

**Nombre del Asesor**

**“ING. AMILCAR SERRANO ÁVILA”**

**ABRIL 2020**

**Que Presenta el Alumno:**

**“EDER ALBERTO MOSSO PANCHÍ”**

**“PROPUESTA BÁSICA DE UN MANUAL PARA EVITAR EL ROBO DE IDENTIDADES EN SITIOS DE COMPRAS EN LÍNEA”**

**“PROPUESTA BÁSICA DE UN MANUAL PARA EVITAR EL ROBO DE IDENTIDADES EN SITIOS DE COMPRAS EN LÍNEA”**

**ÍNDICE**

**INTRODUCCIÓN**

Desde la apertura de la web todo ha sido de gran ayuda en la vida cotidiana, los trabajos escolares, trabajos de oficina, ocio, etc. Pero no todo en la vida es de color de rosa, siempre va a existir ese tipo de paginas piratas que se aprovecharan para sacar todo tipo de información necesaria para el beneficio de lo terceras personas. Cuando alguien accede a la red, siempre esta propensa a todo tipo de vulnerabilidad, ya sea por virus o robo de identidades, es por eso que la seguridad informática se tiene que tomar en serio, saber realmente que es lo que se debe y lo que no es lo que hay que ingresar, ya que cualquier descuido puede ser fatal.

Este es el fin de este manual, conocer las medidas de seguridad que se deben de tomar antes de navegar por la web, analizar que tipo de datos debemos registrar en algún sitio de interés y así poder protegerse de los piratas informáticos, la finalidad es conocer y saber diferenciar entre una pagina de internet verdadera y cual es la falsa, basta con saber diferenciar los enlaces ingresados.

Este manual informara detalladamente como navegar seguros sin miedo a ser estafados y así poder comprar en línea con mas confianza al agregar todo tipo de tarjetas bancarias.

**PLANTEAMIENTO DEL PROBLEMA**

Hoy en día, la sociedad está abierta a todo tipo de tecnología, desde electrodomésticos hasta dispositivos electrónicos, tales como los dispositivos móviles o computadoras. Las computadoras, desde su popularización y distribución en los hogares han sido indispensables para la realización de trabajos, tareas o para uso cotidiano en la internet.

Desde la apertura de la web o comúnmente conocida World wide web (www.) cual fue fundada en el CERN (Centro Europeo de Investigación Nuclear) en Suiza en el año de 1989 (Tanenbaum, 2012).

Actualmente existe una gran variedad de sitios en internet, que los usuarios visitan regularmente. En la web se puede encontrar todo tipo de páginas de internet; Buscadores (Google, Yahoo!, Bing), Redes Sociales (Facebook, Twitter, Instagram), Noticieros (Cnn, New york times), sitios de entretenimiento (YouTube) y una enorme gama de páginas que se desconocen de su existencia. Todos los días en la web, se registran datos personales, tales como son; nombres, apellidos, domicilios, fechas de nacimiento, números telefónicos y, sobre todo, una de las más comunes, las tarjetas bancarias. La vulnerabilidad está a la orden del día, y los más afectados son los niños, los adultos mayores, que no tienen noción alguna sobre tecnología y los jóvenes adultos que desconocen la informática y son vulnerables a las trampas de la internet. En la web existen sitios de compras en línea (Mercado Libre, Amazon, EBay, Best Buy), sitios de tiendas comerciales (Wal-Mart, Liverpool, Sears), hasta los sitios de apuestas en línea (Beat365, CalienteSports, Bwin), estas páginas están a la espera de obtener los datos personales de cada cliente y así crear su base de datos. Es ahí donde operan los piratas informáticos, esas personas que están dispuestas a robar todo tipo de información posible para su beneficio, personas que no se tocan el corazón para vaciar las cuentas bancarias sin darse cuenta de ello, a esos piratas comúnmente los llaman “HACKERS”

Estos supuestos hackers, los hay en variedad, los White hat (sombrero blanco), los que buscan vulnerabilidades en las empresas y son conocidas como excelentes personas de ética, los Grey hat (sombrero gris), que no están ni del lado del bien ni del mal, hackers que no utilizan la información para su uso y los Black hat (sombrero negro), los que descargan información valiosa para su beneficio y extorsionar a sus víctimas.

Es ahí donde entran los Carder, piratas que solo buscan las cuentas bancarias de la sociedad, aquellos que descifran la información por sus medios con la inteligencia de la ingeniería social o por métodos informáticos.

En la actualidad, la sociedad no distingue entre las URL reales y las falsas, aquellas que son sitios clonados de la original solo para extraer la información necesaria, desconocen aquellas páginas que tienen protocolos de seguridad y sin observar ese detalle, ingresan sus datos bancarios solo para adquirir ese producto que desean, sin saber si es seguro o no.

En mayoría de veces, las personas vulnerables caen fácilmente en las trampas de los piratas informáticos, al recibir las URL falsas, argumentándoles que ganaron algún premio, pidiéndoles que ingresen sus datos para solicitar algún crédito en línea en bancos fantasmas, enlaces de los bancos que en realidad no son los correctos, pero no se distingue la veracidad de la web o mostrando en sus redes sociales aquel producto tan llamativo que les gustaría obtener y que en realidad no existe como tal.

La internet no es como se muestra en realidad, es una red maravillosa, llena de información de interés y entretenimiento para toda la familia, pero también es un lugar muy inseguro, un sitio donde tener el más mínimo descuido puede afectar a la economía y sobre todo al bienestar social.

Antes de navegar por la red, es necesario saber a qué sitio ingresará, observar el entorno de la página a cuál se ingresó, investigar si cumple con los protocolos de seguridad que tiene que llevar toda la web de compras antes de ingresar los datos, ya que si no se toman las medidas necesarias esto puede afectar gravemente al usuario.

**¿Cuál es la razón por la cual las personas son estafadas en las compras en línea?**

**JUSTIFICACIÓN**

Esta propuesta de navegación segura es muy importante, ya que en ella se podrá encontrar las maneras mas factibles de contar con los métodos suficientes para acceder a la internet, sin miedo al que o como pasaran las cosas, esta contemplada para toda persona que desconoce como se maneja y funciona la red como tal. El uso del manual traerá beneficios para la sociedad, al no caer en engaños que trae consigo las páginas de internet, podrán identificar como se ve realmente una URL y así poder identificar si es real o no, antes de ingresar los datos solicitados.

El manual estará realizado únicamente para reforzar los conocimientos básicos de la navegación segura, la información proporcionada será de utilidad ya que las vulnerabilidades están a la vuelta de la esquina y es necesario evitar toda causa maliciosa.

Para este manual es necesario comparar las investigaciones cualitativas, buscar datos y comparar con otras estadísticas recabadas en la investigación.

**OBJETIVO GENERAL**

Proponer un manual básico para evitar el robo de identidades en compras en línea, mediante la información proporcionada y recabada, para evitar ser estafado.

**OBJETIVOS ESPECÍFICOS**

Crear un manual para que los usuarios que desconocen la informática, puedan navegar mas seguros por la internet y así no tengan que sufrir estafas o robo de información por el mal uso de las herramientas de la web o visitando paginas falsas.

**HIPÓTESIS**

El motivo de las estafas hacia las personas mediante sus compras en línea, es la falta de información y la total inexperiencia sobre el tema de la informática, en el cual se dejan manipular fácilmente por los anuncios encontrados en la internet e ingresan su información sin antes haber investigado la veracidad de la publicación.

**METODOLOGÍA**

La investigación científica que se llevara a cabo es parte del estudio de la problemática que conlleva la desinformación que existe en la sociedad al momento de navegar en la web.

Para esta investigación se tomaron los siguientes métodos científicos:

MÉTODO CUANTITATIVO: Este método se utilizó para la obtención de los datos sobre las personas afectadas con el robo de identidades.

MÉTODO INDUCTIVO: Este método fue utilizado para brindar una hipotesis de la investigación, mediante la observación de los datos obtenidos en línea.

MÉTODO ANALÍTICO: Este método fue utilizado para analizar a detalle las estafas a los derechohabientes y así poder deducir la problemática.