estos últimos años. La información que contiene se encuentra, básicamente, en formato HTML (HiperText Markup Language) recuperable en red mediante el Protocolo de Transferencia de HiperTexto (HTTP). (Angel Ibeas Portilla, 2000, pág. 29)

2.1.2 Generaciones de los sitios Web

Primera generación

Según (Mora, 2002)

La primera generación abarca desde el nacimiento de la Web (1992) hasta mediados de 1994. La creación de páginas web durante esta generación se ve limitada por diversas razones tecnológicas: ancho de banda limitado (módems de 2.4 Kbps), navegadores poco desarrollados, monitores monocromos, etc.

Las características principales de estas páginas son:

- Tiempo de carga rápido: son paginas basadas en texto, con muy pocas imágenes y ningún recurso multimedia.
- Navegación poco estructurada, con falta de coherencia.
- Paginas largas, que parece que nunca se acaban. La información no se suele organizar en varias páginas, ya que así se reduce el número de transferencias.
- Texto escrito como si fuera una hoja de papel: de lado a lado de la página y desde el principio hasta el final.
- Empleo de saltos de línea como separadores.
- Empleo de líneas horizontales para separar secciones en una misma página.
- Empleo de listas para organizar la información.
- Poco uso de los enlaces entre páginas de un mismo sitio web.
- Como las paginas son muy largas, se emplean muchos enlaces intradocumentales.
- Listas interminables de enlaces a otros sitios web.
- Se pueden visualizar correctamente casi en cualquier navegador (incluso los navegadores no gráficos), pero son aburridas y poco legibles.
- Las páginas web poseen un contenido educativo o científico. Pocas empresas poseen un sitio web.

En definitiva, durante este primer periodo, se emplea la Web como si fuera uno de los medios de comunicación tradicionales (libros, revistas, etc.). Aun no se sabe cómo aprovechar todas las posibilidades que ofrece la Web (p.26).

Segunda Generación

La segunda generación se extiende desde 1995 hasta la actualidad. La diferencia principal con las páginas web de la generación anterior es la masiva incorporación de elementos gráficos en las páginas web:

- Los iconos sustituyen a las palabras.
- El color de fondo se sustituye por una imagen de fondo.
- Los banners sustituyen a los encabezados de las páginas.
- Las listas normales se sustituyen por listas con topos (bullets) gráficos.

Sus características principales son:

- Tiempo de carga lento: se emplean imágenes con multitud de colores y animaciones en exceso, debido a la novedad de su uso. No se comprueba el rendimiento de las páginas con conexiones lentas: no se tiene en cuenta al usuario final.
- El color de fondo de las páginas deja de ser el blanco o el gris. Incluso, se emplean imágenes como fondo de las páginas.
- Empleo de tablas, aunque no con el propósito de situar el contenido (tablas invisibles), sino para mostrar datos tabulados.
- Las páginas todavía poseen una estructura de arriba abajo.

- La navegación suele ser jerárquica, a partir de una página principal. Sin embargo, no existe una filosofía de planificación de la navegación.
- Aparecen tecnologías multimedia propietarias, que necesitan la instalación de un *plug-in* para su visualización. Prima el uso de tecnologías (imágenes y sonidos), aunque luego el público no pueda visualizar correctamente las páginas.

En definitiva, las páginas web de esta generación se caracterizan porque prima el uso de la tecnología, sin tener en cuenta el propósito del sitio web. Además, no se tiene en cuenta la legibilidad o claridad de la presentación de la información (p.28).

2.2 Conceptos y principios generales

Esta investigación hace referencia a varios conceptos claves, relacionados con el origen del Internet y las páginas Web que son utilizados en estas aplicaciones y que cumplen una función específica. De tal modo, han contribuido al desarrollo de la Internet y las telecomunicaciones.

- **Dirección IP:** Es una convención numérica para identificar unívocamente cada equipo conectado a una red que emplea el protocolo IP. La dirección identifica al equipo en su red. La definición inicial del protocolo (protocolo IPv4) definió las direcciones IP como una secuencia de cuatro dígitos, de 8 bits cada uno. (Miguel Moro Vallina, 2014, pág. 8)

- **Protocolo TCP/IP:** Esta es la denominación que recibe una familia compuesta por varios protocolos de comunicación utilizados por diferentes servicios de Internet. (Angel Ibeas Portilla, 2000, pág. 22)

- **Explorador Web:** Es un programa que nos permite ver documentos escritos en lenguaje HTLM. Estos documentos son páginas Web. (Salinas, 2003, pág. 5)

- **Web 1.0 y 2.0:** Básicamente, si la web 1.0 era la red de los datos, la 2.0 es la de las personas. Se podría definir también a la web 2.0 como "la red convertida en un espacio social, con cabida para todos los agentes sociales, capaz de dar soporte y formar parte de una verdadera sociedad de la información, la comunicación y/o el conocimiento". (Sánchez-Ocaña, pág. 12)

- **Intranet:** Es una red de comunicaciones que emplea los protocolos TCP/IP para intercambiar información, o compartir funcionalidades, recursos, aplicaciones, etcétera, en el seno de una organización (una empresa, una institución, una universidad, un centro de investigación,…). (Miguel Moro Vallina, 2014, pág. 18)

- **Fibra Óptica:** Es un medio de transmisión flexible y transparente, fabricado con vidrio o materiales plásticos, que se emplea para transportar ondas luminosas. El medio posee un materia en su interior y otro que lo recubre, ambos transparentes; el exterior posee un índice de reflexión algo más bajo, haciendo que el haz de la luz se refleje completamente y

quede confiando en el interior del medio, que funciona así como una guía de ondas. (Miguel Moro Vallina, 2014, pág. 12)

2.3 Tipos de páginas web

Existen diversos tipos de páginas web que se diferencian de sus características, fines, funciones y objetivos según al público al que van dirigidos. Esto quiere decir que hoy en día todo usuario o navegador en Internet, tiene opción a ingresar a diferentes páginas en busca de información, entretenimiento, noticias, redes sociales, etc.

Sin embargo, en esta sección hace referencia a los tipos de páginas web según su función y objetivos. Esto es con el objetivo de ir ambientando el tema de investigación, que va dirigido a las estrategias de marketing utilizadas por empresas que se dedican al robo de información y al fraude y publicidad engañosa en las redes sociales y páginas web en el sector de telecomunicaciones. Antes que nada, esta indagación hace hincapié en sus orígenes.

Existen diferentes tipos de páginas web según sus características, contenidos y complejidad. Según (Saavedra, 2009) se clasifican en distintas clases:

Según la forma en que se actualiza el contenido:

- **Estático:** cuando la actualización del contenido es hecha manualmente.
- **Dinámico:** cuando un programa, con la ayuda de una base de datos, cambia el contenido en forma automática, sin intervención de nadie.

Según la complejidad y cantidad de información publicada:

- **Personales:** son las páginas de Internet creadas por personas naturales en servicios gratuitos de publicación de sitios web (como GooglePages o Geocities).
- **Corporativas:** sitios web generalmente de compañías que buscan promocionar sus productos o servicios.
- **Portales:** son complejas páginas de Internet especializadas en ciertos temas en particular. Se caracterizan por ofrecer contenido de interés a grupos específicos de personas. Usualmente requieren de un registro previo para poder descargar todo su contenido.

Según la forma en que los usuarios utilizan el sitio web:

- **Informativos:** cuando el flujo de información solamente se da desde el sitio web a los usuarios (no en sentido contrario).
- **Interactivos:** cuando el flujo de información en ambos sentidos, es decir, los usuarios no solamente reciben información del sitio web, sino que también pueden enviar su propia información al sitio web o a otros usuarios.

2.3.1 Tipos de sitios web

Existen una gran cantidad de sitios web que comúnmente tienen una particularidad que los diferencia uno de otros. Dentro de sus clasificaciones, estos van dirigidos a un público en específico, satisfaciendo sus necesidades de acuerdo al contenido de dichos sitios web. Algunos sitios web son:

- **Sitios de Comercio Electrónico:** Estos sitios son destinados para la venta y compra de bienes y servicios. Un ejemplo de esto es Amazon.com, Ebay.com, etc.

- **Blogs:** Estos sitios son utilizados para introducir artículos por autores y a la vez generar o recibir comentarios de los lectores. Normalmente existen páginas en las que se pueden crear blogs como Google, Wordpress, Blogger, entre otras.

- **Sitios web para descargas:** A través de estas páginas, los usuarios pueden acceder a las informaciones publicadas y al mismo tiempo descargar todo tipo de aplicaciones, juegos, películas, imagen y contenido de importancia según el contenido que se dedique a publicar la página.

- **Sitios web institucionales:** Estos sitios son diseñados por una entidad, a través de este dan a conocer los servicios que ofrecen, su misión, visión, valores e historia. También brindan información de libre acceso para los ciudadanos de un país.

- **Sitios web educativos:** Estos sitios ofrecen información educativa a los usuarios que acceden al mismo. También ofrecen cursos virtuales, realizan convocatorias para cursos presenciales, archivos e información para descargar, entre otras informaciones.

- **Sitios de noticias:** Estos ofrecen información de noticias acontecidas en un lugar determinado con el fin de mantener informado a los usuarios de la actualidad en el mundo y en la sociedad.

- **Sitios de juegos:** Es un sitio de entretenimiento que ofrece una gran variedad de juegos que se pueden descargar o jugar online.

- **Sitios religiosos:** Dirigido a aquellas personas que desean mantenerse informados sobre una religión en específica y a la vez buscar y leer artículos de interés religioso.

Estos son algunos de los diferentes sitios web que existen en la Internet y que los usuarios tienen libre acceso a estos lugares para obtener la información que desean. Por consiguiente, la web ha evolucionado a través del tiempo ofreciendo más contenido y variedad a los usuarios, también es un medio mediante el cual se ha desarrollado el marketing, descubriendo nuevas necesidades de los consumidores y creando nuevos servicios para generar rentabilidad.

2.4 Origen de las Redes Sociales

Las redes sociales son un instrumento de comunicación que hoy en día es utilizado por millones de personas en todo el mundo. Han contribuido con el avance de la comunicación entre personas a larga distancia, las empresas dan a conocer sus bienes y servicios que ofrecen al público al que van dirigido, los artistas han logrado tener más contacto con sus fanáticos y a través de estos medios logran detectar las necesidades de su público. También, son un buen terreno para pequeñas y medianas empresas que inician a comercializar sus productos y a través de estas redes pueden servicios de calidad. En este capítulo hablaremos de los orígenes de estas redes y como se han ido popularizando a través de los años.

Las redes sociales en Internet son sistemas que permiten establecer relaciones con otros usuarios a los que se puede o no reconocer en la realidad. (Prato, 2010, pág. 19)

Ilustración 2. Redes Sociales

Fuente: https://gorbrit.wordpress.com/2014/06/24/las-redes-sociales-origen-y-evolucion/

Algunos datos que dan origen a las redes sociales según (Marketing Directo, 2011) son:

- ✓ **1971:** Se envía el primer mail. Los dos ordenadores protagonistas del envío estaban uno al lado del otro.
- ✓ **1978:** Se intercambian **BBS** (Bulletin Board Systems) a través de líneas telefónicas con otros usuarios.
- ✓ **1978:** Las primeras copias de navegadores de internet se distribuyen a través de la plataforma Usenet.
- ✓ **1994:** Se funda **GeoCities**, una de las primeras redes sociales de internet tal y como hoy las conocemos. La idea era que los usuarios crearan sus propias páginas web y que las alojaran en determinados barrios según su contenido (Hollywood, Wall Street, etc.).
- ✓ **1995: TheGlobe.com** da a sus usuarios la posibilidad de personalizar sus propias experiencias online publicando su propio contenido e interactuando con otras personas con intereses similares.
- ✓ **1997:** Se lanza AOL Instant Messenger.
- ✓ **1997:** Se inaugura la web Sixdegrees.com, que permite la creación de perfiles personales y el listado de amigos.
- ✓ **2000:** La “burbuja de internet” estalla.

Según expresa (Prato, 2010):

Estos sitios o espacios sociales nacen luego de la caída de las puntocom en el 2001. En el año 2002 aparece el primer sitio capaz de generar círculos sociales: **Friendster**. En mayo de 2002 nace el sitio de publicación de fotografías

Fotolog.com, y ya en febrero del 2005 superaba el millón de usuarios. El termino fotolog (o fotoblog) originalmente se refería a una variante de weblog para la publicación de imágenes.

En el 2003 nace **MySpace**, la segunda web más visitada de internet. MySpace suele definirse como “un lugar de amigos”, donde es posible chatear, mandar mensajes, crear blogs, invitar a amigos a participar, e incluso personalizar la página, subir fotos y videos.

LinkedIn es una red social cuyo objetivo es hacer conexiones de tipo profesional entre personas y entre personas y empresas, también lanzada en el 2003.

En el mismo año (2003) comenzó a funcionar del.icio.us, un servicio de gestión de marcadores sociales en la Web, que podría compararse con nuestros favoritos, pero en este caso compartirlo con miles de usuarios. del.icio.us permite la construcción colectiva de marcas, que ayuda a otros usuarios a descubrir contenidos que quizás de otra manera nunca hubieran encontrado (p.19-20).

Más adelante en el 2004 nace **Facebook**, concebida originalmente como una plataforma para conectar a estudiantes universitarios. Su pistoletazo de salida tuvo lugar en la Universidad de Harvard y más de la mitad de sus 19,500 estudiantes se suscribieron a ella durante su primer mes de funcionamiento.

Luego, en el 2006 se inaugura la red de microblogging **Twitter**. (Marketing Directo, 2011).

Una de las redes sociales más recientes es **Instagram**, según (Wikipedia, 2016) esta red tiene su historia iniciada en San Francisco centrando los esfuerzos de Kevin Systrom y Mike Krieger en un proyecto de fotografía para móvil. El producto fue lanzado en el Apple App Store el 6 de octubre de 2010.

2.4.1 Tipos de Redes Sociales

Según (Prato, 2010) las redes sociales se pueden clasificar en la siguiente tipología:

- **Redes para encuentros amorosos:** en este ámbito se destacan dos empresas como la americana Match y la francesa Meetic. Las dos son de pago, aunque en Meetic las mujeres pueden emplear los servicios gratuitamente. En ambos casos el acceso a la red social es libre para cualquiera que haya pagado la correspondiente cuota y la finalidad es única: entrar en contacto con una persona para establecer una relación efectiva.

Ilustración 3. Red Social Match.com

Fuente: http://vicarlone.com/match-com-portal-para-encontrar-pareja-online/

- **Redes profesionales:** como la norteamericana LinkedIn o la alemana OpenBC. De origen español se destacan Neurona y eConozco. Todas ellas buscan unir profesionales entre si y están especialmente indicadas para perfiles comerciales.

Ilustración 4. LinkedIn

Fuente: http://www.inboundcycle.com/blog-de-inbound-marketing/c%C3%B3mo-multiplicar-por-10-el-tr%C3%A1fico-de-tus-publicaciones-de-linkedin

- **Comunidades de amigos:** estas permiten conocer a gente a través de sus aficiones y opiniones. Son quizás las más difundidas y que mayor cantidad de miembros en sus comunidades poseen. Las más conocidas actualmente son MySpace, Twitter y Facebook (p.20-21).

Ilustración 5. Facebook, Twitter & MySpace

Fuente: http://nicksagan.blogs.com/nick_sagan_online/2010/11/twitter-facebook-myspace.html

CAPÍTULO III

ORIGEN DEL FRAUDE ELECTRÓNICO Y LA PUBLICIDAD ENGAÑOSA

3.1 Antecedentes históricos del fraude electrónico y la publicidad engañosa

3.1.1 Origen del fraude electrónico

El fraude electrónico es una forma de estafar a las personas a través de medios electrónicos que están conectados a Internet. Este se ha desarrollado con el auge del comercio electrónico, la banca por internet y el aumento de los servicios de distintas compañías a nivel mundial.

Cada día, más personas se conectan a Internet a realizar transacciones que por obligación y requisitos de las páginas a las que acceden, deben de proporcionar su información personal y datos financieros. Por lo tanto, miles de usuarios son propensos a caer en estafas a través de estos medios electrónicos.

Según expresa (Cano, 2011):

Durante todo el siglo pasado, los cambios en la economía, entre ellos la creación de áreas de actividad industrial, han sido fuente de nuevos modos de fraude. La introducción de nuevas tecnologías, y su extensión a todas las actividades económicas, significo la aparición de formas de fraude conocidas genéricamente como fraude informático, en particular en las últimas décadas. En otros casos, los cambios solo modificaron las maneras y los medios para cometer los fraudes ya conocidos, sin llegar a generar formas totalmente novedosas.

Más importante aún fue el cambio que se produjo en el área de la investigación; el fraude informático dio origen a la informática forense y al uso de los soportes digitales de información como fuente de pruebas. Tanto en lo que respecta al uso de redes y grandes sistemas de almacenamiento en el campo laboral como en la utilización de sistemas personales (dispositivos inalámbricos, celulares con capacidad de gestionar casillas de correo electrónico, agendas, servicios GPS, equipos orientados al entretenimiento, etc.), las nuevas tecnologías se ha convertido en una fuente sustancial de potenciales pruebas para investigaciones internas de las empresas o para procesos judiciales (p.17 – 18).

Más adelante se implementaron estrategias y métodos para estafar a través de Internet, utilizando programas y técnicas para engañar a los usuarios con el fin de obtener información y robos en cuentas bancarias, tomar el control de un equipo informático, envío de correos masivos “Spam” para uso y robo de información, entre otros métodos.

Una de las primeras técnicas es el Phishing que consiste en enviar correo electrónico a las personas y a través de este, incentivar a ofrecer sus informaciones como usuario y contraseñas bancarias para de esta forma realizar una estafa a través de transferencias de fondos de una cuenta a otra, vía los canales electrónicos financieros.

Por otro lado, (Garcia, 2010) informa que el término *Phishing* aparece por primera vez en el año 96 en las newgroups de hackers y en la edición del

Magazine 2600. Este término tiene dos orígenes: 1) “Fishing” o pesca, refiriéndose a la pesca de credenciales o a la pesca de ingenuos para intentos de fraude, 2) Phishing – “Password Harvesting” que viene a significar cosecha de contraseñas.

En 1996 un *phisher* se hizo pasar por técnico de AOL y envió mensajes haciendo uso de la ingeniería social en los que solicitaba que el usuario verificase su cuenta o confirmase una factura y así poder solicitar las credenciales personales de la víctima. Con estos datos ya podía realizar acciones como el envío de spam. Para intentar solucionarlo, AOL incluyó como texto *by default* en el intercambio de mensajes: "AOL nunca le solicitará contraseñas o información de facturación".

En 2001 aparecen los primeros scam en Hotmail con el texto "Usted es uno de los 100 ganadores de Hotmail" junto con un formulario que solicitaba el usuario y la contraseña de la cuenta de la víctima. Aunque este mensaje aparecía firmado por el Staff de Hotmail, en realidad provenía de una dirección IP de Ucrania. También AOL informó de un caso similar en donde el usuario recibía un mensaje que le avisaba de un error en su registro y no podían facturarle, para evitar que se le diera de baja debería rellenar un formulario lo antes posible. Además incluía un enlace a una página para realizar la facturación de AOL. Ese mismo año se recibieron mensajes informando que un grupo de hackers había accedido a la base de datos de MSN en donde solicitaban el envío de un correo con los datos personales y la cuenta (usuario y contraseña) porque de lo contrario serían borrados de la base de datos.

3.1.2 La publicidad engañosa

La publicidad tiene origen en la antigüedad, cuando en Europa y Egipto empezaron a utilizar el papel y la imprenta. A través de la imprenta, se desarrolló la comunicación y empezaron a utilizarse las primeras formas de publicidad al difundir mensajes impresos de manera masiva.

No obstante, (Aragon, 2014) expresa:

La publicidad existe desde los orígenes de la civilización y el comercio. Desde que hay productos que comercializar ha habido la necesidad de comunicar la existencia de ellos. La forma más común de publicidad era la expresión oral.

Después de la Segunda Guerra Mundial las empresas anunciantes comenzaron a asociar la necesidad de vincular los procesos publicitarios creativos con los estudios de mercado para optimizar la relación entre las necesidades comunicativas o de desarrollo y crecimiento de la empresa con las estrategias de comunicación adecuadas a dichas necesidades.

En el mundo actual la publicidad está en todas partes. Se define la **publicidad** como la comunicación masiva cuya finalidad es transmitir información o inducir sobre las actitudes para impulsar al cliente o consumidor a un comportamiento favorable al anunciante (p.236).

A través del tiempo el comercio y la alta competencia se han desarrollado en todos los sectores comerciales e industriales. Esto ha logrado un crecimiento en la industria de la publicidad, las empresas cada vez más competitivas diseñan campañas de publicidad para persuadir a segmentos a los que van dirigidos sus bienes y servicios de manera legal. Contrario a esto, hay personas y empresas que se dedican al robo de información a los clientes, a través de publicidad engañosa en Internet con el objetivo de obtener información, robo de dinero, control de computadoras para reproducir virus, entre otras prácticas.

Por consiguiente, según (Uceda, 2011) “Es engañosa la publicidad que de cualquier manera, incluida su presentación, induce o puede inducir a error a sus destinatarios, pudiendo afectar a su comportamiento económico, o perjudicar o ser capaz de perjudicar a un competidor. Es asimismo engañosa la publicidad que silencie datos fundamentales de los bienes, actividades o servicios, cuando dicha omisión induzca a error de los destinatarios”. La **publicidad engañosa** es aquella que de cualquier manera, tanto en su forma como en su fondo, trate de inducir a error a sus destinatarios (p.463).

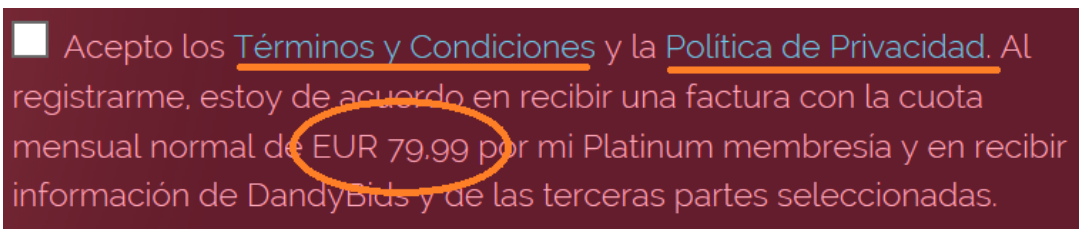
3.1.3 Ejemplo de publicidad engañosa

Ilustración 6. Publicidad engañosa

Fuente: https://www.osi.es/es/actualidad/avisos/2015/05/mucho-cuidado-con-los-tweets-promocionados.html

Esta imagen invita una oferta para obtener un “Drone” por tan solo EUR$2.00, en la parte derecha el usuario deberá introducir todos sus datos personales para poder lograr obtener el artículo que esta de oferta. Pero detrás de todo esto hay una estafa, ya que en los términos y condiciones, en letras pequeñas, se le informa al usuario recibir una factura de EUR$79.00 por una membresía.

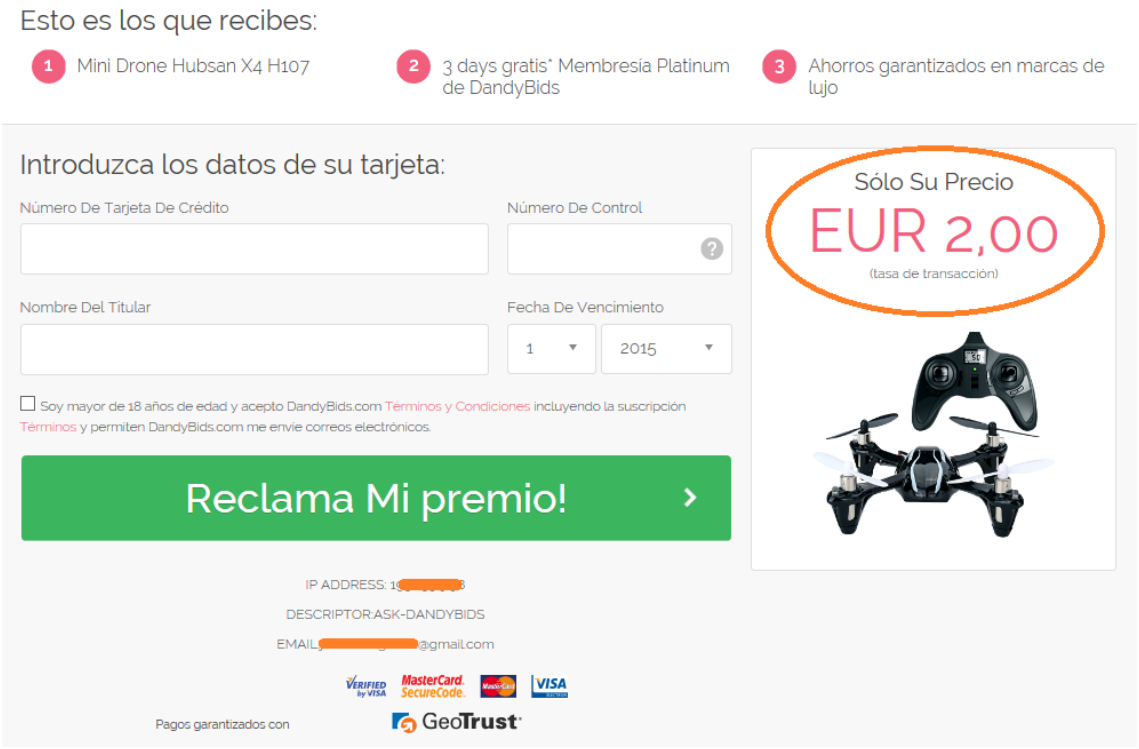
Ilustración 7. Términos y Condiciones



Fuente: https://www.osi.es/es/actualidad/avisos/2015/05/mucho-cuidado-con-los-tweets-promocionados.html

Más adelante, luego de que el usuario acepta los términos y condiciones, se le pide que introduzca los números de tarjeta de crédito para que se le aplique el cargo de los EUR$2.00 que supuestamente vale el artículo.

Ilustración 8. Introducción de los Datos



Fuente: https://www.osi.es/es/actualidad/avisos/2015/05/mucho-cuidado-con-los-tweets-promocionados.html

Por consiguiente, según opina (OSI Oficina de Seguridad del Internauta, 2015):

Como indican en la propia página web: "Puedes elegir cancelar tu suscripción en cualquier momento contactando a nuestro Servicio al Cliente por correo electrónico a [dirección email] o por vía telefónica al número que encontrarás en el sitio web de [nombre sitio web]". Atendiendo a esto un usuario puede pensar en facilitar los datos y cancelar la suscripción posteriormente, antes de los 3 días para que no le realicen el cargo. Sin embargo, en la sección de «Términos y

condiciones» indica lo siguiente: “Cancellation of the membership prior to paying the first month’s membership fee will void any free promotional gift offer.”, es decir, “La cancelación de la membresía antes de pagar la cuota del primer mes, anulará cualquier oferta de regalo promocional gratuito.”, lo que quiere decir que se habrán pagado 2 euros para nada.

Es más, “Para recibir nuestro regalo de bienvenida, los usuarios deben confirmar su identidad enviando la siguiente documentación probatoria: copia escaneada de una identificación válida (pasaporte o licencia de conducir) y copia escaneada del formulario firmado de la tarjeta de crédito. Descarga y llena el formulario desde este enlace. Todos los documentos requeridos deben ser enviados a [dirección email] dentro de los 14 días posteriores al pago de la oferta del regalo de bienvenida o de lo contrario, la oferta del regalo de bienvenida no será válida.” lo que supone un gran riesgo para nuestra privacidad al facilitar información tan confidencial.

3.2 Tipos de fraudes electrónicos y publicidad engañosa

Hoy en día, en los medios digitales existen diferentes tipos de ataques contra páginas web y publicidad engañosa a través de las redes sociales, que direccionan al usuario a otras páginas para obtener información confidencial. En las redes sociales se utilizan aplicaciones de cualquier índole para motivar y persuadir a los usuarios a ingresar a dichas aplicaciones. A través de las mismas existe la posibilidad de que haya un fraude enmascarado. Por lo tanto, existen

diferentes técnicas de fraude online que hoy en día están perjudicando a los usuarios.

Como enuncia (Ardila, 2013), Según el Informe sobre Medios de pago y Fraude en Comercio Electrónico de 2012 elaborado por la Asociación Española de la Economía Digital:

- El 85% de las empresas encuestadas declaran unas pérdidas anuales por fraude online por debajo del 0,5 % de su facturación anual. No parece un problema de gravedad, pero si tenemos en cuenta que el comercio electrónico es un mercado joven, es para empezar a preocuparse.

- El 25% de las empresas encuestadas declaran utilizar algún sistema de control de fraude online, una cifra demasiado baja: no hay conciencia sobre el problema.

No obstante, (20 Minutos, 2012) habla sobre los tipos de fraudes en la web, los cuales son:

- **Fraudes en la compraventa o webs de alquiler entre particulares.** Aparatos tecnológicos y smartphones, coches de segunda mano, alquileres en supuestas fantásticas viviendas muy céntricas o apartamentos vacacionales muy atractivos, todos con apariencia de

auténticas gangas se ofrecen en venta o alquiler en Internet. Se usa el atractivo de estos productos para realizar los intentos de fraude en webs de compraventa o alquiler entre particulares.

- **Ofertas de trabajo falsas para sacar dinero a los que buscan empleo.** La fuerte demanda de empleo hace que desaprensivos traten de beneficiarse fraudulentamente de ellos. Peticiones de dinero por adelantado "para el temario o cursos previos del puesto a desempeñar" o "para cerrar los trámites de contratación" o pedir que se llamen a un teléfono de alto coste son algunas de las estafas más denunciadas.

- **Virus para estafar al internauta haciéndose pasar por entidades.** Este año se han extendido mucho virus que utilizan la imagen de entidades conocidas y que se hacen pasar por la Policía Nacional española, la Sociedad General de Autores de España o la Agencia Española de Protección de Datos para lograr instalarse de forma fraudulenta en los dispositivos. El virus funciona bloqueando el ordenador, inventándose una supuesta multa de 100 euros por haber detectado pornografía infantil en el disco duro o archivos que violan la propiedad intelectual o la Ley Orgánica de Protección de Datos. Se pide el pago a través de medios no rastreables y nunca se recupera el normal funcionamiento del ordenador.

- **Phishing sobre cuentas en redes sociales y de correo.** El Phishing es tratar de obtener las claves de usuario del internauta para luego obtener

beneficios fraudulentos con esos datos. Se hace sobre todo haciéndose pasar por un banco y pidiendo datos del mismo. El engaño más novedoso este año ha sido enviar un SMS para solicitar los datos de la tarjeta de crédito, para desbloquearla, por supuestos motivos de seguridad.

- **Fraude para suscribir en SMS Premium y llamadas a teléfonos de alta tarificación.** Los ganchos utilizados son varios: desde supuestos paquetes que no se han recogido (inexistentes, claro está) a supuestas llamadas de personas que no tienen saldo y requieren contactar con ellos a través de esos medios, falsos premios -gadgets o dinero- en concursos en los que, curiosamente, no se ha participado o mensajes ambiguos de supuestas personas recién separadas y que quieren tomar un café.

En cuanto a la publicidad engañosa, en esta investigación se hace referencia a diversos tipos de formas de publicidad engañosa a través del Internet. Según expresa (Talaya, 2008):

- La **publicidad desleal**, que es la que perjudica a otras personas o empresas y en especial a los competidores.

- **Publicidad ilícita**. Se constata la prohibición de la publicidad encubierta, que es la presentación intencionada de productos y marcas a cambio de una remuneración, que pueda inducir al público a error.

Sin embargo, (Eduinnova, 2010) expresa:

- **Publicidad ilícita:** es aquella que atenta contra la dignidad de las personas o vulnera los valores o derechos reconocidos en la Constitución, especialmente si estos, se refieren a la infancia, la mujer y la juventud.

- **Publicidad engañosa:** Podemos destacar en la publicidad engañosa tanto a la que silencia datos acerca de sus servicios, productos, atención…, importantes para el consumidor, como a la que miente directamente al consumidor.

- **Publicidad desleal:** Es la que por su contenido, forma o difusión provoca descredito, menosprecio a otra empresa, persona o producto, servicio o calidad. También se considera desleal a la publicidad que no se apoya en demostraciones objetivas sobre la calidad de su producto, esenciales para anunciarlos.

- **Publicidad subliminal:** Se entiende por publicidad subliminal aquella que inserta imágenes en la publicidad que no son analizadas conscientemente por nuestro sistema cognitivo, pero quedan registradas en nuestro subconsciente promoviendo a la compra del producto. La publicidad subliminal suele emitir estas imágenes utilizando un único fotograma que dura milésimas de segundo, el tiempo necesario para que la imagen no sea analizada.

3.3 Tipos de software malicioso

Existen diferentes tipos de software que son utilizados para realizar fraudes, robo de información, daños en otro software y que vulneran la seguridad de los equipos donde se instalan. Antes de hablar sobre estos tipos de software maliciosos, hay que tener un concepto claro de que esto significa.

Al **software malicioso**, o malware, término que surge de las palabras en inglés "malicious software", se le considera todo tipo de software cuyo objetivo es provocar daños en un sistema informático. (Maria Del Pilar Alegre Ramos, 2011, pág. 70)

Consecuentemente, los virus o software malicioso se instalan en los sistemas operativos de los usuarios sin que este lo pueda percibir, provocando que dichos sistemas sufran daños que el usuario no pueda reparar.

Según describe (Miguel Moro Vallina, 2014), existen diversos tipos de virus. Algunos de los principales son los siguientes:

- **Virus de macro.** Se transmiten a través de macros de aplicaciones informáticas como procesadores de textos, hojas de cálculo o bases de datos; estas macros vienen incluidas en los propios documentos, con lo que el virus infecta el ordenador al abrir el documento. Conviene por ello

deshabilitar las macros en dichas aplicaciones, habilitándolas solamente para los archivos que consideremos fiables.

- Los **virus del sistema** detienen o corrompen el sistema operativo, destruyendo la información de la tabla de particiones, formateando el disco o eliminando los sectores de arranque. Una vez que el virus ha actuado, habitualmente deberemos formatear el equipo y volver a instalar el sistema operativo.

- Los **troyanos** son programas de apariencia inofensiva (ocultos muchas veces bajo otro nombre) que se instalan en el ordenador del usuario y abren en él una puerta de comunicación para ser controlado a distancia desde otro ordenador. Una vez efectuada la infección, el ordenador infectado puede (sin el consentimiento ni el conocimiento del usuario) transmitir información a otras personas o ser, a su vez, origen de una nueva infección (p.76).

Por otro lado, (Maria Del Pilar Alegre Ramos, 2011) dice que:

- **Gusanos:** Son programas, al igual que los virus, pero su comportamiento es diferente. Se dedican a hacer copias de sí mismos muchas veces y a gran velocidad con la intención de colapsar el sistema informático o la red.

- **Adware:** Este tipo de software malicioso se dedica a mostrar publicidad no requerida, ni deseada.

- **Backdoors:** Los backdoors o puertas traseras, entran en un equipo sin permiso y conceden al programa que accede derechos de administrador. Pueden espiar los datos del sistema, pero su uso más habitual consiste en instalar otros programas dañinos para el sistema.

- **Botnets:** Redes (nets) de robots (bot). Son redes de ordenadores que se controlan remotamente infectando ordenadores a través de internet, que pueden llegar a ser un número muy elevado (incluso miles).

- **Dialers:** Los dialers o programas de marcación se dedican a establecer conexiones telefónicas, normalmente a través de Internet, utilizando líneas sin el consentimiento de su propietario, o sin que este se haya dado cuenta de que lo ha dado. Estos programas marcan números de tarificación especial con un alto coste.

- **Exploit:** Es un software malicioso que se dedica a atacar la vulnerabilidad de un sistema operativo, como los bugs o agujeros del sistema.

- **Hijacker:** Se dedica a cambiar la configuración de los navegadores de Internet modificando la página de inicio del mismo para que entre en sitios web sin el consentimiento del usuario, como sitios con pornografía, o lugares donde pueden copiar información del usuario, como las claves de acceso.

3.5 Criterios para tipificar la publicidad engañosa en la República Dominicana

Según expresa (Consumidor, 2014), en la Resolución del Consejo Directivo que Regula la Publicidad Engañosa en la República Dominicana, en el artículo segundo. Los criterios utilizados para la determinación de la existencia de publicidad engañosa serán los siguientes:

1. Inducir o tratar de inducir intencionalmente al consumidor o usuario a adquirir un bien o servicio que luego resulte ser falso o inexistente;

2. Ofertar o publicar un determinado bien o servicio como señuelo, estando en conocimiento de que no está disponible, para atraer al consumidor e intentar venderle otro bien o servicio;

3. Desalentar la compra de un bien o servicio anunciado y ofrecer otro en sustitución;

4. Exponer, vender u ofrecer para la venta medicamentos, sin la debida autorización de la entidad estatal competente en materia de salud;

3.6 Efectos y daños causados a los clientes

Hoy en día muchas personas están sufriendo las consecuencias del fraude electrónico y la publicidad engañosa, por falta de conocimiento o prevención, también por descuido o por dejarse persuadir ante dicho señuelo.

Estos casos son de mucha importancia y las autoridades deben de prestar atención a dichos delitos. Los usuarios o clientes son propensos a ser víctimas de robos en cuentas bancarias, robo de información personal para acceder a lugares donde este registrado el usuario para cometer un fraude.

Uno de los casos más comunes que afecta a los clientes son las clonaciones y transacciones fraudulentas en las tarjetas de crédito. Clientes de diferentes entidades bancarias han sido víctimas de fraudes a través de las tarjetas de crédito. Frecuentemente, hay casos de clonación, consumos no reconocidos por el cliente, ya sea nacional e internacional.

Según (Diario Libre, 2016), En República Dominicana, atacar a los clientes de las instituciones financieras supone el 80% de los casos del ciberdelito, según la Procuraduría, siendo las consecuencias principales la clonación de tarjetas y transferencia de dinero, sin dejar a un lado el muy usado "Phishing".

Entre octubre de 2010 y diciembre de 2013, la Superintendencia de Bancos recibió 9,861 reclamaciones de transacciones fraudulentas de los usuarios. Y para conocer la situación de los lectores, DL realizó una encuesta en su página web que arrojó que de 131 participantes, el 44% alguna vez fue víctima de robo de sus datos bancarios.

Ilustración 9. Cantidad de Reclamaciones de transacciones fraudulentas de usuarios de los servicios financieros

Fuente: http://www.diariolibre.com/noticias/fraudes-bancarios-son-el-80-de-los-ciberdelitos-FLDL477561

Para 2013, la cantidad de tarjetas de crédito en República Dominicana era de aproximadamente 2.5 millones. En los últimos 10 meses, la nueva Procuraduría

Especializada contra Crímenes y Delitos de Alta Tecnología decomisó más de 3 mil plásticos que estaban en manos de delincuentes, según informa el titular de esa dependencia, John Henry Reynoso Ramírez. En ese mismo período, recibió 562 denuncias de clonación.

3.7 Estrategias y tipos de fraudes utilizados en las páginas web y redes sociales

A través de los años, las Redes Sociales han aumentado su demanda para las empresas y el número de seguidores. Por lo que defraudadores cada día van implementando nuevas estrategias para engañar a los usuarios, ofreciendo ofertas de negocios que realmente son falsas, vendiendo la imagen de que es un negocio rentable para que las personas puedan acceder de manera fácil y rápida.

Según el informe de (El Pais.com, 2015), Facebook anunció que su lucha contra los "me gusta" falsos está dando tan buenos resultados que muchos "malos actores" que construyeron negocios con esta estrategia, están cerrando sus tiendas. Lea también: ¿Qué se puede y qué no se puede publicar en Facebook?

Los avances en tecnología para reconocer patrones sospechosos de "me gusta" han permitido a la red social bloquear las actividades de este software dañino, cuentas fraudulentas y "granjas" de clics, que emplean ejércitos de trabajadores mal pagados.

"Continuamos adaptándonos y mejorando los métodos que usamos para prevenir los falsos 'me gusta' porque los estafadores evolucionan constantemente y prueban nuevos métodos para tratar de intervenir nuestros sistemas de prevención", dijo en un blog el ingeniero de seguridad de Facebook, Kerem Cevahir.

"Este trabajo ha dificultado extremadamente a las personas desde vender los 'me gusta' fraudulentos hasta lograr entregarlos a sus clientes".

En los últimos seis meses, Facebook ha triplicado el número de "me gusta" falsos detectados y bloqueados antes de llegar a las páginas, según Cevahir.

Facebook también removió los "me gusta" fraudulentos de páginas en la red social, notificando a los administradores de esas cuentas. Cevahir indicó que este comportamiento fraudulento era solo una "pequeña fracción" de todas las actividades en Facebook.

"Los 'me gusta' creados por cuentas falsas o gente sin verdadera intención son malos para las personas en Facebook, anunciantes y Facebook en sí mismo", indica la guía de seguridad de la red social, basada en California.

"Tenemos un iniciativa fuerte para ir agresivamente detrás de los actores nocivos, detrás de los 'me gusta' falsos porque los negocios y la gente que use nuestra plataforma quiere conexiones y resultados reales", señaló.

Ilustración 10. Transacción fraudulenta

Fuente: https://contrafraudesenmexico.blogspot.com/

Por otro lado, en las redes sociales están circulando cuatro (4) estafas que están afectando a los usuarios según (BBC Mundo, 2015):

Las redes sociales son el lugar ideal para que los delincuentes de internet encuentren víctimas para sus estafas.

Además de tener millones de usuarios, admiten aplicaciones de software abierto.

Así, cualquier programador más o menos experimentado puede escribir un código malicioso que funcione en estas plataformas y con el que pueda engañar a los usuarios.

Los fraudes suelen consistir en ofrecer productos o servicios que el usuario nunca recibe.

Pero en el proceso para conseguir los premios o regalos prometidos, suele abrir las puertas a virus o malware, o entrega sus datos personales.

Los ciberdelincuentes o bien comercializan con ellos o suscriben a las víctimas a servicios de mensajería denominadas Premium.

Así, cuando aún sin saberlo están inscritos a estos, reciben mensajes con música, juegos, concursos, noticias, campañas y otro tipo de contenidos a un costo superior al de los SMS convencionales.

Hay fraudes de todo tipo, pero te presentamos los cuatro que más están circulando en los últimos tiempos.

1. Cupones de descuento

Si te están ofreciendo cupones de descuento de US$500 a cambio de que contestes a unas cuantas preguntas, sospecha. Es lo que advierte la empresa de seguridad en internet Kapersky Lab.

Quienes llevan a cabo estas estafas suelen utilizar como gancho el nombre de empresas conocidas.

Incluso suelen crear páginas de internet ficticias de las empresas para hacer las campañas más creíbles.

Y la dinámica suele ser siempre la misma: piden que se responda a una encuesta, después solicitan que se comparta, y por último dicen que requieren de tus datos para poder enviar el supuesto cupón.

Éste nunca llega, pero lo que el usuario sí podría recibir es una factura más elevada a finales de mes.

2. Solicitudes de "Phishing"

"Alguien acaba de publicar una foto tuya", dice el mensaje que acabas de recibir.

Como quieres ver la imagen en cuestión, haces clic en el enlace adjunto.

Éste te lleva a la página de inicio de una sesión de Twitter o Facebook, así que introduces tu usuario y tu contraseña.

Y cuando lo haces, un delincuente cibernético obtiene tus datos, porque la página de acceso a las redes sociales era falsa.

3. Mensajes de voz de WhatsApp

Es posible que hayas recibido un correo electrónico advirtiendo que uno de tus contactos te dejó un mensaje de voz en WhatsApp e invitándote a descargarlo.

Cuidado, es un fraude, advierten los expertos de Kapersky Lab.

Si caes en la trampa y tratas de reproducirlo o descargarlo, abrirás la puerta a un malware que se instalará en tu equipo.

La propia empresa advierte que se trata de una estafa.

En su página de internet, WhatsApp aclara que no envían mensajes de texto ni correos electrónicos, a no ser que el usuario se haya puesto en contacto anteriormente con el equipo de soporte.

4. Notificaciones de envío de paquetería

Es un sistema similar al del fraude de los cupones de descuento.

Recibes un mensaje en nombre de una empresa de paquetería en el que se te notifica un envío.

Si no esperas ningún paquete, lo más probable es que sea un fraude.

En ese caso llevará adjunto un fichero con código malicioso.

Para no sucumbir a esta estafa, los expertos dicen que basta con comprobar el remitente, ya que no suele coincidir con el de la empresa de paquetería.

En cuanto al resto, Kapersky Lab recomienda ser cauteloso y desconfiar siempre de promociones y de concursos.

Así, si te encuentras con la promoción de una marca conocida en las redes sociales, los expertos en seguridad te aconsejan comprobar si existe en el perfil de la empresa en Facebook o Twitter.

También señalan que conviene prestarle atención al URL de la página web a la que remite la promoción, sobre todo si está acortado, y desconfiar de los errores ortográficos.

Por su parte, Norton, la división de antivirus de la empresa de seguridad en internet Symantec, recomienda no incluir información personal como el correo electrónico o el número de teléfono al crear o actualizar el perfil en una red social.

Asimismo, los expertos en seguridad de internet señalan que deberías tener cuidado con los correos que advierten del cierre de cuentas de Facebook o Hotmail; con los que informan de la muerte de algún personaje famoso; con las solicitudes de donaciones; y con cualquier enlace que te pide confirmar tu cuenta agregando tu usuario y contraseña.

Esto te ayudará a no sucumbir a estos fraudes en internet.

3.7.1 Usuarios propensos a ser defraudados

Muchos usuarios son víctimas de distintas trampas y engaños a través de la web, porque no tienen conocimiento de cómo evitar ser víctimas de estas malas prácticas. Es recomendable que todo usuario sea responsable y se preocupe por orientarse sobre las diferentes estrategias que hay en internet para engañar a las personas.

Por lo tanto, (El Tiempo, 2010) informa que casi dos tercios de los usuarios de Internet son víctimas de fraude.

Así lo afirmó el miércoles la empresa de seguridad Symantec, que hizo la investigación.

Entre las personas encuestadas para este estudio, bautizado 'Norton Cybercrime report: the human impact' (Informe de Cibercrimen de Norton: el impacto humano), el 65 por ciento dijo haber sido víctima de criminalidad en Internet.

China ocupa el primer lugar, pues un 83 por ciento de los usuarios interrogados dijeron haber sido infectados por un virus de Internet, por robos de identidad, fraude en la tarjeta de crédito u otros fraudes.

Brasil e India lo siguen, ambos con el 76 por ciento, delante de Estados Unidos, donde se registra un 73 por ciento.

Les siguen Nueva Zelanda (70 por ciento), Italia y Australia (69 por ciento), Canadá (64 por ciento) Alemania y España (62 por ciento), Gran Bretaña (59 por ciento), Francia (57 por ciento), Suecia (56 por ciento) y Japón (36 por ciento).

Symantec, que presentó este estudio con motivo del lanzamiento de la actualización de su sistema de seguridad Norton, explicó que las víctimas, muchas veces indignadas, no están bien informadas y no suelen denunciar los crímenes porque piensan que hay pocas posibilidades de que se tomen medidas al respecto.

No obstante, Sysmantec afirma que es crucial hacer una denuncia cuando se es víctima de criminalidad informática, pues la policía puede investigar y, estableciendo analogías entre varios casos similares, puede llegar a conclusiones.

"Los cibercriminales roban pequeñas sumas por gusto para que no los detecten, pero el total se suma", señala en los comentarios del estudio Adam Palmer, uno de los responsables de los productos Norton. Palmer también dice que al no denunciar un robo se "ayuda a los criminales a quedar impunes".

Para Joseph LaBrie, profesor asociado de psicología en la universidad Loyola Marymount de Los Ángeles, citado en la presentación del estudio, el hecho de que las víctimas renuncien a luchar juntas se parece a "cuando se es estafado por un mecánico: si no conocen de autos, no va a discutir con el mecánico".

Este estudio revela también lagunas en la percepción de lo que es legal o ilegal en Internet, ya que casi la mitad de las personas interrogadas piensan que es legal descargar una película sin pagar, y el 24 por ciento piensan que no es reprochable leer los correos electrónicos de otra persona o mirar secretamente sus consultas en Internet.

"Las personas son reticentes a protegerse o asegurar su ordenador, ya que piensan que es muy complicado", afirmó Anne Collier, una responsable de la

organización sin fines de lucro ConnectSafely.org, que participó en el estudio Norton.

"Pero todo el mundo puede tomar medidas simples, como tener un programa de seguridad actualizado. Para la criminalidad en Internet, algunos gramos de prevención valen toneladas de remedio", agregó.

El estudio fue realizado en febrero de 2010 por la empresa StrategyOne entre 7.066 adultos de 14 países.

3.8 ¿Cómo prevenir el fraude y la publicidad engañosa?

Cada vez más, en la actualidad los defraudadores buscan todas las formas de estafar a las personas. Todo usuario debe de tener precaución al momento de ingresar informaciones personales en cualquier página web o aplicación. Porque existe mucho riesgo de ser engañado. Cada día, miles de personas son estafados a través de Internet, ya sea realizando compras en páginas web, clonación de tarjeta de crédito, Phishing, entre otras actividades fraudulentas.

Por lo tanto, existen medidas de prevención para que el usuario lo medite y de esta manera evita ser engañado por publicidad desleal colocada en Internet y por diferentes tipos de fraudes que circulan en la red.

Para (Petovel, 2012), algunos consejos para prevenir el fraude el internet son:

- **No confiar en precios sospechosamente bajos**, compruebe cuál es la media en el mercado verificando anuncios similares en la plataforma (cuidado con la publicidad engañosa).

- **Utilizar la mensajería interna** del sitio para un mejor seguimiento.

- **Evitar hacer clic en cualquier enlace** que pueda resultar sospechoso o no relacionado con la operación que está intentando llevar a cabo. Tampoco abra archivos adjuntos que sean de dudosa procedencia. Este tipo de tácticas podría ser utilizada por un usuario malicioso para infectar su equipo y hacerse luego con sus datos personales o financieros.

- **Sea cauteloso con la información personal o bancaria** que comparta al vender o comprar en línea, y evita realizar grandes transferencias de dinero si no está seguro sobre el perfil del vendedor.

- **Evite utilizar sistemas de giros de pagos y transferencias anónimos como Western Union o MoneyGram,** que no aseguren un reembolso en caso de estafa. Utilizar transferencias bancarias, contra reembolso o realizar los pagos personalmente. Cuando haga una venta controle siempre la calidad de los billetes que se entregan.

- **Utilizar contraseñas seguras y únicas para cada servicio.** No use contraseñas relacionadas a fechas de nacimiento, números de documento o secuencias de letras o numéricas. Cree claves de más de 8 caracteres combinando minúsculas, mayúsculas, números y caracteres especiales siempre que sea posible. Renueve las contraseñas con cierta periodicidad.

- **Evite acceder a su correo electrónico y sitios desde equipos públicos o utilizando redes Wi-Fi inseguras o públicas.** Recuerde siempre finalizar su sesión antes de dejar el equipo. Se recomienda visitar páginas reconocidas.

- **Desconfíe de las personas que no provean un número telefónico verificable.** Siempre trate de contactarse con teléfonos fijos de los puntos de venta.

- **Evite adquirir réplicas de productos conocidos.** No sólo estará cometiendo un delito sino que estará poniendo en riesgo la privacidad de sus datos al intentar ahorrar un poco de dinero comprando un producto de inferior calidad.
- Por último, **use el sentido común:** si algo le resulta sospechoso o tiene dudas no continúe con la operación. Infórmese antes de poner en riesgo su privacidad y seguridad.

CAPÍTULO IV

ANÁLISIS DE LAS ESTRATEGIAS DE MARKETING, FRAUDES Y PUBLICIDAD ENGAÑOSA EN LAS REDES SOCIALES Y PAGINAS WEB EN EL SECTOR DE TELECOMUNICACIONES

4.1 Presentación del Análisis

4.1.1 Segmentación de mercado

Esta investigación va dirigida a hombres y mujeres mayores de 18 años que utilicen el Internet y las redes sociales.

4.1.2 Presentación de la muestra

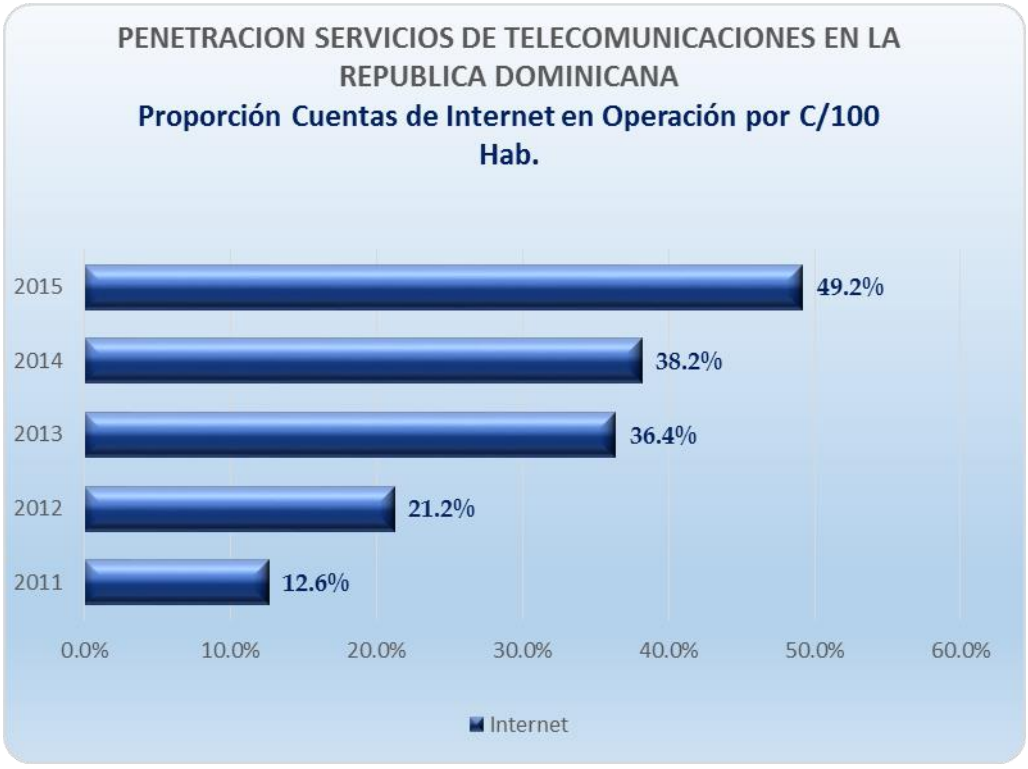
Partiendo de los datos suministrados por el Instituto Dominicano de las Telecomunicaciones (INDOTEL) en el año 2015, estiman un total de 4, 909,933 cuentas de Internet.

Tabla 11. Cantidad de cuentas de Internet 2011 - 2015

VARIABLES			PENETRACION
AÑOS	Ctas. De Internet	Población	**Internet**
2011	1,211,343	9,581,682	12.6%
2012	2,054,905	9,682,774	21.2%
2013	3,558,024	9,782,489	36.4%
2014	3,773,134	9,881,439	38.2%
2015	4,909,933	9,980,240	49.2%

Fuente: http://indotel.gob.do/category/estadisticas-telecomunicaciones/#

Ilustración 11. Gráfico proporción de cuentas de Internet por cada 100 habitantes 2011 - 2015



Fuente: http://indotel.gob.do/category/estadisticas-telecomunicaciones/#

Muestreo

El tipo de muestro utilizado es el Muestreo Probabilístico. Por lo tanto, dado a que la población pasa de los 100,000 habitantes, utilizamos la siguiente formula:

Ilustración 12. Formula de Muestreo Probabilístico

$$n = \frac{Z^2 \cdot p \cdot (1-p)}{e^2}$$

Fuente: http://www.netquest.com/blog/es/que-tamano-de-muestra-necesito/

n = El tamaño de la muestra

N = Tamaño del universo

Z = Nivel de confianza. Los valores más frecuentes son:

Nivel de confianza 90% -> Z=1,645

Nivel de confianza 95% -> Z=1,96

Nivel de confianza 99% -> Z=2,575

e = Es el margen de error máximo

p = Probabilidad a Favor

Datos:

N = 4, 909, 933

Z = 95% ≥ Z = 1, 96 e = 5% p = 50%

$$n = \frac{(1.96)^2 (0.50) (10.50)}{(0.05)^2}$$

$$n = \frac{3.84 (0.50) (0.50)}{0.0025}$$

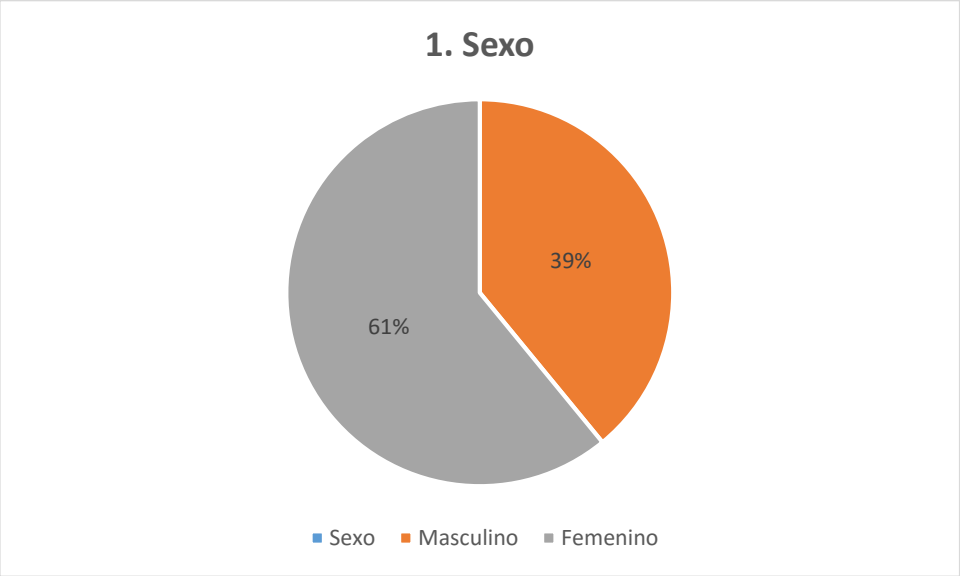
$$n = \frac{0.96}{0.0025}$$

n=384

- ✓ La muestra representativa para el realizar la investigación es de **384.**

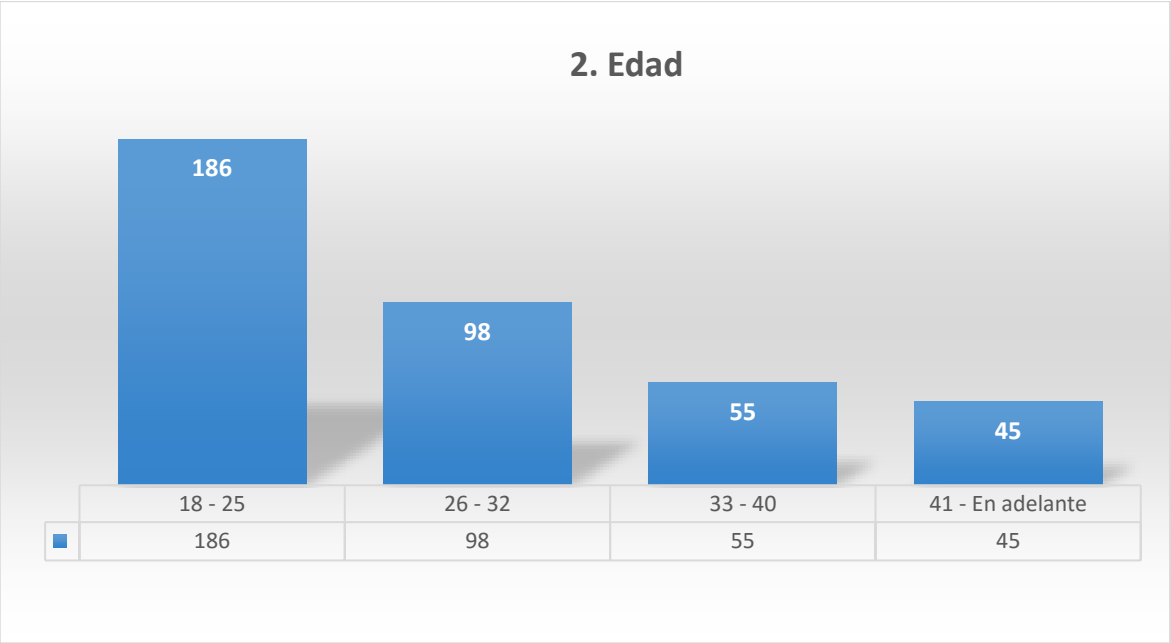
4.1.3 Presentación de los resultados

La encuesta fue realizada a 384 personas, utilizando el muestreo probabilístico.



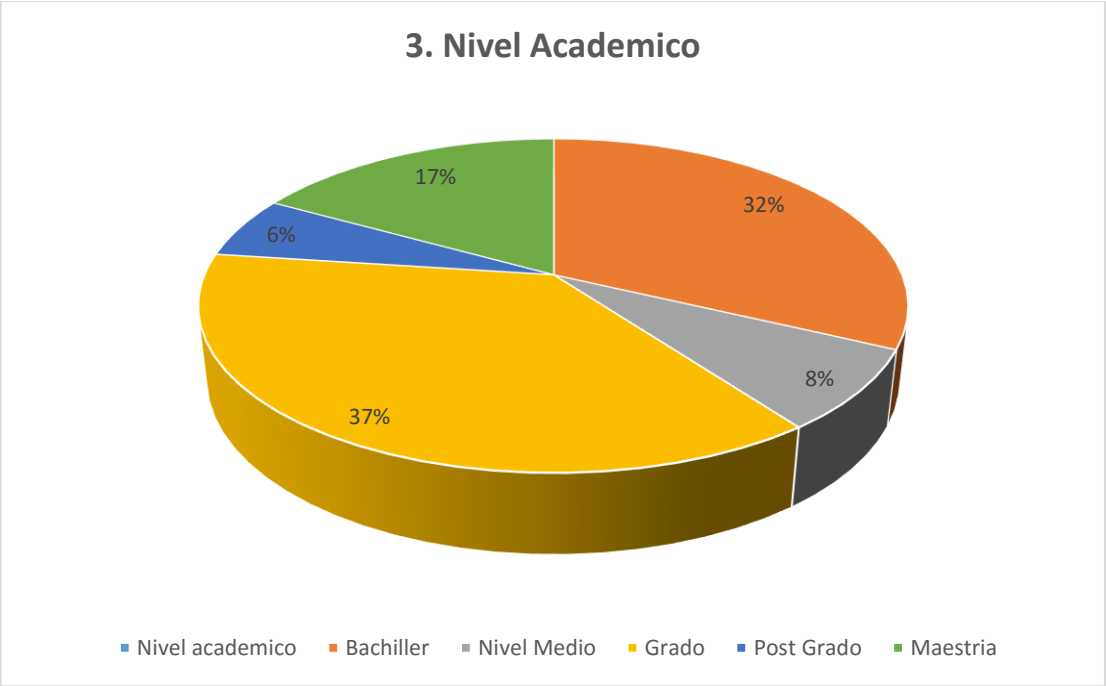
Fuente: Elaborado por el sustentante

Análisis: El número de personas encuestadas que en total son 384, un 61% representa el sexo femenino y un 39% el sexo masculino.



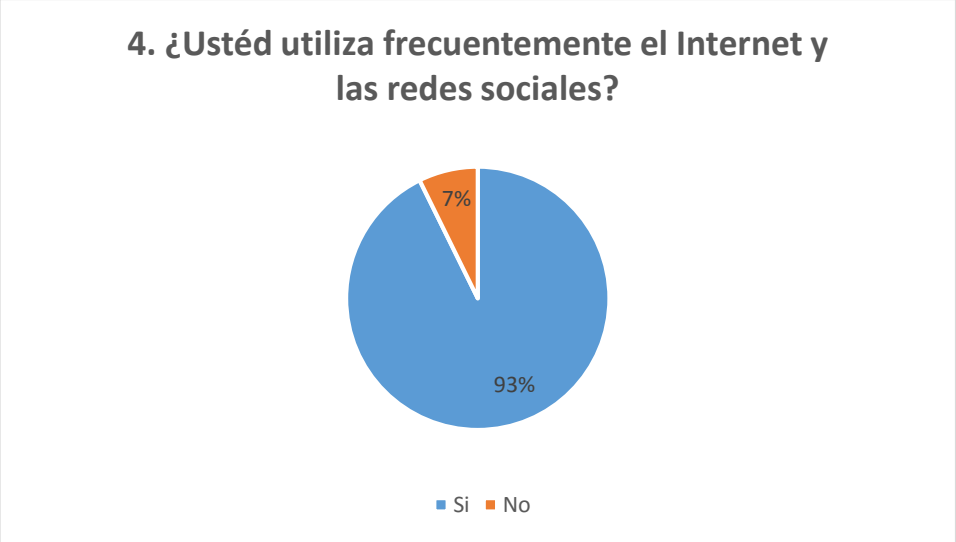
Fuente: Elaborado por el sustentante

Análisis: Se ha determinado que el mayor número de personas de la población que utiliza las redes sociales y páginas web están en un rango de edad de 18 – 25 años, quedando en segundo lugar de 26 – 32 años de edad, siguiendo los adultos de 33 – 40 años de edad y por último los adultos de 41 años en adelante.



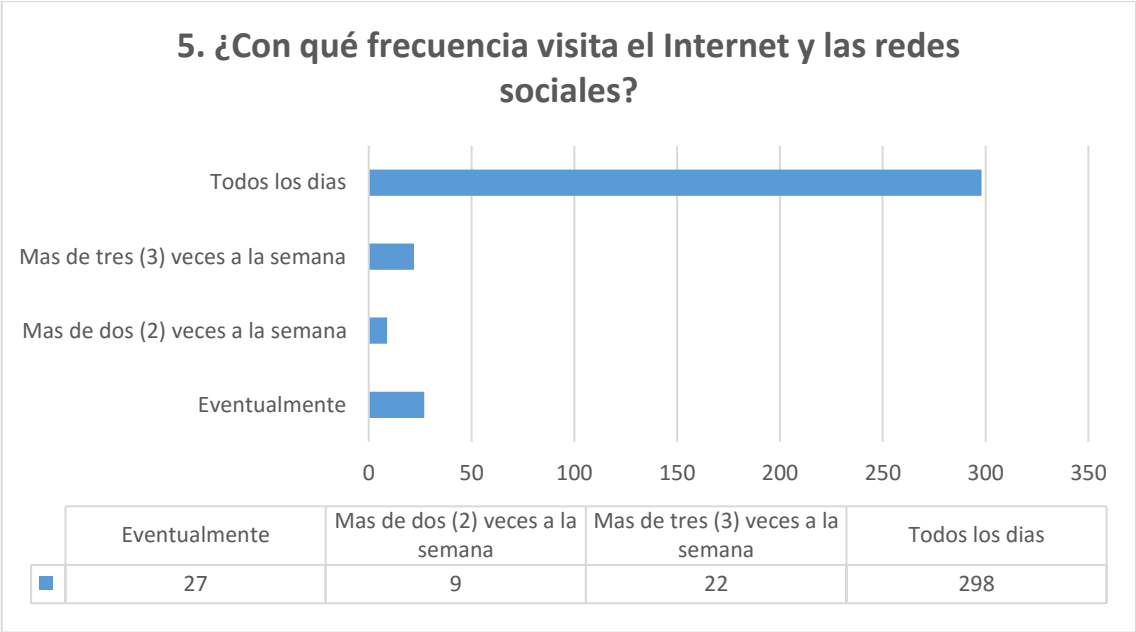
Fuente: Elaborado por el sustentante

Análisis: Se determinó que las personas que están más conectados a la web representan un 37% que son estudiantes universitarios, seguido de bachilleres que representan un 32%, un 17% de maestría, un 8% de nivel medio y un 6% de post grado.



Fuente: Elaborado por el sustentante

Análisis: Según los datos obtenidos se ha demostrado que el 93% de la muestra accede a las redes sociales y navega por el Internet, indiciando que utilizan estos medios para mantenerse actualizados y comunicados. Este porcentaje tiene más probabilidad de ser víctima de fraude electrónico y publicidad engañosa. Y se ha determinado que el 7% restante no utiliza el Internet y las redes sociales porque según los datos obtenidos, a muchos no les gusta, otros no tienen tiempo para acceder a estos medios.



Fuente: Elaborado por el sustentante

Análisis: A través de estos datos se identifica que 298 personas utilizan el Internet todos los días, otras 22 personas indican que acceden más de tres (3) veces a la semana, 9 personas más de dos (2) veces a la semana y 27 personas acceden eventualmente.

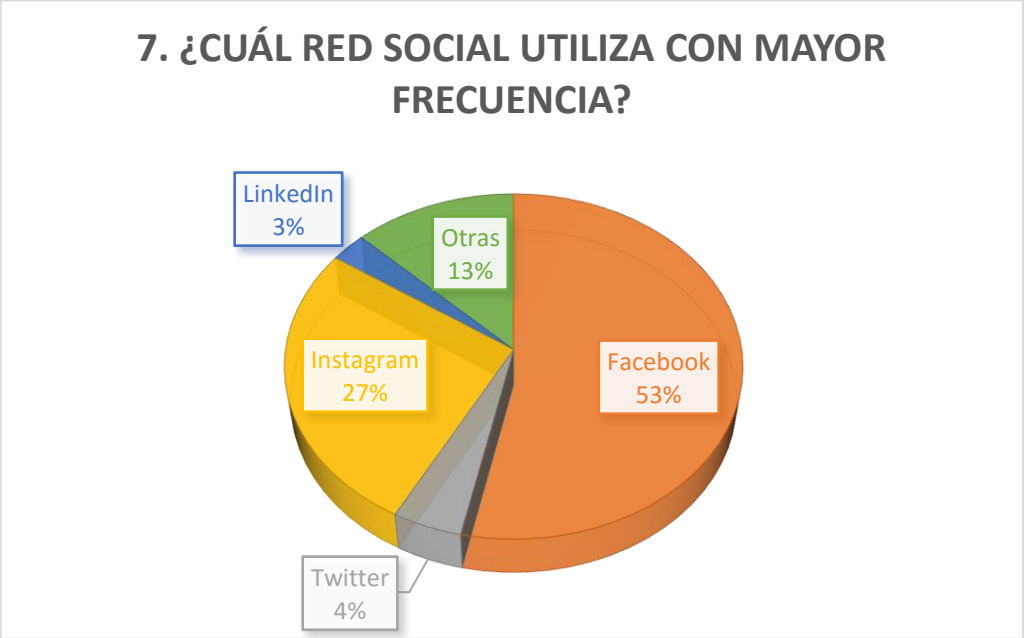
6. ¿Cuáles páginas web acostumbra a utilizar?

Los usuarios indicaron a cuales páginas acceden con frecuencia y contestaron lo siguiente:

- Amazon
- Facebook, Instagram, Marketing Directo, Puro Marketing, Wales University, Google scholar, Amazon, etc.
- Instagram, Facebook, Twitter.

- Gmail, Facebook, Google, Hotmail, Netbanking de 3 bancos distintos y YouTube.
- Facebook, Instagram, Snapchat, google.
- Google, Wikipedia, YouTube.
- Google
- Listindiario.com, Diariolibre.com, Gmail.com, Amazon.com.
- Google, Facebook, monografias.com, entre otras.
- Amazon
- Facebook, upsclo, YouTube, Google, LDS.org, el faro mormon.
- Facebook
- Noticiassin.com, remolacha.net, CNN.com, CNN en español, listindiario.com, diario libre.com.
- Google, remolacha.net, periódicos, etc.
- www.google.com, www.amazon.com.
- Google
- Instagram, Google.
- Facebook, Instagram, twitter.
- Google
- Hotmail, Google redes sociales.
- www.diariolibre.com, www.listin diario.com.
- www.youtube.com, www.facebook.com.
- Google, Wikipedia, Gmail.
- Wikipedia, Diario libre.
- Google, LinkedIn.
- ESPN, CNN, Marca, Facebook, YouTube, Netflix.

- EBay, Remolacha, LinkedIn, Amazon.
- Instagram, Snapchat, Facebook.
- Askmen.com, Pitchfork.com, Diariolibre.com, HBR.com, Netflix.com, Amazon.com.
- Google.Com, aldaba.Com.
- Jw.org, Wikipedia, Pordede.
- Remolacha.net

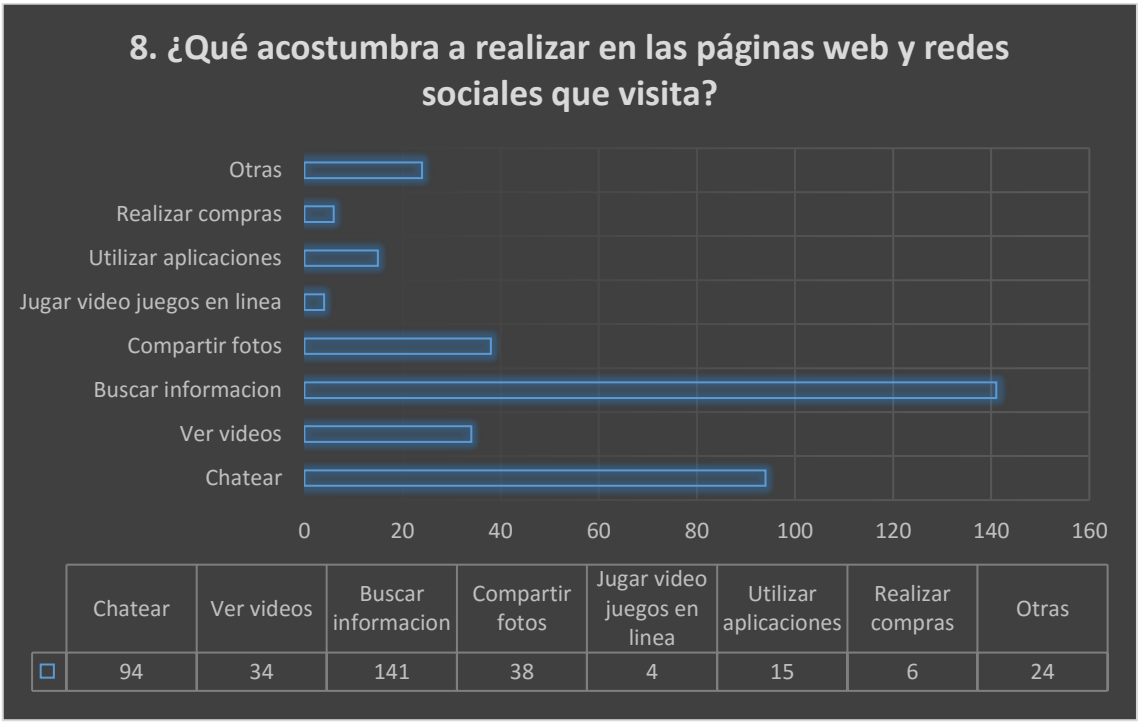


Fuente: Elaborado por el sustentante

Análisis: Se ha comprobado que del total de la muestra, un 53% utiliza Facebook con mucha frecuencia, Instagram con un 27%, Twitter con un 4%, LinkedIn con un 3% y un 13% otras redes.

Facebook es la red social con mayor número de seguidores, por lo que los defraudadores utilizan estrategias para inducir a muchos usuarios a ofrecer

informaciones y datos personales con el fin de obtener beneficios de manera ilegal, realizando daños a los usuarios.

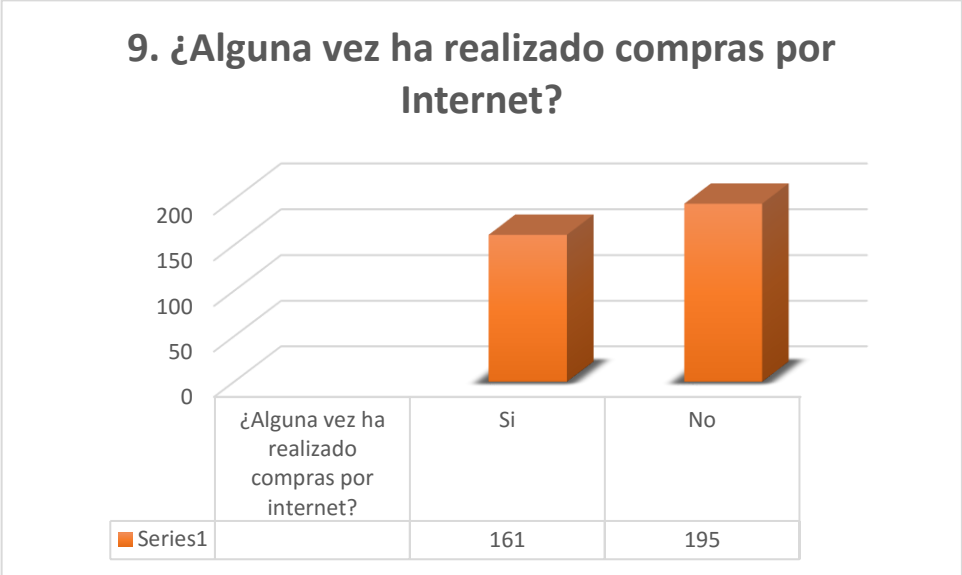


	Chatear	Ver videos	Buscar informacion	Compartir fotos	Jugar video juegos en linea	Utilizar aplicaciones	Realizar compras	Otras
□	94	34	141	38	4	15	6	24

Fuente: Elaborado por el sustentante

Análisis: Se ha detectado que la mayoría de los usuarios ingresan a la web para buscar informaciones de todo tipo, según el interés y las necesidades de cada usuario.

Por lo tanto, la web y las redes sociales ofrecen una gran cantidad de información y todo esto resulta ser un punto clave para que los defraudadores ingresen a estos medios para lograr introducir software para espiar a los usuarios. Sin embargo, 141 personas indicaron que ingresan a dichos medios a buscar información, 94 acceden a las redes para chatear con sus amigos y familiares, 38 comparten fotos, 34 ven videos y 24 realizan otras actividades.



Fuente: Elaborado por el sustentante

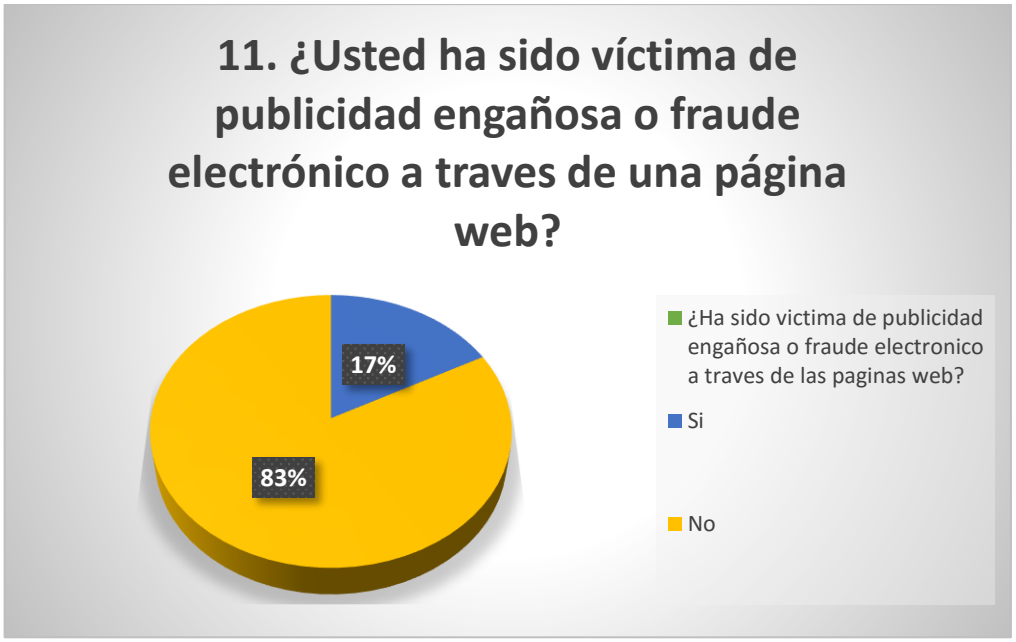
Análisis: Según la investigación, 161 personas indicaron que alguna vez ha realizado compras a través de la web porque según los argumentos de esos usuarios, informan que a través de Internet encuentran artículos a menor precio y mejor calidad. Pero 195 personas indicaron que no, porque no se sienten seguros de realizar compras, a otras personas no les gusta y muchos indican que no tienen tarjeta de crédito y usuario en páginas de compra.

10. Generalmente, ¿en cuales páginas acostumbra hacer sus compras?

Los usuarios encuestados respondieron lo siguiente:

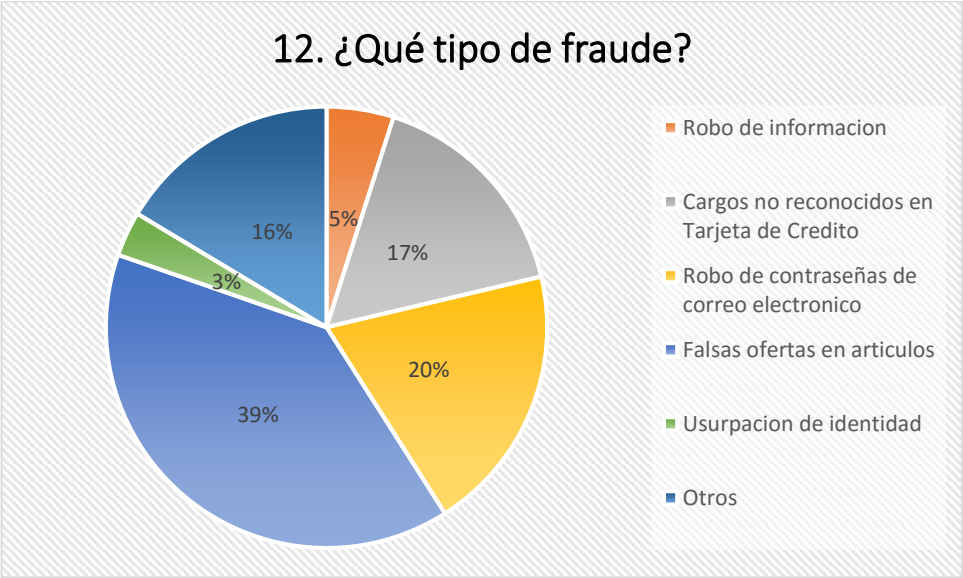
- EBay, Amazon.
- Amazon
- Global industrial
- EBay

- Ninguna
- EBay, Amazon.
- Amazon, 6pm.com, Forever 21.com.
- Amazon
- Amazon
- amazon.com, ebay.com.
- amazon.com, etsy.com, corotos.com.do.
- Old Navy, Victorias Secrets, Party City, Gap, Carters, The children place.
- Amazon, 6pm, forever21, Old Navy.
- Amazon
- www.amazon.com
- EBay, Amazon.
- amazon.com, ebay.com.
- Amazon
- eBay
- www.amazon.com, www.eps.com.do
- Amazon, carters.com
- Old Navy, Amazon, eBay.
- Aeropostal, Victoria Secrets.



Fuente: Elaborado por el sustentante

Análisis: Del 100% de la muestra, un 83% indico que no han sido víctima de fraude electrónico o publicidad engañosa. Sin embargo, se determinó que un 17% alguna vez ha sido víctima de fraude electrónico o publicidad engañosa a través de la web.



Fuente: Elaborado por el sustentante

Análisis: Se ha determinado que el 39% ha sido víctima de publicidad engañosa a través de falsas ofertas en artículos en la web, un 20% han sido objetivo de robo de contraseñas de correo electrónico, teniendo como consecuencia el robo de información y no lograr acceder a su correo. Por otro lado, a un 17% se les realizo consumos a su tarjeta de crédito a través de clonación u otro tipo de fraude llamado Phishing. Un 16% ha sufrido otros tipos de fraude, 5% de robo de información y un 3% de los usuarios se les usurpo su identidad.

13. ¿En qué página web ha visto publicidad engañosa?

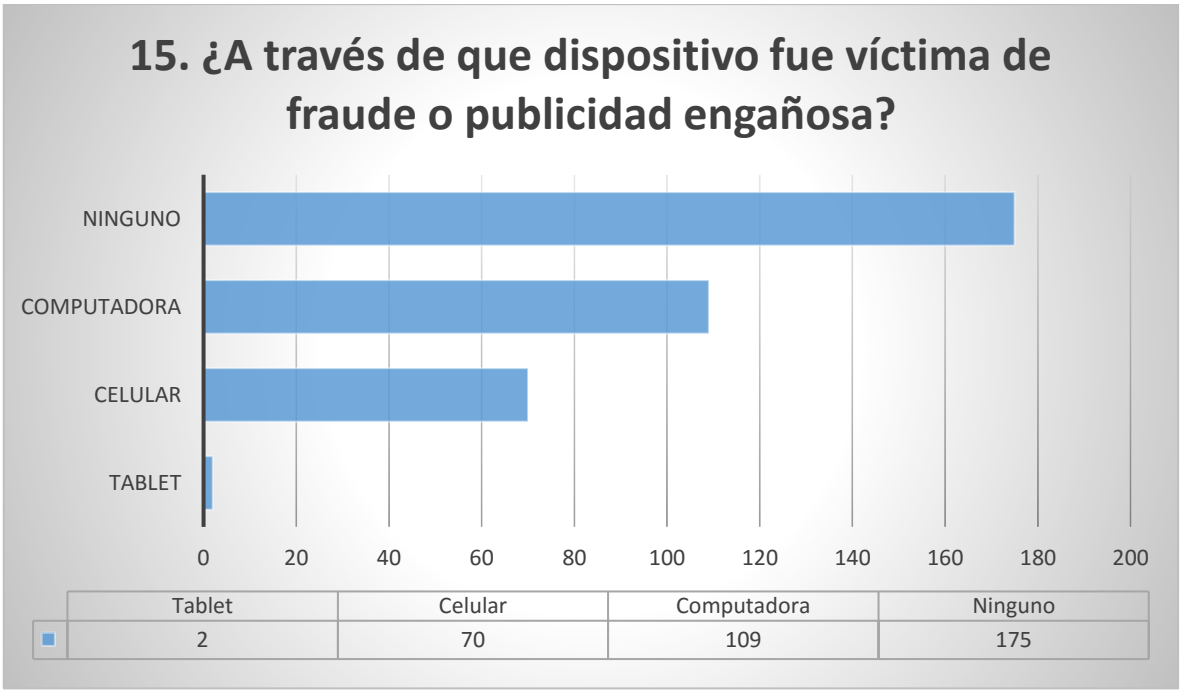
Los usuarios encuestados dieron su opinión respecto a las páginas en donde han visto publicidad engañosa. Las páginas son las siguientes:

- Facebook
- En ninguna
- Amazon
- Viagrupo
- EBay
- Roseweek
- Páginas de películas
- Animeflv.com
- Telemarketing
- Wish.com
- Superofertas.com
- La pulga.com
- Instagram
- Tpido.com
- Burger King.com
- PayPal

Fuente: Elaborado por el sustentante

Análisis: Un gran porcentaje de personas que han sido víctimas de fraude o publicidad engañosa, según lo indicado en la investigación es de 45% en Facebook, siendo esta la mayor red social con más seguidores y a la vez con mayor índice de criminalidad electrónica. Por otro lado, un 49% indico que no ha sido víctima de estas acciones.

Sin embargo, en Instagram y Twitter solamente se detectó un 1% de fraude y publicidad engañosa.



Fuente: Elaborado por el sustentante

Análisis: De la muestra que utiliza el Internet y redes sociales ciento setenta y cinco (175) personas indicaron que en ningún dispositivo ha sido víctima de estas malas prácticas. Sin embargo, se determinó que a través de la computadora ciento nueve (109) personas fueron víctimas mientras usaban su equipo. También, setenta (70) personas fueron defraudadas a través de su celular y dos (2) personas indicaron que fueron defraudadas a través de una Tablet.

16. ¿Qué daños ha sufrido usted como usuario?

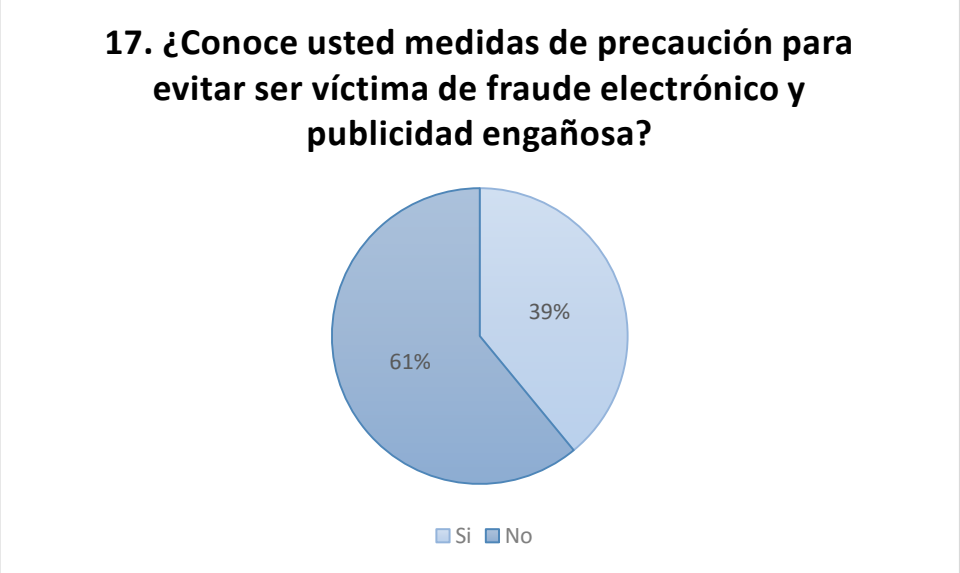
Los usuarios respondieron lo siguiente:

- Han ofertado artículos específicamente en Facebook, donde te piden compartir una foto y seguir por página. Y resulta que al llegar la fecha indicada del concurso, desaparece el anuncio de la promoción del concurso, no hay ganadores, ni artículo. Solo ganan likes y seguidores.

He perdido tiempo, y credibilidad. Además de haber seguido a una página que de acuerdo a mi preferencia no me habría interesado seguir. Y luego hasta se me olvida que página era, para dejar de seguirla.

- Recibí un artículo que no tenía las características que ofrecía la página.
- Pagar dinero e intereses de tarjetas de créditos, por cobro sin autorización de una membresía.
- Compre una chaqueta que nunca llego y un pelo que no era el de la foto.
- Virus en la pc por ir al enlace del anuncio.
- Pérdida de tiempo.
- Sentir inseguridad al querer hacer una transacción.
- Pornografía.
- Ninguno, soy muy cautelosa.
- Como usuario ninguno, solo un falso artículo.
- Pérdida de tiempo y dinero.
- Desconfianza a la hora de buscar en las redes.
- Page unos dólares a la tarjeta de crédito.
- No volver a recuperar mi correo electrónico.
- Pérdida de dinero.
- Hasta el momentos ninguno.
- Ninguno daño nocivo, pero si molestias.
- Pánico al tener que comprarle a otra persona.
- Cargos a mi tarjeta de crédito no reconocidos por mí.
- Hackearon mi cuenta de Hotmail.
- Pérdida de tiempo.
- Cobro no reconocido.

- Robo
- Perdida de dinero y daño emocional.
- Engaños.
- Me clonaron las tarjetas y hackearon varias veces mi mail y Facebook.
- Perdida de información y violación de mi privacidad.
- Desconfianza en la publicidad.
- Han tratado de hackear mi cuenta.
- Informaciones incorrectas.
- Bloqueo de tarjeta para evitar cargo.



Fuente: Elaborado por el sustentante

Análisis: Según la investigación realizada, un 61% de los usuarios no conoce ninguna medida de precaución para evitar caer ante los defraudadores en Internet. A pesar de que es muy bajo el índice de personas defraudadas, muchos no tienen conocimiento de cómo evitar caer ante estos delitos que frecuentemente se están cometiendo en la red. Por otro lado, un 39% indico que

conocen medidas para evitar este tipo de situaciones. Muchos expresaron que es recomendable no introducir datos personales en páginas que no estén certificadas.

18. ¿Cuáles medidas de precaución usted conoce?

Estas fueron las respuestas de la mayoría de los usuarios encuestados:

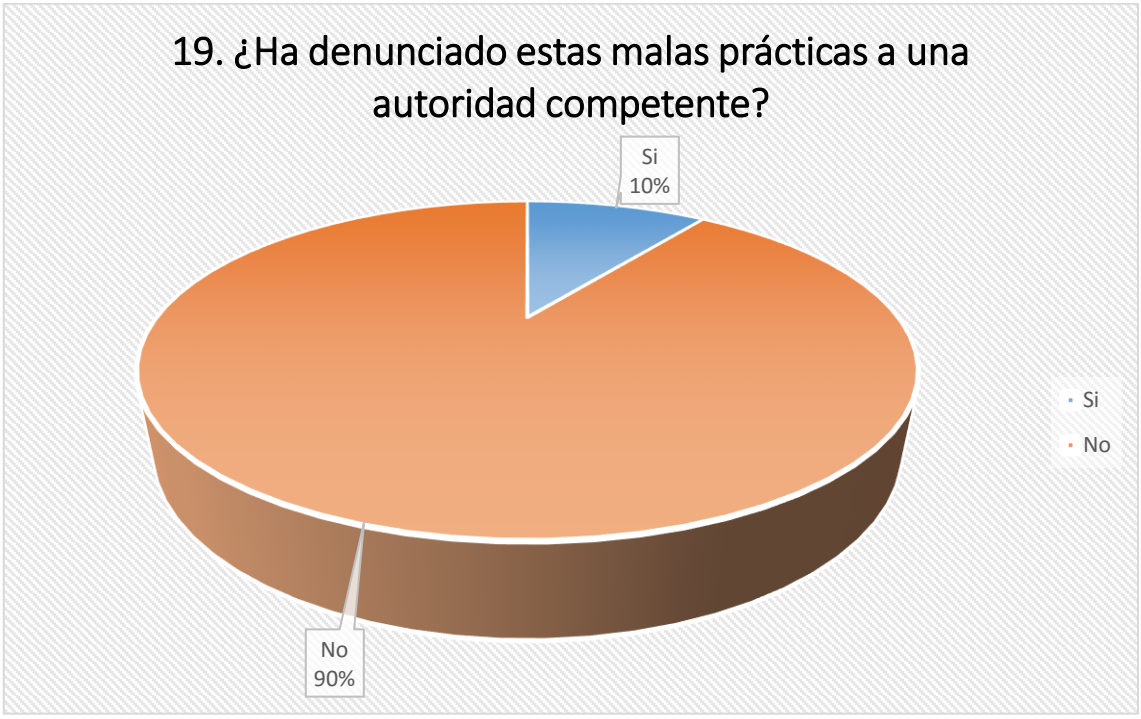
- Principalmente mantener la privacidad de sus datos personales e información financiera.
- Sentido común, conocimiento y manejo de softwares.
- Ninguna
- No ofrecer datos personales, no hacer clic en publicaciones sospechosas.
- No dejar su contraseña en lugares visibles y no agregar personas extrañas.
- No publicar informaciones personales.
- Ver los comentarios de los usuarios que ya compraron.
- Mantener en secreto las claves.
- Las medidas de correcto uso de las tarjetas de crédito.
- Utilizar el navegador en privado, no dar datos personales.
- Antivirus.
- No entrar a páginas bancarias desde buscadores, si no tiene candado no es segura para pagos, que tenga certificado, etc.
- No dar las contraseñas a nadie, no usar las redes en computadoras o dispositivos públicos, mantener sus aparatos bloqueados.
- Una contraseña que contenga mayúsculas, símbolos y números.

- No hacer mi información de perfil pública.
- No dar información personal o bancaria por teléfono.
- Claves de acceso.
- Verificación de validez de la página y búsqueda de comentarios al respecto.
- Comprobar la dirección.
- Revisar la página tenga el icono de candado y el https, navegar como incognito, Softwares, antivirus (ej.: Malware).
- Ninguna, además de ser precavido.
- Visitar páginas registradas.
- No dar datos personales en páginas web sin seguridad.
- No entro a páginas dudosa no doy mi clave.
- La "s" en http para saber que es seguro.
- No dar información personal.
- No entrar en páginas desconocidas.
- Indagando en Internet respecto a la publicidad, no proporcionar datos de clave del correo electrónico.
- El candado donde está la dirección de la página web.
- No poner todos tus datos personales.
- Utilizar una clave que incluya letras mayúscula, minúscula, números y caracteres especiales.
- No dar información personal por esas vías.
- Ser minuciosos en la información que compartimos en las redes sociales. Evitar conectarse a redes Wi-Fi no protegidas. Avisar a la policía ante

cualquier comportamiento sospechoso presentado en la persona con la que se está conversando.

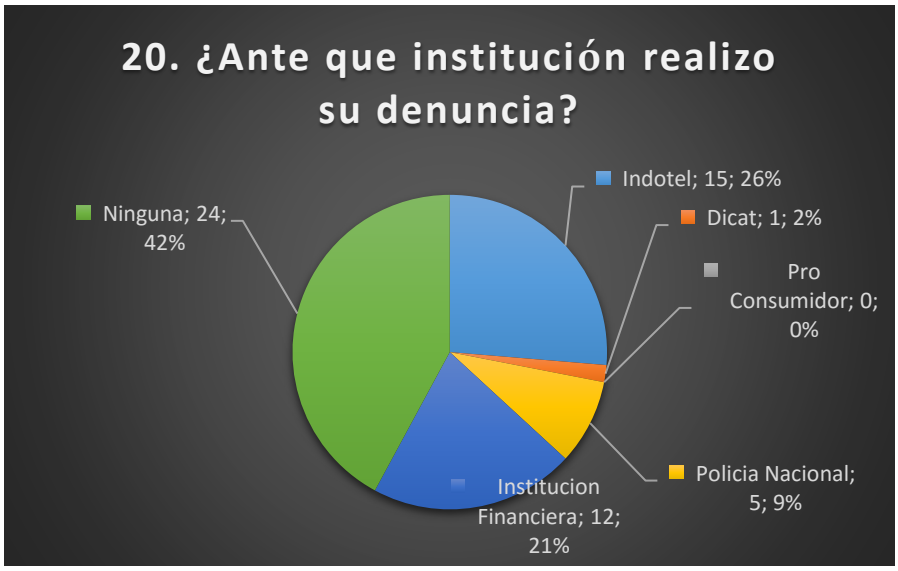
- Poner las redes privadas.
- Ignorar anuncios que aparecen de la nada en la web.
- Utilizar páginas conocidas, no dar información personal a menos que no sea requerida en una compra.
- Mirar siempre la página donde esté.
- No poner datos personales en páginas de conocidas, no añadir tarjetas de créditos o informaciones financieras.
- No abrir links que contenga imágenes vulgares, no colocar contraseñas de sus tarjetas de créditos.
- Dejar correo cerrado cuando no se esté usando el computador.
- No ofrecer contraseñas.
- No dar contraseña, no ingresar a páginas desconocidas.
- No leer correo malicioso.
- No guardar contraseñas en el celular.
- Verificar la reputación del comprador. No comprar en páginas desconocidas o baja reputación.
- Confirmación vía mensaje de texto o llamadas al celular.
- No usar páginas desconocidas, verificar que tiene seguridad la dirección de la página (https), no compartir mis datos con extraños ni colocar mi número de tarjeta en páginas dudosas.
- Asesorarme de las páginas y la publicidad, para así evitar caer en fraude.
- No introducir información sobre domicilio, fechas de nacimiento real, números de teléfonos, etc.

- Leer bien antes de comprar.
- No dar datos personales.



Fuente: Elaborado por el sustentante

Análisis: Se ha concluido que de las personas que han sido víctimas ante el fraude electrónico y la publicidad engañosa, un 90% no ha denunciado estas malas acciones ante una autoridad o institución que vele por la seguridad de los consumidores o usuarios. Por otro lado, un 10% informo que si realizo denuncias a las autoridades competentes.



Fuente: Elaborado por el sustentante

Análisis: De la cantidad de usuarios que fueron defraudados, un 42% no realizó ninguna notificación ante una institución que regule estas malas prácticas que hoy en día se han propagado en la red. Pero un 21% realizo su denuncia a una institución financiera ya que estos fueron defraudados a través de algún producto con la institución competente. Otro 26% realizo su reporte a Indotel, un 2% al Dicat, un 9% a la Policía Nacional y un 0% a Pro Consumidor.

Fuente: Elaborado por el sustentante

Análisis: Según lo indicado, del número de personas que fueron defraudadas a través de la web, 36 personas indicaron que la institución a la cual realizaron su reporte, realizo el trabajo correspondiente de manera eficiente, protegiendo los intereses y deberes del consumidor. Y 21 personas informaron que no fueron resueltos sus inconvenientes reportados.

4.2 Entrevistas

4.2.1 Entrevista a Pro Consumidor

El resultado de la entrevista realizar a Pro Consumidor es el siguiente:

Fecha: 23/06/2016

Nombre: Juana Peguero

Puesto de trabajo: Oficina de Acceso a la información pública

Lugar: PRO CONSUMIDOR

1. **¿Cómo afecta a los usuarios las distintas formas de estafa y publicidad engañosa en las redes sociales y páginas web?**

La publicidad conlleva a una compra compulsiva al consumidor para atraerlo y de esta forma incitar al consumo del producto vendido. Muchas veces ofrecen un precio y características que no son reales.

2. **¿Qué estrategias marketing y publicidad engañosa utilizan los defraudadores en Internet?**

Utilizan diferentes estrategias que atraen a los consumidores, tales como: Falsas ofertas, imágenes de productos irreales, mensajes subliminales.

Todo esto, con el fin de engañar a los usuarios.

3. **¿Qué consecuencias y pérdidas trae el fraude electrónico ante el comercio por Internet?**

Trae muchas consecuencias y genera desconcierto ante el consumidor.

4. **¿Qué recomendaciones usted puede realizar para que los usuarios eviten ser víctimas de la publicidad engañosa y fraude electrónico?**

Verificar que tan real es la publicidad y si el artículo corresponde con las características que ofrece la publicación. También, realizar una compra inteligente, ver todos los detalles del producto para evitar caer en estas trampas vía Internet.

Muchas gracias por su tiempo

4.2.2 Entrevista en Ministerio de Industria y Comercio

Entrevista a personalidad del Ministerio de Industria y Comercio

Fecha: __07/07/2016_____

Nombre: José Antonio Rodríguez Mena

Puesto de trabajo: Soporte Administrativo

Lugar de trabajo: Viceministerio de Comercio Interno / Ministerio de Industria y Comercio, MIC

1. **¿Cómo afecta a los consumidores el fraude electrónico a través de la compra por Internet?**

Estos hechos afectan de manera negativa a los clientes o consumidores que realizan transacciones de compra vía Internet. Dicha situación genera desconfianza, por lo tanto, el volumen de ventas de una empresa puede reducirse por el auge del fraude electrónico.

2. **¿Cuáles consecuencias sufren las empresas que se dedican al comercio electrónico por el auge de las estafas en Internet?**

- Reducción en las ventas
- Pérdida de clientes
- Aumento en los inventarios.
- Mayor tiempo para hacer llegar el producto hacia el consumidor.

3. **¿Qué actividades coordina el Ministerio de Industria y Comercio para concientizar a los comerciantes y consumidores finales sobre sus derechos y precauciones al momento de la compra?**

El Ministerio de Industria y Comercio realiza actividades de orientación al comerciante y colaboración con las pequeñas empresas que se está agregando al mercado, con los fines de que puedan generar ingresos y ganar la confianza de sus clientes.

4. **¿Qué recomienda usted a los usuarios para evitar caer ante el fraude electrónico?**

Es bueno orientarse bien de cómo realizar compras a través de Internet, de manera que podamos evitar ser defraudado. También, no debemos ofrecer nuestros datos personales en páginas o comercios que no estén certificados.

Muchas gracias por su tiempo

CONCLUSIONES

Tomando como base los objetivos de esta investigación, en los últimos años miles de empresas están comercializando a través de las páginas web y redes sociales con el objetivo de obtener relaciones con los clientes, beneficios económicos e intercambio de bienes y servicios. Esto ha dinamizado las economías de los países y cada vez más se va desarrollando los negocios electrónicos.

El Internet cada vez más está llegando a todos los hogares, por lo que miles de personas tienen acceso a las telecomunicaciones con el fin de obtener facilidad de comunicación entre sí.

Sin embargo, queda demostrado que existen numerosas formas de engañar a los usuarios de servicios de telecomunicaciones, el uso masivo de publicidad engañosa ha provocado pérdidas de dinero a miles de personas que navegan en Internet e interactúan en redes sociales al momento de acceder a realizar alguna compra o suscribirse a alguna aplicación.

Por lo tanto, hoy en día se utilizan software para realizar fraude electrónico a través de estos medios. Algunos de los softwares más utilizados y que frecuentemente los defraudadores tienen éxito al utilizarlos, tales como:

- Malware
- Troyano
- Spyware
- Spam
- Gusanos
- Adware
- Keyloggers
- Entre otros

Estos son los programas más utilizados para el robo de información a los usuarios y existe un alto índice de personas que han sido infectadas a través de páginas de Internet y en las redes sociales, tan solo dando clic a alguna publicación no oficial o falsa.

Muchos de los defraudadores o hackers utilizan estrategias para atraer a los usuarios a publicaciones que no son reales a través de técnicas de publicidad desleal para engañar y estafar. Incluso, utilizan estrategias de marketing para vender “productos” de calidad vía la web para persuadir a los consumidores e inducir a la compra.

La publicidad engañosa está abarrotando el Internet y miles de personas que son usuarios de Internet, son propensos a caer ante el fraude a través de publicidad no leal. Por consiguiente, la investigación se ha demostrado que un

gran número de personas han visto y han sido víctimas de publicidad engañosa en las redes sociales y en Internet. Esto genera descontentos en las personas que utilizan estos medios para interactuar con amigos y familiares, también a personas que se dedican a comercializar bienes y servicios. Por lo tanto, esto afecta el comercio electrónico y minimiza la efectividad de los servicios a través de la web.

Algunas páginas en las que los usuarios han sido defraudados, en su gran mayoría son sitios web de venta de productos y servicios, tales como: EBay y Amazon. Se ha verificado que muchos clientes de estas páginas, alguna vez han visto publicidad engañosa y otros han realizado compras de artículos que nunca les han llegado y muchas veces el producto no resulta ser el mismo que está en la web y con las características que ofrece la página.

Por consiguiente, muchos expertos y el Instituto Nacional de las Telecomunicaciones (Indotel), hacen recomendaciones que son factibles para los usuarios y de gran utilidad para evitar caer ante las diferentes trampas que están en la web.

Se ha determinado que los usuarios que no ofrecen sus datos personales en páginas no certificadas, son menos propensos a ser defraudados. También, no instalar programas sospechosos en el computador, celular, Tablet u otro dispositivo que trabaje con un sistema operativo, evitara que el usuario sea

engañado por publicidad engañosa que se instala en los navegadores y en las distintas páginas web y redes sociales que los usuarios visitan.

Existen empresas que en sus sitios web ofrecen productos que no son acordes con la realidad de los mismos. Un ejemplo de esto es McDonald, una empresa de comida rápida. Muchas veces utiliza publicidad engañosa en sus sitios web y redes sociales para persuadir a los consumidores o clientes para llevarlos al establecimiento comercial e inducirlos a la compra de sus productos.

Por otro lado, se ha comprobado que los hackers ponen en circulación virus a través de las redes sociales para el robo de información a los usuarios, con el fin de acceder a cuentas bancarias y realizar transacciones fraudulentas como el “Phishing”, que es muy común hoy en día en el sector de las telecomunicaciones y en la Banca electrónica. Un alto índice de clientes de distintas instituciones bancarias fueron defraudados a través de Internet y se les ha robado información por medio del correo electrónico.

Por consiguiente, las empresas tienen un compromiso importante, ya que deben de cumplir con los estándares de calidad de sus servicios y tener responsabilidad social conforme a las leyes establecidas en el sector de las telecomunicaciones. Es responsabilidad de las empresas prestadoras de servicios de telecomunicaciones, preservar la identidad de los usuarios y ofrecer un servicio óptimo.

Por lo tanto, es de importancia que cada entidad y usuarios, asuman el compromiso de orientarse sobre todos los detalles que indica la ley de telecomunicaciones para evitar realizar cualquier tipo de fraude o ser defraudado.

RECOMENDACIONES

Con el fin de garantizar la seguridad de los usuarios a través de los distintos servicios de telecomunicaciones en Internet y las redes sociales, esta investigación ha desenlazado las distintas técnicas para defraudar a las personas y también se ha identificado muchas formas de evitar ser víctima de publicidad engañosa y fraude electrónico. Se recomienda:

- ✓ Todas las instituciones encargadas de regular las leyes de los consumidores a través de las telecomunicaciones, deben de realizar un plan estratégico de orientación a los usuarios para que estos puedan estar precavidos ante las distintas trampas que hay en la Internet.

- ✓ Es de suma importancia crear una campaña publicitaria a través de las páginas web y redes sociales. De manera interactiva y dinámica, ofreciendo informaciones contundentes sobre las amenazas que existen en la web y las consecuencias al momento de ofrecer informaciones personales a desconocidos e introduciéndolas en sitios de Internet que no son seguros. Orientar y brindar información de seguridad virtual a todos los usuarios que realizan compras a través de Internet.

- ✓ Realizar conferencias de seguridad cibernética como inicio de futuros proyectos para crear innovaciones en el sector de telecomunicaciones con el fin de garantizar la protección de los usuarios.

- ✓ También, se recomienda a las instituciones estatales que se encargan de regular las telecomunicaciones y la protección al usuario. Diseñar un programa informático o software que sirva para alertar a los usuarios sobre las distintas páginas a las cuales no se debe acceder por su bajo nivel de seguridad y a la vez que dicho software haga recomendaciones a los usuarios sobre las nuevas tendencias de fraude electrónico, emitiendo mensajes breves de cómo protegerse y que realice notificaciones de las diferentes pautas que establece la Ley de Telecomunicaciones No.153-98.

De esta manera, los usuarios constantemente recibirán notificaciones en sus dispositivos móviles, sobre nuevas tendencias en la web sobre fraude electrónico y publicidad engañosa y a la vez ofreciendo información útil para el usuario, para evitar caer ante las distintas estrategias que utilizan los defraudadores.

Por otro lado, las páginas que son afectadas por ataques cibernéticos deben de utilizar software de gran seguridad para evitar ser enlace o servir como vía para propagar virus y publicidad engañosa para engañar a los usuarios. Eliminar toda publicidad fraudulenta en los laterales de las páginas que muchas veces los usuarios acceden por error al dar clic en la publicación.

También, se recomienda a los usuarios utilizar software o antivirus que bloquean todo tipo de publicidad malintencionada y modificar los protocolos de seguridad de los equipos a los que accede a diario. Esto es con el fin de lograr mantener

la seguridad de la información personal y garantizar el buen funcionamiento de los equipos electrónicos. Por lo tanto, se debe de ser cauteloso, estar bien informado sobre los derechos que tienen los usuarios en la web.

Es vital saber qué instituciones respaldan la seguridad de los usuarios para saber a qué lugar acudir al momento de realizar una reclamación por alguna estafa o robo de información a través de Internet. Por consiguiente, es compromiso de todas las personas tener conocimiento sobre las leyes que regulan las telecomunicaciones y hacer hincapié en los distintos métodos de seguridad para evitar ser defraudado.

BIBLIOGRAFÍA

Angel Ibeas Portilla, J. M. (2000). e-logistics(I). Nuevas tecnologias de la informacion. Sant Andreu de la Barca (Barcelona): Novoprint, SA.

Aragon, M. E. (2014). La Publicidad (Marketing en la actividad comercial). Pozuelo de Alarcon, Madrid: Editex, S.A.

Cano, D. (2011). Contra el Fraude. Naucalpan de Juarez, Mexico: Ediciones Granica Mexico, S.A. de C.V.

Constantino Perez Vega, J. M. (2007). Sistemas de Telecomunicacion. España: Eujoa Artes Graficas.

Erostarbe, I. I. (2005). *Como crear una web docente de calidad.* Madrid: Gesbiblo, S.L.

Figueiras, A. (2002). Una panoramica de las telecomunicaciones. España: Pearson Educacion, S.A.

Frederic Barbier, C. B. (2007). Historia de los medios: de Diderot a Internet. Buenos Aires: Ediciones Colihue S.R.L.

Gustavo Docampo Otero, E. (2000). La radio antigua. España: Marcombo, S.A.

Hiddekel Morrison, M. (2005). Las Telecomunicaciones en Republica Dominicana. Republica Dominicana: Editora Republica Dominicana.

Hiddekel Morrison, M. (2005). Las Telecomunicaciones en Republica Dominicana. Republica Dominicana: Editorial Republica Dominicana.

Higuera, M. A.-Z. (2001). Fraude y corrupción en la arquitectura del Siglo de Oro. Santander: Graficas Calima, S.A.

Hurtado, A. G.-C. (2011). *Seguridad Informatica.* Madrid: Ediciones Paraninfo, SA.

Isaac Alfonso Devis Granados, E. R. (2008). Derecho de los usuarios de las telecomunicaciones. Colombia: Editorial Universidad del Rosario.

Maria Del Pilar Alegre Ramos, A. G.-C. (2011). Seguridad Informatica . Madrid: Ediciones Paraninfo.

Miguel Moro Vallina, A. R. (2014). Marketing Digital: Comercio y Marketing. Madrid: Ediciones Paraninfo, SA.

Miguel Moro Vallina, A. R. (2014). Marketing Digital: Comercio y Marketing. Madrid, España: Ediciones Paraninfo, SA.

Mora, S. L. (2002). Programacion de aplicaciones web: historia, principios basicos y clientes web. San Vicente, España: Editorial Club Universitario.

Moya, J. M. (2006). *Redes y servicios de telecomunicaciones.* Madrid: Thomson.

Perez, E. H. (2004). Introduccion a las telecomunicaciones modernas. Mexico: Limusa.

Prato, L. B. (2010). Aplicaciones Web 2.0 - Redes Sociales. Villa Maria: Eduvim.

Salinas, S. S. (2003). Internet y Correo Electronico. Informacion y Comunicacion. España: Ideas Propias Editorial.

Sampieri, R. H. (2006). Metodologia de la Investigacion. Iztapalapa, Mexico : McGraw-Hill Interamericana.

Sánchez-Ocaña, A. S. (s.f.). La Web 2.0 ... y la madre que la Parió. Madrid: Lulu.com.

Serrano, M. J. (2012). Comunicacion y atencion al cliente. Madrid: Ediciones Paraninfo, S.A.

Szymanczyk, O. (2013). Historia de las telecomunicaciones mundiales. Buenos Aires: Editorial Dunken.

Talaya, A. E. (2008). Principios de Marketing. Ponzuelo de Alarcon, Madrid: ESIC, Editorial.

Uceda, M. G. (2011). Las claves de la publicidad. Pozuelo de Alarcon, Madrid: ESIC EDITORIAL.

Uceda, M. G. (2011). *Las claves de la publicidad.* Madrid: Esic Editorial.

PÁGINAS WEB

153-98, L. G. (27 de Mayo de 1998). *Instituto Dominicano de las Telecomunicaciones (INDOTEL).* Obtenido de http://indotel.gob.do/wp-content/uploads/2015/11/Ley_153_98_Telecomunicaciones-1.pdf

20 Minutos. (28 de Diciembre de 2012). Obtenido de http://www.20minutos.es/noticia/1688800/0/estafas-internet/timos-engano/formas/

Alegsa, L. (12 de Mayo de 2010). *Alegsa.com*. Obtenido de http://www.alegsa.com.ar/Dic/trafico%20web.php

Aranda, V. T. (25 de Diciembre de 2004). *Autores Cientifico-Tecnicos y Academicos.* Obtenido de http://www.acta.es/recursos/revista-digital-manuales-formativos/298-el-nacimiento-de-la-informatica-personal

Ardila, I. (23 de Octubre de 2013). *P&M Publicidad & Mercadeo*. Obtenido de http://www.revistapym.com.co/noticias/comercio-electronico/9-tipos-fraude-online

BBC Mundo. (17 de Septiembre de 2015). Obtenido de http://www.bbc.com/mundo/video_fotos/2015/09/150915_tecnologia_estafas_redes_sociales_lv

Consumidor, P. (2014). *Pro Consumidor Instituto Nacional de Proteccion de los Derechos del Consumidor.* Obtenido de http://www.proconsumidor.gob.do/files/16-2014.pdf

Diario Libre. (10 de Junio de 2016). Obtenido de http://www.diariolibre.com/noticias/fraudes-bancarios-son-el-80-de-los-ciberdelitos-FLDL477561

Eduinnova. (Enero de 2010). Obtenido de http://www.eduinnova.es/ene2010/Tipos_publicidad.pdf

El Pais.com. (18 de Abril de 2015). Obtenido de http://www.elpais.com.co/elpais/internacional/noticias/facebook-aplaca-vendedores-me-gusta-fraudulentos-su-red-social

El Tiempo. (8 de Septiembre de 2010). Obtenido de http://www.eltiempo.com/archivo/documento/CMS-7897770

ourquet, M. (29 de Diciembre de 2015). *Marketing Digital*. Obtenido de https://marcelofourquet.wordpress.com/2015/12/29/fraude-publicitario-ad-blockers-como-reducir-su-impacto/

Garcia, L. (24 de Enero de 2010). *SBD SecurityByDefault.com*. Obtenido de http://www.securitybydefault.com/2010/01/origen-y-evolucion-del-efraude.html

Gomez, L. (19 de Febrero de 2015). *Beevoz*. Obtenido de http://www.beevoz.com/2015/02/19/historia-de-la-television-origenes-evolucion-y-curiosidades/

Heredia, V. M. (Abril de 2010). *Wikitel*. Obtenido de http://wikitel.info/wiki/Rep%C3%BAblica_Dominicana:_Marco_Jur%C3%ADdico_y_Fiscal

Herrera, P. &. (31 de Julio de 2012). *Pellerano & Herrera. Attorneys at law.* Obtenido de http://phlaw.com/imagen?file=articulos/282/34ley-general-telecomunicaciones-no-153-98-republica-dominicana34

INDOTEL. (2015). *Instituto Dominicanao de las Telecomunicaciones*. Obtenido de http://indotel.gob.do/indotel/sobre-nosotros/origenes/

INDOTEL. (2015). *Instituto Dominicano de las Telecomunicaciones.* Obtenido de http://indotel.gob.do/category/leyes-oai/

Marketing Directo. (31 de Enero de 2011). Obtenido de http://www.marketingdirecto.com/digital-general/social-media-marketing/breve-historia-de-las-redes-sociales/

OSI Oficina de Seguridad del Internauta. (13 de Mayo de 2015). Obtenido de https://www.osi.es/es/actualidad/avisos/2015/05/mucho-cuidado-con-los-tweets-promocionados.html

Petovel, P. (01 de Noviembre de 2012). *Merca2.0*. Obtenido de http://www.merca20.com/10-claves-para-prevenir-fraudes-en-internet/

Piantini, Y. C. (12 de Noviembre de 2011). *Escuela de Organizacion Industrial*. Obtenido de http://www.eoi.es/blogs/yoenaicharitoperez/2011/11/12/un-poco-sobre-la-historia-de-las-telecomunicaciones-en-republica-dominicana/

Ponzio, G. (22 de Septiembre de 2014). *GROU Crecimiento Digital*. Obtenido de https://blog.grou.com.mx/fraude-en-internet-genera-cambios-al-marketing-digital#sthash.JZcjfRvj.dpbs

Publicidad. (10 de Agosto de 2015). *Marketing Directo*. Obtenido de http://www.marketingdirecto.com/actualidad/publicidad/el-drama-del-fraude-en-la-publicidad-online-son-los-clientes-los-unicos-perjudicados/

Saavedra, C. A. (20 de Agosto de 2009). *Universidad ICESI*. Obtenido de http://www.icesi.edu.co/blogs_estudiantes/emicasanchez/2009/08/20/tipos-de-paginas-web/

Tejeda, L. (20 de Noviembre de 2015). *Listin Diario*. Obtenido de http://www.listindiario.com/economia/2015/11/20/396914/crecen-quejas-de-fraude-y-cargos

Veras, T. (13 de Enero de 2010). *La cabina de Teo Veras*. Obtenido de http://www.teoveras.com.do/breve-resena-historica-de-la-radiodifusion-en-la-republica-dominicana.html#.Vz-7ppF97IU

Wikipedia. (25 de Marzo de 2016). *Wikipedia La enciclopedia libre*. Obtenido de https://es.wikipedia.org/wiki/Instagram

ANEXOS

DECANATO DE CIENCIAS ECONÒMICAS Y EMPRESARIALES
ESCUELA DE MERCADOTECNIA

Anteproyecto de Tesis de Grado para Optar por el Título de Licenciatura en Mercadotecnia

Estrategias de Marketing, fraudes y publicidad engañosa en las redes sociales y páginas web en el sector de telecomunicaciones en República Dominicana desde el año 2014 hasta el 2015.

SUSTENTADO POR:

Charlie Enrique Perez Acosta
2009-1582

ASESOR (A):
María Luisa Montás

Santo Domingo Distrito Nacional, República Dominicana
2016

Los conceptos expuestos en esta investigación, son de exclusiva responsabilidad del autor.

ÍNDICE

TÍTULO

ESTRATEGIAS DE MARKETING, FRAUDES Y PUBLICIDAD ENGAÑOSA EN LAS REDES SOCIALES Y PAGINAS WEB EN EL SECTOR DE TELECOMUNICACIONES EN REPÚBLICA DOMINICANA DESDE EL AÑO 2014 HASTA EL 2015

1.1 INTRODUCCION

Las actividades de comercialización de productos, bienes y servicios han desarrollado y dinamizado el comercio en todos los ámbitos. Actualmente las empresas están implementando estrategias para ingresar a nuevos segmentos de públicos a los que quieren hacer llegar sus bienes y servicios.

Los medios digitales están a la vanguardia en los últimos años. El marketing ha logrado introducirse en los medios digitales creando estrategias de promoción de ventas y captación de clientes potenciales que utilizan dichos medios para comunicarse con otras personas, buscar información, comprar productos, etc.
Esto es de provecho para las empresas ya que pueden lograr introducir publicidad en los laterales de las páginas web y redes sociales según las necesidades de los clientes. De manera que puede ser atractiva para lograr vender y distribuir bienes y servicios.

Esta investigación tiene como objetivo estudiar las distintas estrategias de marketing, fraudes y publicidad engañosa en los medios digitales en el sector de telecomunicaciones con el fin de identificar las los métodos utilizados para realizar este tipo de acciones.

2.1 JUSTIFICACION

En los últimos años, la importancia de los servicios e interacción con los clientes de manera más personalizada a través de los distintos medios de comunicación, han logrado revolucionar las tendencias en los servicios y la forma en que estos se ofrecen al público al que va dirigido. Las estrategias de marketing y publicidad a través de las redes sociales y páginas web son de mucha importancia para la atracción de nuevos públicos y lograr vender, satisfacer necesidades y posicionar una marca.

Sin embargo, hoy en día la industria de telecomunicaciones tiene un gran reto para combatir el fraude electrónico, que consiste en el robo de información al usuario a través de distintas aplicaciones en la Internet. También existe lo que llamamos publicidad engañosa, que cosiste en colocar informaciones distintas a las que ofrece una marca, con el objetivo de engañar al cliente.

El objetivo de esta investigación es determinar cómo influye en el consumidor que se están utilizando para el robo de información y fraudes a través de publicidad engañosa y marketing en las redes sociales y páginas web. Esto ayudará a las empresas a identificar cuales métodos se están implementando para realizar este tipo de acciones.

Además, contribuirá con la implementación de nuevas estrategias para proteger a los usuarios y su información personal.

3.1 DELIMITACION DEL PROBLEMA Y PLANTEAMIENTO DEL PROBLEMA

3.1.1 Delimitación

Esta investigación se basará en delimitar las estrategias de marketing, fraudes y publicidad engañosa en las redes sociales y páginas web en el sector de telecomunicaciones, bajo la Ley No.53-07 sobre Crímenes y Delitos de Alta Tecnología. En la ciudad de Santo Domingo, República Dominicana. Durante el periodo correspondiente al 2014-2015.

3.1.2 Planteamiento del problema

El mundo de las telecomunicaciones, en la actualidad está a la vanguardia, interconectando servicios y facilidades para los consumidores con el fin de ofrecer paquetes de beneficios y ofertas de interés para satisfacer necesidades y lograr una gran captación de clientes.

A través de los medios de comunicación digitales como redes sociales y páginas web, las empresas colocan publicidad ofreciendo servicios y distintas ofertas que son de interés para las personas que regularmente utilizan estos medios.

Con la colocación de publicidad en los laterales de las páginas web y anuncios a través de aplicaciones vía las redes sociales tales como: Facebook, Twitter e LinkedIn. Muchos usuarios con falsas identificaciones, tales como los llamados hackers o usurpadores de medios digitales se aprovechan de estos medios para emitir informaciones engañosas con la colocación de publicidad, con el fin de robar identidad, informaciones personales, dinero, entre otras informaciones de interés para estas personas.

Estas personas utilizan distintas estrategias a través de las redes que son enmascaradas a través de múltiples aplicaciones que motivan a los usuarios a ingresar para poder utilizarlas pero detrás de todo esto, esas aplicaciones redirigen al usuario fuera de la red social o página web hacia otra página donde se le pide al usuario ingresar ciertas informaciones tales como: correo electrónico, edad, sexo, número telefónico, etc. A través de esta solicitud, el usuario se ve expuesto a recibir notificaciones a su correo electrónico de manera masiva, invitaciones para ingresar a dicha aplicación e instalar un programa en el equipo.

Por otro lado, envío de mensajes instantáneos a los teléfonos celulares de distintas compañías telefónicas para el robo y consumo de facturas, y realización de llamadas generando cargos y fraudes a las cuentas de los clientes afectados. De esta forma los hackers pueden lograr ingresar a toda la información personal de los usuarios.

3.2 Formulación del Problema

¿Cuáles son las estrategias de marketing, fraudes y publicidad engañosa en las redes sociales y páginas web en el sector de telecomunicaciones en República Dominicana durante los periodos 2014 – 2015?

3.2.1 Sistematización del Problema

1. ¿Cuáles son los tipos de estrategias de fraudes y publicidad engañosa que han causado mayor daño a los usuarios en el periodo 2014 – 2015?
2. ¿Cuáles software son los más utilizados para el robo de información al usuario?
3. ¿Cuáles empresas de telecomunicaciones resultan ser más vulnerables ante el fraude electrónico?
4. ¿Cuáles páginas web son más propensas a ser afectadas por la publicidad engañosa y fraudes?
5. ¿Cuáles son las medidas de precaución que están implementando las empresas de telecomunicaciones para evitar las transacciones fraudulentas?

4.1 OBJETIVOS

4.1.1 Objetivo General:

Conocer y analizar las estrategias de marketing, fraudes y publicidad engañosa en las redes sociales y páginas web en el sector de telecomunicaciones durante el periodo 2014 – 2015.

4.1.2 Objetivos Específicos:

- Identificar los distintos fraudes a través de publicidad engañosa que han afectado a usuarios durante el periodo 2014 – 2015.
- Identificar cuáles software son los más utilizados para el robo de información y espionaje cibernético.
- Conocer las medidas necesarias para evitar ser víctima de estafa y las recomendaciones realizadas por el Instituto Dominicano de Telecomunicaciones (INDOTEL).
- Investigar cuales empresas, páginas web y redes sociales del sector de telecomunicaciones que son más vulnerables ante el fraude electrónico y publicidad engañosa.
- Investigar las medidas de precaución que toman las empresas de acuerdo a lo que indica la ley en estas malas prácticas.

CAPÍTULO I

5.1 Marco Referencial

5.1.1 Marco Teórico

Las quejas ocasionadas por supuesto fraude y aplicación de cargos no reconocidos o indebidos, son los mayores reclamos de los dominicanos en las entidades orientadas a proteger a los consumidores o usuarios de los servicios de telecomunicaciones, del sistema financiero, en electricidad y en consumo de alimentos.

Según Lilian Tejada (2015) en su artículo en el www.listindiario.com, en la sección de Economía señala que "Ese tipo de quejas ha ido en aumento, de acuerdo a las estadísticas de las propias instituciones, como el Instituto Dominicano de Telecomunicaciones (INDOTEL); el Departamento de Pro usuario, de la Superintendencia de Bancos; el Instituto de Protección al Consumidor (Pro Consumidor) y del Protecom".

"En telecomunicaciones el mayor reclamo se registra en la telefonía alámbrica, seguida de la inalámbrica (móviles o celulares), lo que ha llevado al Indotel a obligar a las proveedoras de todos los servicios a reembolsar a los usuarios más de RD$87.3 millones en 12 años (2003-2015). En octubre de este año se registraron 661 reclamos de los usuarios de celulares, 153 en el uso del internet, 121 en los que usan cables, en su mayoría llevado a cabo de forma personal.

Los usuarios de servicios de telecomunicaciones fueron a hacer sus quejas personalmente, mientras que los demás utilizaron el recurso del internet, por teléfono, a través de la Oficina Presidencial de Tecnologías de la Información y la Comunicación (Optic); mediante el punto GOB, y por correspondencia. A favor de las prestadoras de servicios de telecomunicaciones se determinó un monto superior a RD$38.2 millones de agosto 2003 a octubre 2015".

Además en el portal Marketing Directo (2015) en la sección Publicidad informa que "la sombra del fraude en la publicidad online se ha ido extendiendo de forma silenciosa en los últimos meses poniendo en jaque a un sector que no sabe muy bien como solventar este problema. En junio de 2013, Bob Hoffman, director general y presidente de Hoffman/Lewis Advertising, agencia especializada en retail marketing, señalaba que nos encontrábamos ante un escándalo que superaba los 7.500 millones de dólares".

Este dejó claro en su momento que las redes de anuncios, compradores de medios y agencias de publicidad venden anuncios sabiendo que más o menos la mitad de los que se compren jamás serán vistos por seres humanos de carne y hueso. Señalaba que las redes publicitarias venden a sabiendas del creciente aumento del tráfico bot en los editores ya que las impresiones obtenidas en los anuncios hacen ganar dinero a coste de los clientes que están pagando precisamente por esas impresiones. Unas acusaciones que lo cierto es que no tuvieron mucha repercusión en su momento pero que ahora, cuando miles de millones de dólares y cientos de puestos de trabajo se encuentran en la cuerda floja, cobran una especial relevancia.

El principal problema reside precisamente en las bases de medición de la propia industria. La publicidad online se basa en las impresiones y una impresión, ocurre siempre que una máquina o red publicitaria responde a una solicitud de otro equipo como por ejemplo, un navegador. Aquí los seres humanos poco o nada tiene que ver por lo que hablar de impresión como un usuario que ha visto un determinado anuncio no es una afirmación del todo cierta.

La pregunta que surge ahora es, ¿por qué nadie está poniendo esto de relieve? El Interactive Advertising Bureau (IAB) emitió el pasado mes de diciembre unas directrices por las que las redes de publicidad deberían tener como objetivo un 70% de visibilidad, Facebook anunció que se encuentra trabajando con el Media Rating Council (MRC) para desarrollar unos estándares más robustos de impresiones visibles.

Por su parte, la American Association of Advertising Agencies, la Association of National Advertisers e IAB, anunciaron el pasado año la creación de una nueva organización, Trustworthy Accountability Group para luchar contra los problemas de la publicidad online como es eliminar el tráfico fraudulento, combatir el malware, luchar contra la piratería en internet y promover una mayor transparencia.
(Publicidad, 2015, www.marketingdigital.com)

Por consiguiente, cerca de 36 por ciento de todo el tráfico en la web en Estados Unidos es falso, creado por computadoras infectadas con virus y programadas

para visitar sitios web, según estimaciones recientes de Interactive Advertising Bureau (IAB), una asociación con sede en Nueva York que agrupa a empresas de medios y tecnología que analizan los tipos de mercadotecnia, las estrategias de marketing de servicios y los tipos de publicidad en internet.

El tráfico falso, que en inglés se llama “bot”, engaña a los anunciantes ya que las empresas normalmente, en el marco de su plan de marketing pagan por los avisos cada vez que estos aparecen en respuestas a las visitas de usuarios a determinadas páginas de Internet, independientemente de si los cibernautas son personas de carne y hueso.

Los estafadores crean sitios con tráfico falso, en base a una estrategia seo, y recaudan pagos de empresas a través de los intermediarios que combinan el espacio de muchos sitios y que luego revenden para la mayoría de los anunciantes en la web.

(Ponzio, 2014)

Por consiguiente, según Fourquet (2015) en su artículo Marketing Digital, el fraude publicitario en Internet se apoya en los modelos de “pago por clic” y de “pago por impresiones” que hoy dominan el mercado de publicidad online.

Los estafadores crean redes de páginas web cuyo único contenido son banners y videos, para luego inscribir estos sitios en redes de publicidad digital o AdNetworks.

A continuación, estos sitios son visitados por programas automáticos (“bots”) que simulan clics, impresiones y visualizaciones, sin que ningún usuario real esté delante de ellas.

El creador de la red de páginas web cobra en función de los acuerdos que tenga con la red de publicidad digital. El 99% de ese dinero corresponde a beneficios netos, es difícil de creer que la totalidad del dinero se quede solo en manos del estafador.

Más de la mitad del presupuesto publicitario se dilapida como consecuencia del llamado “tráfico no humano”. Es decir que más de la mitad del tráfico, el engagement y las visualizaciones de marca, no son más que estos “bots” usados para falsear los datos de resultados obtenidos por la publicidad online.

Los anunciantes se ven obligados a afrontar el coste de dichas acciones publicitarias, que nunca llegan a alcanzar a los consumidores.

Los bots son “scripts” de software diseñados para actuar exclusivamente en redes de sitios web creadas a tal efecto. Estas redes se conocen como “botnet”. Hay seis tipos de “bots”:

- Básico.
- Mejorado.
- Altamente mejorado.
- Avanzado.

- Altamente avanzado.
- Humanoide.

La diferencia entre ellos, se basa en la capacidad de imitar de manera convincente, patrones de comportamiento humano.

Otra técnica de fraude en Internet, es el llamado “malvertising”. Este redirige a usuarios reales a páginas web que no pretendían visitar con el objetivo de aumentar de manera artificial el tráfico de usuarios.
(Fourquet, 2015, https://marcelofourquet.wordpress.com)

Se puede identificar que varias fuentes indican que hay congruencia en el tema del engaño a través de las redes. Indican cuales son los métodos a utilizar para llevar a cabo estas acciones que hoy en día están afectando a muchas empresas y usuarios.

5.2 Marco Conceptual

A. Red de Telecomunicaciones: Está formada por los sistemas de transmisión y, cuando proceda, los equipos de conmutación y demás recursos que permitan la transmisión de señales entre puntos de terminación definidos mediante, cable, medios ópticos o de otra índole.

(Moya, 2006)

B. Publicidad engañosa: Es engañosa la publicidad que de cualquier manera, incluida su presentación, induce o puede inducir a error a sus destinatarios, pudiendo afectar a su comportamiento económico, o perjudicar o ser capaz de perjudicar a un competidor.

(Uceda, 2011, pág. 463)

C. Trafico Web: En internet, el tráfico hace referencia a la cantidad de visitantes, visitantes únicos, hits, megabytes transferidos o cualquier otra forma de medida, que se produce en un servidor web o en un sitio web específicos en un determinado período de tiempo.

(Alegsa, 2010)

D. Página Web: Las páginas web son los documentos básicos del World Wide Web y se visualizan con navegadores de Internet.

(Erostarbe, 2005, pág. 35)

E. Fraude: Se usaba en la Edad Media para designar las variaciones en la cantidad de metal noble que portaban las monedas; pero es la literatura picaresca del Siglo de Oro la que consagra el termino para referirse a un delito en el que con engaño se da una cosa en lugar de otra.

(Higuera, 2001, pág. 1)

F. Cliente: Los clientes y, principalmente, los consumidores son los pilares de la empresa, los que generan su fuente de ingresos, los que hacen que

pueda desarrollar y crecer o, por el contrario, caer en quiebra y desaparecer del mercado.

(Serrano, 2012, pág. 9)

G. Software malicioso: término que surge de las palabras en inglés “malicious software”, se le considera todo tipo de software cuyo objetivo es provocar daños en un sistema informático.

(Hurtado, 2011, pág. 70)

H. Recolección de datos: Se fundamenta en la medición (se miden variables o conceptos contenidos en las hipótesis). Esta recolección o medición se lleva a cabo al utilizar procedimientos estandarizados y aceptados por una comunidad científica.

(Sampieri, 2006, pág. 5)

CAPÍTULO II

6.1 Tipo de investigación

El tipo de investigación a utilizar es la explicativa porque ayudará a explicar las causas de estas malas prácticas, el por qué y los intereses que tienen las empresas y personas que se están dedicando a realizar estafas vía internet.

6.2 Método de Investigación

El método a utilizar es el analítico ya que a través de este se van a buscar todas las causas del fenómeno, descomponiendo todas sus partes para analizar cada una de ellas y así llegar a una conclusión.

6.3 Técnica de investigación

La técnica de recolección de datos es el cuestionario mediante una encuesta para obtener informaciones precisas sobre lo que piensan los usuarios afectados a través del fraude electrónico. Otra técnica a utilizar será la entrevista para obtener información a través de una personalidad que tenga conocimientos del tema. También, otra técnica será la revisión y análisis de documentos para obtener información sobre las leyes que regulan el manejo de la publicidad engañosa y los fraudes en telecomunicaciones.

BIBLIOGRAFÍA

Erostarbe, I. I. (2005). *Como crear una web docente de calidad.* Madrid: Gesbiblo, S.L.

Higuera, M. A.-Z. (2001). Fraude y corrupción en la arquitectura del Siglo de Oro. Santander: Graficas Calima, S.A.

Hurtado, A. G.-C. (2011). *Seguridad Informatica.* Madrid: Ediciones Paraninfo, SA.

Moya, J. M. (2006). *Redes y servicios de telecomunicaciones.* Madrid: Thomson.

Sampieri, R. H. (2006). Metodologia de la Investigacion. Iztapalapa, Mexico : McGraw-Hill Interamericana.

Serrano, M. J. (2012). Comunicacion y atencion al cliente. Madrid: Ediciones Paraninfo, S.A.

Uceda, M. G. (2011). *Las claves de la publicidad.* Madrid: Esic Editorial.

PÁGINAS WEB

Alegsa, L. (12 de Mayo de 2010). *Alegsa.com*. Obtenido de http://www.alegsa.com.ar/Dic/trafico%20web.php

Fourquet, M. (29 de Diciembre de 2015). *Marketing Digital*. Obtenido de https://marcelofourquet.wordpress.com/2015/12/29/fraude-publicitario-ad-blockers-como-reducir-su-impacto/

Ponzio, G. (22 de Septiembre de 2014). *GROU Crecimiento Digital*. Obtenido de https://blog.grou.com.mx/fraude-en-internet-genera-cambios-al-marketing-digital#sthash.JZcjfRvj.dpbs

Publicidad. (10 de Agosto de 2015). *Marketing Directo*. Obtenido de http://www.marketingdirecto.com/actualidad/publicidad/el-drama-del-fraude-en-la-publicidad-online-son-los-clientes-los-unicos-perjudicados/

Tejeda, L. (20 de Noviembre de 2015). *Listin Diario*. Obtenido de http://www.listindiario.com/economia/2015/11/20/396914/crecen-quejas-de-fraude-y-cargos

Encuesta a usuarios que navegan en Internet y utilizan las redes sociales

Saludos, soy estudiante de la Universidad Apec de la carrera de Mercadotecnia. Estoy interesado en saber su opinión acerca del fraude electrónico y publicidad engañosa a través de las páginas web y redes sociales en el sector de las telecomunicaciones.

1. Sexo
    a) Masculino
    b) Femenino

2. Edad
    a) 18 – 25
    b) 26 – 32
    c) 33 – 40
    d) 41 – En adelante

3. Nivel Académico
    a) Bachiller
    b) Nivel medio
    c) Grado
    d) Post Grado
    e) Maestría

4. ¿Usted utiliza frecuentemente el Internet y las redes sociales?
    a) Si
    b) No

¿Por qué?_____

Nota: **Si la respuesta es "No", termina la encuesta.**

5. ¿Con que frecuencia visita el Internet y las redes sociales?
    a) Eventualmente
    b) Más de dos (2) veces a la semana
    c) Más de tres (3) veces a la semana
    d) Todos los días

6. ¿Cuáles páginas web acostumbra a utilizar?

7. ¿Cuál red social utiliza con mayor frecuencia?
    a) Facebook
    b) Twitter
    c) Instagram
    d) LinkedIn

e) Otra
Especifique_____

8. ¿Qué acostumbra a realizar en las páginas web y redes sociales que visita?
   a) Chatear
   b) Ver videos
   c) Buscar información
   d) Compartir fotos
   e) Jugar video juegos en línea
   f) Utilizar aplicaciones
   Continúe detrás
   g) Realizar compras
   h) Otras
   Especifique_____

9. ¿Alguna vez ha realizado compras por Internet?
   a) Si
   b) No

Justifique su respuesta_____

Nota: **Si la respuesta es "No", justifique y pasa a la pregunta 11.**

10. Generalmente, ¿en cuáles páginas acostumbra a realizar compras?

11. ¿Usted ha sido víctima de publicidad engañosa o fraude electrónico a través de las páginas web?

    a) Si

Especifique _____

    b) No

Nota: **Si la respuesta es "No", pase a la pregunta 13.**

12. ¿Qué tipo de fraude?
    a) Robo de información
    b) Cargos no reconocidos en Tarjeta de Crédito
    c) Robo de contraseñas de correo electrónico
    d) Falsas ofertas en artículos
    e) Usurpación de identidad
    f) Otros
    Especifique_____

13. ¿En qué página web (Internet) ha visto publicidad engañosa?

14. ¿En cuales redes sociales ha sido víctima de publicidad engañosa y fraude electrónico?

    a) Facebook
    b) Twitter
    c) LinkedIn
    d) Instagram
    e) Ninguna
    f) Otras
       Especifique_____

15. ¿A través de que dispositivo fue víctima de fraude y publicidad engañosa?
    a) Tablet
    b) Computadora
    c) Celular
    d) Ninguno
    e) Otro
       Especifique_____

16. ¿Qué daños ha sufrido usted como usuario?

17. ¿Conoce usted las medidas de precaución para evitar ser víctima de fraude electrónico y publicidad engañosa?

    a) Si
    b) No (Justifique)

Nota: **Si la respuesta es "No", pase a la pregunta 19.**

18. ¿Cuáles medidas de precaución usted conoce?

19. ¿Ha denunciado estas malas prácticas ante una autoridad competente?
    a) Si
    b) No (Justifique)

Nota: **Si su respuesta es "No", justifique y finaliza la encuesta.**

20. ¿Ante que institución realizó su denuncia?
    a) Indotel
    b) Pro consumidor
    c) Dicat
    d) Policía Nacional
    e) Institución Bancaria
    f) Otros
       Especifique_____

21. ¿Considera usted que la institución a la cual usted reportó la situación resolvió con eficiencia el problema?

a) Si
b) No (Justifique)

Muchas gracias por su tiempo

Entrevista a personalidad de Pro Consumidor

Fecha:

Nombre:

Puesto de trabajo:

Lugar de trabajo:

1. **¿Cómo afecta a los usuarios las distintas formas de estafa y publicidad engañosa en las redes sociales y páginas web?**

2. **¿Qué estrategias marketing y publicidad engañosa utilizan los defraudadores en Internet?**

3. **¿Qué consecuencias y pérdidas trae el fraude electrónico ante el comercio por Internet?**

4. **¿Qué recomendaciones usted puede realizar para que los usuarios eviten ser víctimas de la publicidad engañosa y fraude electrónico?**

Muchas gracias por su tiempo

Entrevista a personalidad del Ministerio de Industria y Comercio

Fecha:

Nombre:

Puesto de trabajo:

Lugar de trabajo:

1. **¿Cómo afecta a los consumidores el fraude electrónico a través de la compra por Internet?**

2. **¿Cuáles consecuencias sufren las empresas que se dedican al comercio electrónico por el auge de las estafas en Internet?**

3. **¿Qué actividades coordina el Ministerio de Industria y Comercio para concientizar a los comerciantes y consumidores finales sobre sus derechos y precauciones al momento de la compra?**

4. **¿Qué recomienda usted a los usuarios para evitar caer ante el fraude electrónico?**

Muchas gracias por su tiempo