CHIHUAHUA
Juntas Sí podemos

FISCALÍA
GENERAL DEL ESTADO

FGE
IESP

ESTADO LIBRE Y SOBERANO DE CHIHUAHUA

Secretaría de Educación y Deporte

FISCALIA GENERAL DEL ESTADO

INSTITUTO ESTATAL DE SEGURIDAD PUBLICA

T E S I N A

"FRAUDE INFORMÁTICO EN LA MODALIDAD DE NAVEGACIÓN 2021-2022"

Para obtener el Grado de:

MAESTRA EN DERECHOS HUMANOS Y PERSPECTIVA DE GÉNERO

Catedrática: MAESTRA ETHEL GARZA ARMENDÁRIZ

Postulante: LIC. KARLA YIBRANI ENRÍQUEZ MEDRANO

Chihuahua, Chih., A Diciembre del 2022

FISCALÍA
GENERAL DEL ESTADO

ESTADO LIBRE Y SOBERANO DE CHIHUAHUA

Secretaría de Educación y Deporte

FISCALIA GENERAL DEL ESTADO

INSTITUTO ESTATAL DE SEGURIDAD PUBLICA

T E S I N A

"FRAUDE INFORMÁTICO EN LA MODALIDAD DE NAVEGACIÓN 2021-2022"

Para obtener el Grado de:

MAESTRA EN DERECHOS HUMANOS Y PERSPECTIVA DE GÉNERO

Catedrática: MAESTRA ETHEL GARZA ARMENDÁRIZ

Postulante: LIC. KARLA YIBRANI ENRÍQUEZ MEDRANO

INSTITUTO ESTATAL
DE SEGURIDAD PÚBLICA

Chihuahua, Chih., A Diciembre del 2022.

INTRODUCCIÓN

El fraude Informático afecta a algunos de los usuarios de la banca en línea, a las pequeñas, medianas y grandes empresas de marcas reconocidas, ya que cada vez son más frecuentes y los costos de las violaciones de datos, ascienden a millones de pesos. La ciberdelincuencia está en todas partes, las personas y empresas están constantemente siendo investigadas y atacadas por los delincuentes en busca de datos confidenciales y debilidades de sus sistemas. Estos delincuentes también aprovechan la falta de capacitación en esta materia de los operadores jurídicos, la marcada carencia de herramientas de investigación y la falta de coordinación que existen dentro de los sistemas de impartición de justicia mexicanos y específicamente los de la ciudad de Chihuahua, Chihuahua, quienes no han tenido la capacidad de definir si le corresponde la investigación de los hechos delictivos a los ministerios públicos del fuero común o a los ministerios públicos del fuero federal, lo cual deriva en la vulneración de los derechos de las víctimas.

INDICE

CAPÍTULO PRIMERO

EL CIBERESPACIO E INTERNET

El concepto de ciberespacio suele asociarse a Internet. Todo aquello que se desarrolla en Internet, a través de sitios web, correos electrónicos, redes sociales, etc., no tiene lugar en un país específico, más allá de la ubicación de los servidores y de los usuarios. El ciberespacio, es más amplio que Internet, por lo tanto «ciberespacio» e «Internet» no son sinónimos.

El ciberespacio es el entorno artificial que necesita de las herramientas informáticas para desarrollarse.

Si internet es un conjunto descentralizado de redes de comunicación a través de protocolos; el ciberespacio es el lugar en el que se producen las comunicaciones de internet. Por ejemplo, cuando hablamos de hackeo, este ataque no se produce en un espacio físico determinado, se produce en el ciberespacio. Es decir, existe una mezcla entre lo real y lo virtual. Tomamos decisiones en un lugar indeterminado de internet y las consecuencias de nuestras acciones tienen influencia directa en la vida real. Esto se debe a que el ciberespacio se construye mediante intercambios de información. Es un espacio en el que se produce la comunicación y también es el medio que posibilita

el intercambio de comunicación. De ahí que haya quienes confundan ambos conceptos y consideren que internet y el ciberespacio son lo mismo.

El término ciberespacio ha llevado a la introducción de otras palabras, como ciberseguridad, ciberdelincuencia, ciberguerra, ciberterrorismo, etc. El ciberespacio en sí proviene de la "cibernética", que a su vez se deriva del griego antiguo "kybernētēs", que significa "steerman", gobernador, piloto, o timón.

El término ciberespacio surgió en relación con la gestión de espacios físicos. Sin embargo, con el inicio de Internet, el término se ha aplicado al espacio virtual que se crea dentro de Internet. El ciberespacio no es más que un espacio simbólico y figurativo que existe dentro del ámbito de Internet. Se puede decir que cualquier cosa que se haga a través del uso de Internet, ocurre dentro de los confines del ciberespacio, ya sea enviando un correo electrónico, un sitio web o jugando un juego, todas estas cosas existen dentro del ciberespacio.

1.1 El ciberespacio

El término inglés "cyberspace" llegó al castellano como ciberespacio. Así se denomina al entorno artificial que se desarrolla mediante herramientas informáticas.

El escritor norteamericano William Gibson es señalado como quien acuñó la noción de ciberespacio. La utilizó por primera vez en un relato de 1981 y luego ayudó a popularizarla a través de "Necromante", una novela que publicó en 1984.

El término "ciberespacio" deriva de "cibernética", el cual fue acuñado por Norbert Wiener en la década de 1940 para hacer referencia al estudio de las analogías entre los sistemas de comunicación y de control de las máquinas y los seres vivos.

En la actualidad, el concepto de ciberespacio suele asociarse a Internet. Todo aquello que se desarrolla en Internet, a través de sitios web, correos electrónicos, redes sociales, etc., no tiene lugar en un país específico, más allá de la ubicación concreta de los servidores y de los usuarios. El ciberespacio, de todos modos, es más amplio que Internet.

Si bien algunas personas utilizan los términos ciberespacio e Internet como sinónimos, es más correcto entenderlos de forma jerárquica: podemos pensar que Internet se encuentra en el ciberespacio, que el gran conjunto de páginas y aplicaciones a las que accedemos desde nuestros dispositivos se alojan en este dominio infinito e intangible, donde también tendrán lugar experiencias futuras que no forman parte del concepto de Internet.

Cuando por ejemplo una mujer que vive en Canadá conoce en la aplicación de citas denominada "Tinder", a un hombre que reside en Nueva Zelanda. Ambos intercambian mensajes, participan en videoconferencias, se envían fotografías y establecen una relación de amistad a distancia. Ese vínculo se desarrolla en el ciberespacio, formando un vínculo virtual comparable con el de una amistad tradicional.

1.2 Herramientas informáticas

Es el conjunto de instrumentos empleados para manejar información por medio de la computadora como el procesador de texto, la base de datos, graficadores, correo electrónico, hojas de cálculo, buscadores, programas de diseño, presentadores, redes de telecomunicaciones, son programas, aplicaciones o, simplemente instrucciones, que al utilizarlas permitirán al usuario realizar un trabajo determinado de la mejor manera posible en algún dispositivo informático.

1.3 Funciones de las herramientas informáticas

Facilitar el trabajo de las personas a la hora de realizar alguna labor.

Permiten llevar el control de las cosas (inventarios, catálogos, inventarios, listas, colecciones, series, etc.)

Se utilizan para la creación de nuevos proyectos bien sea a nivel de contenido o cualquier otra cosa en la que se pueda innovar.

Existen herramientas informáticas más avanzadas que tienen como función sustituir el trabajo de algunas personas.

Función de entretenimiento, debido a que existe una gran cantidad de juegos de computadora y las personas pueden instalarlos en sus máquinas para pasar un tiempo agradable y entretenerse.

1.4 Las herramientas informáticas más utilizadas

Cada herramienta se crea y diseña para realizar una o varias aplicaciones informáticas, y por tanto hablar de los tipos es algo muy extenso.

Tenemos herramientas básicas, de sistema, de limpieza, ortográficas, de gestión, de mantenimiento, de programación, de desarrollo, y un sinfín más. Las más utilizadas y conocidas son:

De procesadores de texto como Lotus Word Pro y Microsoft Word.

De hoja electrónica de cálculo, como Lotus 1-2-3 y Microsoft Excel.

De manejo de base de datos, como Microsoft Access y Visual FoxPro.

De comunicación de datos, como Safari, Mozilla Firefox y Chrome.

De reproductor o editor de video y música, como Windows Media Player y QuickTime.

De presentaciones, como Microsoft Power Point y Windows Movie Maker.

De diseño como Adobe Photoshop, Microsoft Photo Editor, Microsoft Paint y AutoCAD.

De edición como Adobe PageMaker, Adobe InDesign y Adobe Acrobat.

De correo electrónico, como Outlook Express.

De comprensión de archivos como WinZip, gzip y Winrar.

1.5 Diferencia entre herramientas de informática y TICS

Dos conceptos que se confunden con frecuencia son el de las herramientas informáticas y las TICS. Entonces, como ya sabemos qué son las herramientas informáticas expliquemos qué son los TICS (Tecnologías de la Información y la Comunicación).

TICS: comprende un conjunto de tecnologías que han sido desarrolladas para manejar información y comunicarla de un sitio a otro.

La diferencia entre herramientas de informática y TICS radica en que las herramientas de informática se limitan a solo ser software y/o aplicaciones para funciones dentro de

dispositivos que dependan de sistemas operativos para ejercer sus deberes. Y las TICS son el conjunto de esas diferentes herramientas de informática.

1.6 ¿Por qué las herramientas informáticas son tan importantes?

Es sencillo comprender lo qué son las herramientas informáticas, pero la mayoría no somos realmente conscientes de su importancia. Sin estas herramientas no se podrían hacer tareas de un día común, tales como navegar por internet, editar una imagen con Photoshop, escuchar música con Spotify y/o QuickTime, sincronizar contenido con un dispositivo móvil, jugar un juego, mandar correos personales o de trabajo, o interactuar por redes sociales Facebook, Instagram, WhatsApp, etc.

Lo cierto es que cada programa o aplicación tiene su tarea determinada siendo capaz de satisfacer necesidades específicas de los usuarios que las implementan, convirtiéndose en instrumentos de importancia e imprescindibles para la vida diaria, ya que suponen herramientas funcionales a través de las cuales las personas realizan actividades en su día a día.

En los últimos tiempos los centros educativos han necesitado implementar las herramientas tecnológicas para continuar con sus clases de manera virtual, siendo estas las principales colaboradoras tanto para los profesores como para los estudiantes.

En la actualidad los sistemas educativos de todo el mundo se enfrentan al desafío de utilizar las Tecnologías de la Información y la Comunicación para proveer a sus alumnos con las herramientas y conocimientos necesarios que se requieren en estos tiempos. En 1998, el Informe Mundial sobre la Educación de la UNESCO, "Los docentes y la enseñanza en un mundo en mutación", describió el impacto de las TICs en los métodos convencionales de enseñanza y de aprendizaje, augurando también la transformación del proceso de enseñanza-aprendizaje y la forma en que docentes y alumnos acceden al conocimiento y la información.

Los objetivos estratégicos apuntan a mejorar la calidad de la educación por medio de la diversificación de contenidos y métodos, la promoción de la experimentación, la innovación, la difusión y el uso compartido de información y de buenas prácticas, la formación de comunidades de aprendizaje y estimulación de un diálogo fluido sobre las políticas a seguir. Con la llegada de las tecnologías, el énfasis de la profesión docente está cambiando desde un enfoque centrado en el profesor que se basa en prácticas alrededor del pizarrón y el discurso, basado en clases magistrales, hacia una formación centrada principalmente en el alumno dentro de un entorno interactivo de aprendizaje.

Las TICs son la innovación educativa del momento y permiten a los docentes y alumnos cambios determinantes en el quehacer diario del aula y en el proceso de enseñanza-aprendizaje de los mismos.

Las TICs brindan herramientas que favorecen a las escuelas que no cuentan con una biblioteca ni con material didáctico. Estas tecnologías permiten entrar a un mundo nuevo lleno de información de fácil acceso para los docentes y alumnos.

La incorporación de las TICs en la educación tiene como función ser un medio de comunicación, canal de comunicación e intercambio de conocimiento y experiencias. Son instrumentos para procesar la información y para la gestión administrativa, fuente de recursos, medio lúdico y desarrollo cognitivo.

Para muchos docentes el uso de las TICs implica ciertas desventajas, tales como aprender a usar las tecnologías, actualizar los equipos y programas, sobre todo, implica ocupar un tiempo fuera del lugar de trabajo, el cual muchos docentes no pretenden acceder.

Las principales funcionalidades de las TIC en la Educación Básica Regular están relacionadas con lo siguiente:

Alfabetización digital de los estudiantes, profesores y familias.

Uso personal (profesores y alumnos): acceso a la información, comunicación, gestión y proceso de datos.

CAPÍTULO SEGUNDO

ORIGEN Y EVOLUCIÓN DEL DELITO CIBERNÉTICO

Los delitos cibernéticos y los cibercriminales han estado presentes desde que las primeras empresas comenzaron a usar el Internet para el comercio. La tasa de delitos informáticos y su costo para las empresas ha aumentado drásticamente después de la pandemia de COVID 19, así como por la transformación de los delitos cibernéticos, que va pasando de un inconveniente menor a un riesgo significativo que debe ser adecuadamente gestionado. Actualmente las noticias de violaciones de datos a gran escala, en las empresas de marca son más frecuentes que nunca. Los costos de una violación de datos ascienden a millones de dólares. La ciberdelincuencia está en todas partes y las empresas de hoy están constantemente siendo investigadas y atacadas por los delincuentes en busca de datos confidenciales y debilidades del sistema.

En 1971 en Estados Unidos se da el primer caso de fraude telefónico, o mejor conocido como el Spoofing (Suplantación de identidad), (oracle, 2022) es un acto fraudulento en el que la comunicación desde una fuente desconocida se disfraza de fuente conocida en la que el receptor confía. El fraude telefónico esta entre los tres principales delitos en México.

En 1981 fue condenada la primera persona por un delito cibernético y Gerald Wondra quien fue una de las primeras personas condenadas por un delito informático, en 1983 fue condenado a 24 meses de libertad condicional, por acceso no autorizado a los sistemas de entidades financieras de Estados Unidos y utilizarlo para hacer llamadas telefónicas.

En 1990 dos bandas cibernéticas, se involucran en una guerra en línea, promocionando así el robo de tarjetas de crédito y el fraude del cable.

En 2002 Se lanza el sitio web Shadow Crea, el sitio web era un tablero de mensajes y un foro para hackers de sombrero negro (son delincuentes que se introducen en redes informáticas para llevar a cabo algún acto maligno) Los miembros podían publicar, compartir y aprender a cometer una gran cantidad de delitos cibernéticos y evitar la captura. El sitio duró 2 años antes de ser cerrado por el Servicio Secreto. 28 personas fueron detenidas en Estados Unidos y otros 6 países.

En 2007 Los casos de hackeo, robo de datos e infecciones de malware se disparan.

La siguiente ola en la línea de tiempo de la historia del delito cibernético llegó en los años 90 con el avance de los navegadores web. En ese momento había una multitud para elegir, muchos más que hoy, y la mayoría eran vulnerables a los virus. Los virus eran enviados a través de conexiones a internet siempre que se visitaban sitios web cuestionables. Algunos causaban que la computadora funcionara lentamente, otros causaban que la aparición de publicidad molesta invadiera la pantalla o la redirigiera a sitios pornográficos.

El delito cibernético despego a principios del 2000 cuando las redes sociales cobraron vida. La oleada de gente que, poniendo toda la información que podía en una base de datos del perfil, creó una inundación de información personal y el aumento del robo de identidad. Los ladrones utilizaban la información de varias maneras, incluyendo el acceso a cuentas bancarias, la creación de tarjetas de crédito u otros fraudes financieros.

La última ola es el establecimiento de una industria criminal global que suma millones de dólares anuales. Estos criminales operan en pandillas, utilizan métodos bien establecidos y apuntan a cualquier cosa y a todos los que tienen presencia en la web, incluso a quienes solo son usuarios de la banca en línea o por cajeros automáticos.

A pesar de que en 1971 en Estados Unidos se da el primer caso de fraude telefónico y de que en ese mismo año se crean el primer virus y antivirus informático del mundo, es hasta 1981, en ese mismo país, que se obtiene la primera condena por un delito cibernético y es Ian Murphy, también conocido como "Capitán Zap", quien hackeo la red de AT&T y cambió los relojes internos para cobrar tarifas fuera de horario en las horas pico.

Es en 1986 que el Congreso de los Estados Unidos aprueba la Ley de Fraude y Abuso Informático (CFAA), la cual establece que infiltrarse en los sistemas informáticos se considera un delito y es así que nace la primera ley contra delitos cibernéticos.

En México los delitos informáticos tienen un gran retraso en cuanto a su tipificación, además de que para el último trimestre del 2021 se consideró qué existe un 75 % más de probabilidades de ser víctimas de un delito cibernético en comparación con el 2020. Además, con el 22 % de todos los ataques, México ocupa el segundo lugar de todos los delitos informáticos cometidos en la América latina, solo después de Brasil.

CAPÍTULO TERCERO

MALWARE

Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas, también es conocido como software malicioso.

Estos programas se pueden comparar con la gripe en el ser humano, ya que interfiere en el funcionamiento normal del sistema. El malware hostil e intrusivo, intenta invadir, dañar o deshabilitar ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo.

La intención del malware es sacarle dinero al usuario ilícitamente. Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red (existen raras excepciones) sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin su conocimiento o permiso.

3.1 Historia del malware

Dada la variedad de tipos de malware y el enorme número de variantes que pululan libremente a diario, una historia completa del malware comprendería una lista

demasiado larga para incluirla aquí, pero estas son las tendencias principales del desarrollo de malware.

Década de 1980: El fundamento teórico de los "autómatas que se reproducen por sí solos" (los virus) se remonta a un artículo publicado en 1949, y los primeros virus infectaron plataformas anteriores a los ordenadores personales en la década de 1970. No obstante, la historia de los virus modernos comienza con un programa llamado "Elk Cloner", que empezó a infectar sistemas Apple II en 1982. El virus, que se diseminaba mediante disquetes, era inocuo por sí solo, pero se extendía a todos los discos conectados a un sistema y explotaba con tal virulencia que puede considerarse el primer brote de virus informáticos a gran escala de la historia. Se debe tener en cuenta que esto fue anterior a cualquier malware para PC Windows. Desde entonces, los virus y gusanos se han generalizado.

Década de 1990: La plataforma Microsoft Windows apareció en esta década, junto con las macros flexibles de sus aplicaciones, que propiciaron que los autores de malware escribieran código infeccioso en el lenguaje de macros de Microsoft Word y de otros programas. Estos virus de macro infectaban documentos y plantillas, no aplicaciones ejecutables, aunque hablando estrictamente, las macros de los documentos de Word son un tipo de código ejecutable.

De 2002 a 2007: Los gusanos de la mensajería instantánea (código malicioso que se replica por sí solo a través de una red de mensajería instantánea) se aprovechan de las lagunas de la red a escala masiva e infectan las redes AOL Instant Messaging, MSN Messenger y Yahoo Messenger, así como los sistemas empresariales de mensajería instantánea.

De 2005 a 2009: Proliferaron los ataques de adware, que presentaban publicidad no deseada en las pantallas de los ordenadores, a veces en forma de mensaje emergente o en una ventana que los usuarios no podían cerrar. Estos anuncios aprovechaban con frecuencia software legítimo como medio para difundirse, pero en 2008, los editores de software comenzaron a denunciar a las empresas de adware por fraude. El resultado fue el pago de millones de dólares en multas. Finalmente, esto causó el cierre de las empresas de adware.

De 2007 a 2009: Las estafas de malware utilizaron canales de redes sociales como MySpace para distribuir publicidad deshonesta, redirecciones y ofertas de herramientas antivirus y de seguridad falsas. Sus estratagemas estaban diseñadas para embaucar a los usuarios mediante trucos de ingeniería social. Facebook y Twitter se convirtieron en sus plataformas preferidas cuando decayó la popularidad de MySpace. Algunas de las tácticas comunes consistían en presentar enlaces falsos a

páginas de phishing y promover aplicaciones de Facebook con extensiones maliciosas. A medida que esta tendencia fue a menos, los estafadores exploraron otros medios para robar.

2013: Un nuevo tipo de malware denominado ransomware lanzó un ataque con el nombre CryptoLocker, que tuvo lugar desde principios de septiembre de 2013 hasta finales de mayo de 2014 y tenía como objetivo ordenadores con Windows. CryptoLocker consiguió forzar a sus víctimas a pagar alrededor de 27 millones de USD en el último trimestre de 2013. Además, el éxito de este ransomware generó otro ransomware de nombres similares. Con una variante copiada, se embolsaron más de 18 millones de USD de aproximadamente 1000 víctimas entre abril de 2014 y junio de 2015.

De 2013 a 2017: El ransomware, que se distribuía a través de troyanos, exploits y publicidad maliciosa, se convirtió en el rey del malware. El colofón fueron los grandes brotes de 2017 que afectaron a empresas de todo tipo. La actividad del ransomware consiste en cifrar los datos de la víctima y a continuación reclamar pagos para liberar esos datos.

De 2017 hasta ahora: La criptomoneda —y cómo extraerla— ha captado la atención general y ha conllevado la creación de una nueva estafa de malware llamada "cryptojacking", que es el acto de utilizar el dispositivo de otra persona en secreto para extraer criptomonedas, con los recursos de la víctima.

Popularmente se dice que los Macs y los iPad son inmunes a los virus (y no necesitan un antivirus). En gran medida, eso es cierto. Y al menos, no ha ocurrido desde hace mucho tiempo.

3.2 Comportamientos del equipo Infectado con malware

El malware puede manifestarse a través de varios comportamientos, como los siguientes:

- El ordenador se ralentiza (el diccionario de la lengua española (DLE) define ralentizar como 'imprimir lentitud a alguna operación o proceso, disminuir su velocidad), uno de los efectos principales del malware es reducir la velocidad del sistema operativo, tanto si navega por Internet como si sólo utiliza sus aplicaciones localmente.

- La pantalla se llena de oleadas de publicidad fastidiosa. Los anuncios emergentes inesperados son un signo típico de malware, los mensajes emergentes suelen ir unidos a otras amenazas de malware ocultas.
- El sistema se bloquea constantemente o muestra una pantalla azul BSOD (Blue Screen of Death o pantallazo azul), que puede aparecer en los sistemas Windows cuando se encuentra un error grave.
- Observa una pérdida misteriosa de espacio disponible en disco, probablemente debido a un ocupante indeseado de malware que se oculta en su disco duro.
- Se produce un aumento extraño de la actividad del sistema en Internet.
- La utilización de recursos del sistema es anómalamente elevada y el ventilador del equipo comienza a funcionar a toda velocidad, lo cual señala que la actividad del malware se ha apropiado de recursos del sistema en segundo plano.
- La página de inicio del navegador cambia sin su permiso. Igualmente, los enlaces en los que hace clic lo llevan a un destino web no deseado.
- El navegador se llena inesperadamente de nuevas barras de herramientas, extensiones o complementos.
- El antivirus deja de funcionar y no puede actualizarlo, dejándolo desprotegido contra el malware tramposo que lo deshabilitó.

- El ransomware, se anuncia sin disimulo, le dice que tiene sus datos y exige un rescate para devolverle sus archivos.

3.3 Infección con malware

Una infección de malware requiere una larga lista de ingredientes. Los principales son las dos maneras más comunes en las que el malware obtiene acceso al sistema: Internet y el correo electrónico, es decir, básicamente todo el tiempo que está conectado a Internet.

El malware puede penetrar en el equipo al navegar por sitios web pirateados, hacer clic en demostraciones de juegos, descargar archivos de música infectados, instalar nuevas barras de herramientas de un proveedor desconocido, instalar software de una fuente dudosa, abrir un adjunto de correo electrónico malicioso o descargar prácticamente cualquier cosa de la web en un dispositivo que carece de una aplicación de seguridad antimalware de calidad.

Las aplicaciones maliciosas pueden ocultarse en aplicaciones aparentemente legítimas, especialmente cuando se descargan a través de sitios web o mensajes y no desde una App Store segura.

El adware es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador.

El spyware es malware que observa las actividades del usuario en el ordenador en secreto y sin permiso, y se las comunica al autor del software.

Un virus es malware que se adjunta a otro programa y, cuando se ejecuta —normalmente sin que lo advierta el usuario—, se replica modificando otros programas del ordenador e infectándolos con sus propios bits de código.

Los gusanos son un tipo de malware similar a los virus, que se replican por sí solos con el fin de diseminarse por otros ordenadores en una red, normalmente provocando daños y destruyendo datos y archivos.

Un troyano, o caballo de Troya, es uno de los tipos de malware más peligrosos. Normalmente se presenta como algo útil para engañar al usuario. Una vez que está en el sistema, los atacantes que se ocultan tras el troyano obtienen acceso no autorizado al ordenador infectado. Desde allí, los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus y ransomware.

El ransomware es un tipo de malware que bloquea el acceso del usuario al dispositivo o cifra sus archivos y después lo fuerza a pagar un rescate para devolvérselos. El ransomware se ha reconocido como el arma preferida de los delincuentes informáticos porque exige un pago rápido y provechoso en criptomoneda de difícil seguimiento. El código que subyace en el ransomware es fácil de obtener a través de mercados ilegales en línea y defenderse contra él es muy difícil.

El rootkit es un tipo de malware que proporciona al atacante privilegios de administrador en el sistema infectado. Normalmente, también se diseña de modo que permanezca oculto del usuario, de otro software del sistema y del propio sistema operativo.

Un registrador de pulsaciones de teclas es malware que graba todas las pulsaciones de teclas del usuario, almacena la información recopilada y se la envía al atacante, que busca información confidencial, como nombres de usuario, contraseñas o detalles de la tarjeta de crédito.

La minería de criptomonedas maliciosa, denominada también minería fortuita o cryptojacking, es un malware cada vez más prevalente instalado por un troyano. Permite que otras personas utilicen su ordenador para hacer minería de criptomonedas

como bitcoin o monero. Los programas maliciosos de minería de criptomonedas utilizan los recursos de la computadora, pero envían los coins obtenidos a sus propias cuentas, no a las del propietario del equipo. En pocas palabras, un programa de minería de criptomonedas malicioso, le roba recursos para hacer dinero.

Los exploits son un tipo de malware que aprovecha los errores y vulnerabilidades de un sistema para que el creador del exploit pueda asumir el control. Los exploits están vinculados, entre otras amenazas, a la publicidad maliciosa, que ataca a través de un sitio legítimo que descarga contenido malicioso inadvertidamente desde un sitio peligroso. A continuación, el contenido dañino intenta instalarse en el ordenador tras una descarga involuntaria. Ni siquiera es necesario hacer clic. Todo lo que tiene que hacer es visitar un sitio bueno el día equivocado.

CAPÍTULO CUARTO

IMPACTO DEL INTERNET EN LA VIDA COTIDIANA

El internet ha impactado nuestra vida cotidiana, pues ha cambiado el comercio, la educación, el gobierno, la salud e incluso la forma de relacionarnos afectivamente; podría decirse que está siendo uno de los instrumentos principales de cambio social en la actualidad. Es especialmente importante cómo ha afectado a la propia comunicación social.

A medida que la popularidad de Internet ha aumentado con los años, también el número de personas que dependen de ella de manera cotidiana. Muchas personas usan Internet para mantenerse en contacto con amigos, familiares y eventos actuales. Otros simplemente pasan los días antes de la invasión digital. Para bien o para mal, Internet ha cambiado la forma en que viven muchas personas.

4.1 Los usuarios del ciberespacio aumentaron con la pandemia para evitar los contagios de COVID 19, lo cual fue aprovechado por la ciber delincuencia.

La pandemia de coronavirus COVID-19 (CHINA, 2020) fue la crisis de salud global que definió nuestro tiempo. Desde que su aparición en Asia a finales del año 2019, los países libraron una gran batalla contra la propagación de la enfermedad, haciendo

pruebas y dando tratamiento a los pacientes, rastreando los que tuvieron contacto, limitando los viajes, poniendo en cuarentena a los ciudadanos y cancelando grandes reuniones como los eventos deportivos, los conciertos y las escuelas.

La pandemia se movió como una ola, que se rompió sobre los sistemas y las personas menos capaces de hacerle frente, creando crisis sociales, económicas y políticas devastadoras que dejaron profundas cicatrices; Las personas perdieron sus trabajos e ingresos, incluso algunas nunca volvieron a la normalidad.

4.2 Coronavirus

Los coronavirus son una amplia familia de virus que se encuentran tanto en animales como en humanos. Algunos infectan al ser humano y se sabe que pueden causar diversas afecciones, desde el resfriado común hasta enfermedades más graves como el síndrome respiratorio de Oriente Medio (MERS) y el síndrome respiratorio agudo severo (SRAS), es una nueva cepa de coronavirus que no se había identificado previamente en el ser humano, ahora se conoce con el nombre de Covid- 19- no se había detectado antes de que se notificara el brote en Wuhan (China) en diciembre de 2019. Es un virus capaz de causar neumonía grave y en algunos casos fatal.

La transmisión se da de humano a humano, por gotas respiratorias y contacto estrecho, el virus se puede contagiar incluso durante el periodo de incubación (sin síntomas), los primeros síntomas son fiebre, dificultad respiratoria, tos, aumento de la frecuencia respiratoria, dolor muscular, fatiga, dolor de cabeza y diarrea.

Actualmente existen diversas vacunas y tratamientos, sin embargo, las personas continúan contagiándose de COVID 19, a pesar de estar vacunados.

la pandemia de COVID 19, la nueva forma de escuela, el trabajo a distancia y las redes sociales fueron, el caldo de cultivo que los jaquers aprovecharon infinitamente para realizar todo tipo de fraudes electrónicos.

El internet ha cambiado la forma de comunicarse de la gente, pues ha dejado de enviar oficios, cartas y tarjetas manuscritas, en la actualidad la gente suele enviar mensajes de correo electrónico y tarjetas electrónicas. La mensajería instantánea y las redes sociales como WhatsApp, Instagram, MySpace y Facebook utilizan Internet para permitir que la gente hable con amigos y familiares sin tomar nunca el teléfono. Programas de comunicación de Internet, como Yahoo, Messenger y Skype, permiten a la gente hacer llamadas a otros usuarios del programa, reemplazando a los teléfonos tradicionales. Además, estos programas ofrecen la posibilidad de hacer llamadas de vídeo que permiten a la gente verse unos a otros durante la conversación.

En el ámbito del entretenimiento, la disponibilidad de la música digital ha cambiado la forma en que la gente escucha música. Las estaciones de radio difunden en línea para aumentar la sintonía y otros sitios web como Spotify y iTunes permiten transmitir y descargar música, mucha gente transfiere películas y programas de televisión por medio de Netflix, Roku, etc. Además, Internet ha traído consigo un nuevo nivel para juegos de vídeo y de computadora, permitiendo a la gente jugar contra amigos y extranjeros de todo el mundo, tales como Clash royale, Minecraft, b2b extinción, call of duty, Halo.

Realizar compras por Internet ha cambiado la forma en que operan las empresas. Muchas empresas e individuos tienen páginas web de la empresa para promover sus productos. Esta presencia en Internet presenta el negocio a un público amplio y puede incrementar las ganancias. La disponibilidad de los minoristas en línea permite a los consumidores hacer compras sin dejar la comodidad de sus hogares. Además, los consumidores pueden utilizar Internet para investigar sus opciones antes de hacer las compras.

En el rubro de la educación hoy en día los estudiantes deben saber cómo utilizar Internet para tener éxito en la escuela. Los profesores utilizan Internet en sus aulas para fines de instrucción, entretenimiento e investigación. Muchos maestros también

publican tareas, calificaciones y otra información en línea para que los padres sepan lo que su hijo debe trabajar. Además, la introducción del aula en línea ha cambiado la forma en que muchas personas reciben su educación.

Las computadoras están presentes en todos los ámbitos de nuestras vidas. empresas, bancos, escuelas, universidades y hogares, en todos esos contextos los datos en bruto son transformados en valor y conocimiento significativo.

Literalmente las computadoras están presentes en todos los ámbitos de nuestras vidas, los usos de las computadoras son cada vez más ilimitados y su importancia vital. Algunos incluso cuestionan que su alto protagonismo ha creado dependencia, sin embargo, el futuro y las computadoras avanzan. A través de la llamada "revolución digital" las fronteras de la informática son desafiadas a diario, encontramos microprocesadores donde antes sería insólito pensarlo. Empresas, bancos, escuelas, universidades y hogares, en todos esos contextos los datos en bruto son transformados en valor y conocimiento significativo.

Hagamos una breve reflexión del uso e importancia de las computadoras en nuestro día a día.

4.3 ¿Por qué evolucionaron las computadoras?

Por obtener la reducción de los componentes electrónicos o la miniaturización de transistores cada vez más potentes.

Para cambiar sistemas cerrados, por los orientados en redes y en la nube de la informatización

Transformar los estándares de software propietarios a software de código abierto.

La escalada de los recursos multimedia: voz, imagen, video.

El avance de los sistemas de procesamiento de transacciones.

Las metodologías ágiles de desarrollo de software.

Las computadoras son la cara visible del avance tecnológico. Son sinónimo de comunicación global, entretenimiento, generación de conocimiento, análisis y transformación de datos.

4.4 Usos de las computadoras en los hogares

Las computadoras son utilizadas en nuestros hogares para múltiples propósitos, tales como acceder a redes sociales, plataformas bancarias, levantar presupuestos familiares, hacer pagos, buscar todo tipo de información, almacenar y editar contenido audiovisual y para entretenimiento en línea como por ejemplo las plataformas streaming tipo Netflix o Spotify y los videojuegos.

Las computadoras son una manera rápida y fácil de almacenar información, datos y contenido multimedia, descargar y subir información de la web, digitalizar todo tipo de contenidos a través de diferentes dispositivos de entrada.

Mucha gente compra y descarga software informático y aplicaciones que hace más fácil la organización de múltiples tareas domésticas, como control de pagos, recordatorios, seguimientos de gastos.

Este tipo de software ayuda a la gente a un control más eficiente de sus finanzas. Muchos tipos de software crean gráficos que muestran a los dueños de casa en qué están gastando el dinero.

Hoy en día incluso muchas personas trabajan de manera remota desde casa gracias a las computadoras y el internet, son una generación de trabajadores remotos o "freelancers". Otros se capacitan recibiendo clases en línea.

4.5 Las computadoras en las empresas

La mayoría de las empresas registran toda su información operativa y contable en computadoras, no es imaginable un nivel de operaciones comerciales globales de hoy en día sin los usos de las tecnologías informáticas y el internet.

Las computadoras hacen posible el fácil de almacenamiento y mantenimiento de data, facilitan la localización de archivos e información de valor.

Son innumerables las herramientas y software de trabajo que facilitan las labores administrativas y aumentan la productividad como las hojas de cálculo, sistemas contables y administrativos, los sistemas de procesamiento de transacciones y trazabilidad.

Las computadoras utilizadas por las empresas tienen capacidades para computar y resumir la información que es introducida en informes, declaraciones y documentos utilizados para múltiples propósitos.

Las compañías de todos los tamaños utilizan las computadoras para mantener bases de datos. Las bases de datos son programas que organizan información valiosa como datos de contacto de los clientes, también para sus labores de marketing, investigación de mercados y ventas, para sus gestiones de presupuestación y planificación de negocios.

4.6 Las computadoras en la educación

Desde los primeros niveles de educación las computadoras interactúan con los niños, en las propias aulas de preescolar los niños empiezan a aprender los usos y la importancia de las computadoras, a medida que los jóvenes crecen, la necesidad de herramientas computacionales continúa cambiando y creciendo: investigación, redacción, elaboración de informes, prestaciones; todo lo hacen con apoyo del computador.

Desde hace décadas tenemos la educación virtual o a distancia gracias a las computadoras y el internet, así millones de personas en el mundo han alcanzado títulos y competencias técnicas en modalidad virtual.

YouTube, Google Classroom, Google Books, Wikipedia, blogs educativos, libros electrónicos, boletines electrónicos, infografías y otras herramientas educativas no son posibles sin las computadoras que usamos hoy.

Los estudiantes no solo necesitan conocer sobre las tecnologías de la información y computación, sino que las usan durante todas las etapas de su ciclo educativo.

Suites como Microsoft Office son utilizados ampliamente por los estudiantes en todos los niveles.

Usan Microsoft Word para redactar sus investigaciones, Excel para sus cálculos matemáticos, la visualización de cifras mediante gráficos, resuelven y aprenden varias fórmulas matemáticas, financieras y lógicas, asimismo enlazan y resumen contenido cualitativo y cuantitativo para presentarlo con apoyo de Microsoft PowerPoint.

4.7 Las computadoras en la Banca

Los bancos usan las computadoras para registrar, acelerar y precisar millones de transacciones de sus clientes en sus propias agencias o en cualquier parte del mundo.

Los bancos emplean tecnologías de software y hardware para desconcentrar los volúmenes de operaciones dentro de sus agencias, ofrecer conveniencia y

accesibilidad 24/7. Ejemplos de estos recursos son los cajeros automáticos, la banca en línea y la banca por telefonía móvil.

Gracias a sus computadores centrales y servidores los bancos pueden ofrecer soporte a millones de transacciones diarias interbancarias con velocidad y precisión.

El correo electrónico, las video-llamadas, el chat, los portales informáticos para atención en línea, son solo algunas de las tecnologías que distintos bancos han implementado para la brindar servicio y atención a sus clientes.

Las computadoras encuentran un uso diseminado en diversas áreas como la de la salud, las finanzas y los entes gubernamentales, por mencionar algunas, las computadoras simplemente cambiaron nuestras vidas

CAPÍTULO QUINTO

HACKERS DE SOMBRERO NEGRO, BLANCO Y GRIS

Tal vez se tenga la noción de lo que es un hacker. Lo que tal vez no se sepa, es que no todos los hackers son iguales. Se los suele dividir en tres bandos: los de sombrero negro, los de sombrero blanco y los de sombrero gris. La terminología de los sombreros se remonta a las antiguas películas sobre el Lejano Oeste. En aquellos filmes, los protagonistas usaban sombrero blanco o de color claro, mientras que los antagonistas llevaban sombrero negro.

Un hacker se ubica en uno u otro bando en función de sus motivaciones y de la legalidad de sus actos.

5.1 Hacker de sombrero negro:

Los hackers de sombrero negro son delincuentes que se introducen en redes informáticas para llevar a cabo algún acto maligno. Algunos también se dedican a robar contraseñas, números de tarjetas de crédito y otras clases de información confidencial, a tomar sistemas de rehén o a propagar malware diseñado para borrar archivos, solo piensan en su propio beneficio: los motiva el dinero, la venganza o un simple afán

destructivo. Algunos actúan por cuestiones ideológicas y concentran sus ataques en personas con las que disienten.

Por lo general, los hackers de sombrero negro comienzan como "script kiddies". Este término, proveniente de la jerga inglesa, se aplica a los novatos que se dedican a explotar vulnerabilidades con herramientas que les han comprado a otros. Algunos de estos novatos tienen un jefe que los capacita con la esperanza de que le hagan ganar dinero. Los hackers de sombrero negro más avanzados son personas muy capacitadas. Muchos trabajan para organizaciones delictivas sofisticadas que, en ciertos aspectos, se asemejan a una empresa lícita: algunas de estas organizaciones ofrecen herramientas de colaboración a sus empleados y tienen vínculos contractuales con sus clientes. Los kits de malware de sombrero negro que se venden en la web oscura a veces incluyen garantía y números de atención al cliente.

Muchos hackers de sombrero negro tienen una especialidad, como el phishing o las herramientas de acceso remoto. Estos hackers suelen acceder a sus puestos y encargos a través de ofertas que encuentran en los foros o por intermedio de contactos entablados en la web oscura. Algunos hackers de sombrero negro crean y venden herramientas maliciosas por cuenta propia; otros prefieren trabajar a través de

franquicias o con contratos temporales. Los puntos de contacto con el mundo laboral "de todos los días" no son pocos.

Aunque el hacking se ha vuelto una herramienta de inteligencia importante para los gobiernos, la mayoría de estos hackers prefiere trabajar por cuenta propia o con organizaciones delictivas que les permitan hacer dinero fácil.

El hacking puede ser un gran emprendimiento. Su escala puede facilitar la distribución de software malicioso. Las organizaciones delictivas cuentan con redes de socios, proveedores y revendedores, y compran y venden licencias de malware que otras organizaciones utilizan luego en nuevas regiones y mercados.

Algunas organizaciones de sombrero tienen centros de contacto telefónico, que utilizan para llamar y engañar a usuarios incautos. Simulando trabajar para una empresa de renombre como Microsoft, los hackers llaman a una posible víctima y le solicitan que descargue una aplicación o les brinde acceso remoto a su equipo. Cuando la víctima cede a los argumentos de los atacantes y les franquea el acceso a su sistema o descarga el software sugerido, permite, sin saberlo, que le roben sus contraseñas o datos bancarios o que utilicen su sistema para iniciar otros ataques. ¿Lo peor? Muchas víctimas pagan una cifra exorbitante por este amable "servicio".

Pero los ataques no siempre requieren el toque humano: existen métodos automatizados que son mucho más rápidos. Una estrategia de ataque consiste en usar un bot para recorrer la Internet y buscar equipos desprotegidos, en los que sea posible introducirse a través de mensajes de phishing, adjuntos maliciosos o vínculos a sitios infectados.

Los hackers de sombrero negro son un problema mundial y sus actividades son muy difíciles de frenar. Para las autoridades, los mayores escollos son que estos atacantes rara vez dejan pruebas, que utilizan los sistemas de personas ajenas a sus actividades y que llevan a cabo acciones que abarcan más de una jurisdicción. A veces las autoridades logran desarticular un centro de piratería en un país, pero los responsables simplemente reanudan su trabajo desde otro sitio.

Hackers de sombrero negro famosos:

de los hackers de sombrero negro, Kevin Mitnick tal vez sea el más famoso. Mitnick fue, en un momento, el delincuente informático más buscado del planeta. Como hacker de sombrero negro, se introdujo en más de cuarenta empresas de renombre (entre ellas, IBM y Motorola). Hackeó, incluso, el sistema de alertas para defensa nacional de los Estados Unidos. Mitnick fue arrestado y encarcelado por sus actos. Tras cumplir

su condena, se convirtió en consultor de ciberseguridad y hoy usa sus conocimientos como hacker de sombrero blanco.

Otro hacker conocido es Tsutomu Shimomura, experto en ciberseguridad a quien se le atribuye la captura de Kevin Mitnick. Shimomura, quien se desempeñaba como investigador en el área de la física computacional, trabajaba además para la Agencia de Seguridad Nacional (NSA) de los Estados Unidos. Fue de los primeros investigadores en denunciar los problemas de seguridad y privacidad que afectan a los teléfonos móviles. Fundador de Neofocal Systems, Shimomura utilizó sus conocimientos en seguridad con fines éticos y fue fundamental para poner a Kevin Mitnick a disposición de la justicia. Su libro, Takedown, es la base de la película Track Down.

5.2 Hacker de sombrero blanco

Los hackers de sombrero blanco (a veces llamados "hackers éticos" o "hackers buenos") son la antítesis de los de sombrero negro. Cuando se introducen en un sistema o en una red informática, lo hacen meramente para identificar sus puntos vulnerables y poder recomendar modos de subsanar esas falencias, usan sus conocimientos para detectar problemas de seguridad y ayudar a las organizaciones a resguardarse de los hackers peligrosos. Algunas empresas contratan en forma directa

a estos hackers porque están puntualmente interesadas en conocer sus puntos vulnerables.

Las grandes organizaciones sufren menos tiempo de inactividad y tienen menos problemas en sus sitios web debido, en gran parte, al trabajo de estos expertos. Es sabido que los sistemas de una gran empresa son más difíciles de vulnerar que los de una organización pequeña; estas últimas rara vez tienen los recursos para atender a cada posible vulnerabilidad.

Existe un subgrupo de hackers éticos que se dedican a las "pruebas de penetración", una actividad que consiste en buscar puntos débiles y determinar qué tan vulnerable es un sistema.

Los hackers de sombrero blanco usan los mismos métodos que los de sombrero negro, pero sus acciones en un sistema son completamente legales porque tienen el visto bueno del propietario. Cuando encuentran un punto débil, no lo aprovechan para hacer circular sus códigos; por el contrario, colaboran con el encargado de la red vulnerable para que la falencia se corrija antes de que otros la hallen.

Tácticas y técnicas que utilizan los hackers de sombrero blanco:

1. Ingeniería social

Esta técnica ayuda a revelar debilidades en las defensas "de carne y hueso" de una organización. La ingeniería social consiste en usar la manipulación y el engaño para lograr que alguien haga algo indebido, como revelar su nombre de usuario y contraseña o hacer una transferencia bancaria.

2. Pruebas de penetración

Las pruebas de penetración permiten hallar —para, posteriormente, corregir— vulnerabilidades y puntos débiles en las defensas y los endpoints de una organización.

2. Reconocimiento e investigación

Esta técnica consiste en investigar a una organización para hallar vulnerabilidades en su infraestructura física o informática. La idea es recabar y recabar información hasta dar con un modo de sortear legalmente (sin dañar ni violentar nada) los mecanismos y controles de seguridad de la organización.

4. Programación

Los hackers de sombrero blanco pueden crear sistemas señuelo, denominados honeypots, para estudiar a los ciberdelincuentes o distraerlos de otros objetivos.

5. Herramientas físicas y digitales

En las pruebas de penetración, a veces se utilizan equipos y dispositivos que permiten instalar bots y aplicaciones maliciosas en la red o en los servidores a los que se pretende acceder.

Algunos hackers de sombrero blanco toman sus actividades como un juego y participan en programas de "recompensa por errores", en los que compiten con otros para alzarse con premios a cambio de reportar vulnerabilidades. Existen también cursos, eventos y certificaciones dedicadas al hacking ético.

Hacker de sombrero negro vs. hacker de sombrero blanco

La principal diferencia entre las dos clases es la motivación. Los hackers de sombrero negro se introducen en el sistema que les interesa con fines dañinos y de forma ilegal; los de sombrero blanco ayudan a las empresas a detectar falencias en sus sistemas y

a hacer los cambios pertinentes. Hacen esto, precisamente, para que los hackers de sombrero negro no puedan acceder a la información de esas empresas sin autorización.

Hackers de sombrero blanco famosos

Tim Berners-Lee Famoso por ser el inventor de la Web, Tim Berners-Lee también se identifica con el bando de los sombreros blancos. Hoy es el director del World Wide Web Consortium (W3C), el grupo que supervisa el desarrollo de la WWW.

Greg Hoglund es experto en informática forense. Se lo conoce por sus contribuciones en los campos de la detección de malware, los rootkits y el hacking de juegos en línea. Supo trabajar para el gobierno de los Estados Unidos y para la comunidad de inteligencia.

Richard Stallman fundó el proyecto GNU, una iniciativa de software libre que promueve la informática sin restricciones. Dio inicio al movimiento del software libre a mediados de los años 1980, convencido de que las computadoras deben facilitar la colaboración, no entorpecerla.

Charlie Miller es famoso por encontrar vulnerabilidades en los productos de Apple y ganar la edición 2008 de Pwn2Own, un reconocido concurso de hacking. Ha trabajado como hacker ético para la Agencia de Seguridad Nacional (NSA) de los Estados Unidos.

Dan Kaminsky se desempeñó como científico en jefe en White Ops, una empresa que utiliza el lenguaje JavaScript para detectar actividades típicas del malware. Se lo conoce principalmente por descubrir un error fundamental en el protocolo DNS, que podría haber permitido ataques masivos de suplantación de caché.

Jeff Moss trabajó en el Consejo Asesor de Seguridad Nacional de los Estados Unidos durante el mandato de Obama y fue jefe conjunto de un grupo especial sobre habilidades informáticas que se formó bajo la órbita del Consejo. Moss fundó las conferencias de hackers Black Hat y DEFCON. Se desempeña como comisionado en la Comisión Mundial sobre la Estabilidad del Ciberespacio.

5.3 Hackers de sombrero gris

Los hackers de sombrero gris existen en la intersección entre los hackers de sombrero blanco y los hackers de sombrero negro. Combinan, en cierto modo, las características de ambos bandos. Normalmente, buscan vulnerabilidades sin que el propietario del

sistema bajo análisis lo haya permitido. Cuando encuentran un problema, se lo hacen saber al responsable del sistema; a veces también se ofrecen a corregir el inconveniente por un pequeño pago.

Algunos hackers de sombrero gris creen que introducirse sin permiso en la red o el sitio web de una empresa le reporta a esta un beneficio. Sea esto cierto o no, a las compañías rara vez les agradan las intromisiones en su infraestructura de negocios.

A menudo, lo que un hacker de sombrero gris más desea es hacer alarde de sus conocimientos y obtener reconocimiento (o agradecimientos) por lo que ven como una contribución a la ciberseguridad.

Los hackers de sombrero gris pueden infringir alguna ley o precepto ético, pero no actúan con la malicia que caracteriza al hacker de sombrero negro.

Cuando un hacker de sombrero blanco descubre una vulnerabilidad, la aprovecha únicamente si tiene permiso para hacerlo y se compromete a no revelar sus hallazgos hasta que el problema haya sido resuelto. Un hacker de sombrero negro buscaría aprovecharse ilegalmente de la vulnerabilidad o les explicaría a otros cómo explotarla.

Un hacker de sombrero gris no se aprovecharía de la vulnerabilidad y tampoco les diría a otros cómo explotarla.

Estos hackers suelen creer que Internet no es un sitio seguro para las empresas y se consideran moralmente obligados a cambiar esa situación para las personas y las organizaciones. ¿Cómo promueven ese cambio? Hackeando redes y sitios web, esperanzados de que el caos resultante le demuestre al mundo que tenían razón. Los hackers de sombrero gris aseguran que sus actos no son maliciosos. A veces, los motiva solamente la curiosidad de incursionar en un sistema de alto perfil y no piensan en la privacidad ni en la legalidad.

La información que estos hackers les brindan a las empresas es, en muchos casos, valiosa. No obstante, los hackers de sombrero blanco (y gran parte de la comunidad informática) ven sus métodos con malos ojos. Los hackers de sombrero gris actúan sin autorización y sus actos son, por ende, ilegales.

Cómo trabajan los hackers de sombrero gris

Tras introducirse (ilegalmente) en una red o en un sistema, el hacker de sombrero gris puede comunicarse con el administrador y ofrecerle sus servicios (o los de un colega) para corregir el problema a cambio de un pago. Esta práctica ya no es demasiado común: hoy día, es más probable que el administrador denuncie al hacker y no que lo contrate.

Algunas empresas tienen programas de recompensas con los que buscan incitar a estos hackers a reportar sus hallazgos. Al pagar una recompensa, la empresa se evita un problema mayor: que el hacker la ataque para su propio beneficio. Pero no todas las empresas ofrecen estos programas; en tales casos, el único modo que el hacker tiene para mantenerse dentro de la ley es pedir permiso.

Cuando una empresa se niega a cooperar o no responde a tiempo, el hacker puede revelar sus hallazgos en Internet o puede explotarlos por cuenta propia. El sombrero gris, en ese caso, se tiñe de negro.

Hacker de sombrero gris vs. hacker de sombrero blanco

La principal diferencia entre un hacker de sombrero gris y uno de sombrero blanco es que el primero, si una empresa decide ignorarlo, no está atado a ningún precepto ético ni contrato de trabajo. Si encuentra una vulnerabilidad, es libre de explotarla o de darla a conocer en Internet.

Hacker de sombrero gris famoso

De los hackers de sombrero gris, uno de los más reconocidos es el especialista en seguridad informática Khalil Shreateh. En agosto de 2013, estando desempleado, Shreateh hackeó la página de Facebook de Mark Zuckerberg. Lo hizo para obligar a Facebook a corregir un error que él había descubierto y que permitía hacer publicaciones no autorizadas en la página de cualquier usuario. Aunque Shreateh había reportado la situación a Facebook, le habían asegurado desde la empresa que su hallazgo no era un inconveniente. La vulnerabilidad podría haber sido un arma poderosa en manos de un spammer profesional y fue corregida luego del incidente. Shreateh no obtuvo recompensa alguna pues infringió las normas del programa creado por Facebook para hackers de sombrero blanco.

CAPÍTULO SEXTO

FRAUDES ELECTRÓNICOS Y/O SPOOFING

Escurre el spoofing cuando una persona (a la que se le denomina spoofer) pretende ser otra persona con el fin de inducir a su objetivo a que comparta sus datos personales o para que haga alguna acción en nombre del falsificador. Normalmente, el timador se esforzará en establecer una relación de confianza con su objetivo, para asegurarse de que comparta sus datos sensibles con más facilidad. el caso es que la víctima recibe una llamada, de una persona que parece del banco, pero no lo es. Por ejemplo, la victima recibe una llamada a medio día de un martes cualquiera. Su teléfono le indica que se trata de su banco, es decir en su teléfono aparece el número que utiliza el banco, (ya que para hacer que sus llamadas falsas parezcan más reales, los spoofers también han empezado a usar software para falsear la identificación de llamada, acto llamado spoofing de número de teléfono) y, al responder, la operadora del otro lado de la línea le explica que fue recibido en su banco, una alerta de que se ha realizado un movimiento inusual en su cuenta bancaria, la victima confía en la operadora, pues se escucha entre la llamada la grabación con promociones del banco y en el menú de opciones, además de que le dice que proporcione sus datos personales, tales como NIP, número de cuenta, número de tarjeta.

Los cibercriminales emplean una variedad de métodos y técnicas para llevar a cabo ataques de spoofing y robar la información sensible de sus víctimas. Algunos de los tipos más comunes de spoofing son los siguientes:

El spoofing con emails es la más prevaleciente entre todas las formas de spoofing en la red. Similar al phishing, los spoofers envían emails a una gran cantidad de direcciones y usan logotipos oficiales y cabeceras para presentarse falsamente como representantes de bancos, compañías y agencias del orden público. Los emails que envían incluyen enlaces a páginas web maliciosas o fraudulentas en algún otro aspecto y archivos adjuntos con software maligno.

Algunos impostores pueden usar también técnicas de ingeniería social para engañar a la víctima hasta que revela la información voluntariamente. Normalmente crean páginas web falsas de bancos o carteras digitales e introducen enlaces hacia ellos en sus emails. Cuando una víctima inocente pincha ese enlace, accederán a la página falsa donde tendrán que registrarse con su información, y de este modo enviarán esa información al timador que está detrás del email falso.

Spoofing de DNS: Cada ordenador y cada página web en internet tienen asignada su propia y única dirección de IP. Para páginas web, esta dirección es diferente de la

dirección estándar "www" que usa para acceder a ellas. Cuando inserta una dirección web en su navegador y presiona "intro", el Sistema de Nombres de Dominio (DNS) encuentra rápidamente las direcciones IP que encajan con el nombre de dominio que usted ha introducido y le redirige hacia él. Los hackers han encontrado la forma de corromper este sistema y redirigir su tráfico hacia páginas web maliciosas. Esto se denomina falsificación (spoofing) de DNS.

También conocido como envenenamiento de caché, los cibercriminales usan este método para introducir datos DNS corruptos en la terminal del usuario, y por lo tanto impedirles que accedan a las páginas web que quieren visitar. En lugar de esto, cualquier dirección web que introduzcan, el usuario será redirigido a las direcciones IP definidas por el hacker, que en la mayoría de los casos alojan software malicioso o formularios falsos que recogen los datos personales de la víctima.

Spoofing de IP: Tal y como su nombre indica, la falsificación de IP se refiere al uso de una dirección de IP falsa por el remitente, ya sea para disfrazar su identidad real o para llevar a cabo ciber ataques. El remitente se apropia de una dirección de IP existente que no le pertenece, con el fin de enviar paquetes de IPs hacia redes a las que de otro modo no tendrían acceso. Como vienen de direcciones fiables, los sistemas de seguridad en la terminal del receptor verán los paquetes entrantes como

parte de una actividad normal y no será capaz de detectar la amenaza hasta que sea demasiado tarde.

No todos los casos de falsificación de IP son maliciosas. La tecnología de las redes virtuales privadas (VPN) está basada en el spoofing de IP, pero su propósito principal es proteger la identidad del usuario, permitirle el acceso al contenido que de otra manera encontraría censurado, debido a la censura de internet, y para prevenir ciber ataques mientras se usa una Wi-Fi pública. Aunque algunos países como China y Turquía prohíben el uso de VPN, es legal en la mayoría de los países del mundo, siempre y cuando no se use para perpetrar actividades de ciber crimen.

Spoofing de DDoS

El spoofing de DDoS es un subtipo de spoofing de IP que usan los hackers para llevar a cabo ataques de Denegación de Servicio Distribuido (DDoS) contra ordenadores, redes y páginas web. Los atacantes usan varias técnicas para escanear internet en busca de ordenadores con vulnerabilidades conocidas y usan estos fallos para instalar software malicioso. Esto les permite crear botnets, ejércitos de ordenadores "robots", todos controlados a distancia por el hacker.

Cuando ellos quieran, los hackers pueden activar todos los ordenadores en su botnet y usar sus recursos combinados para generar altos niveles de tráfico para atacar páginas web y servidores con el fin de inhabilitarlos. Cada uno de estos ordenadores tiene su propia y única dirección de IP. Si tenemos en cuenta que los botnets se pueden componer de un millón o más ordenadores, todos ellos con su IP única, rastrear la dirección IP del hacker puede resultar imposible.

Spoofing de ARP: Cada dispositivo conectado a internet tiene su propia dirección de Control de Acceso a Soportes (MAC) que está ligada a la dirección IP única del dispositivo a través de la ARP (Protocolo de Resolución de Direcciones). Los cibercriminales pueden entrar en la red local de su objetivo y enviar datos falsos de ARP. Como resultado, la dirección MAC del hacker se conectará con la dirección IP del objetivo, y les dará una visión del tráfico entrante de su víctima.

Los hackers optan por el spoofing de ARP para interceptar datos sensibles antes de que lleguen al ordenador objetivo. También pueden modificar partes de los datos para que el receptor no los pueda ver, mientras que algunos hackers detendrán la entrada de los datos, y por lo tanto impedirán que lleguen al receptor. Los ataques de spoofing de ARP solo se pueden llevar a cabo en redes locales que usan ARP. Además, el hacker primero tiene que conseguir acceder a la red local.

6.1 Ejemplos de ataques de spoofing

En 2006, hackers desconocidos realizaron un gran ataque de spoofing de DNS, fue el primero de este tipo, contra tres bancos locales en Florida. Los atacantes hackearon los servidores del proveedor del internet que alojaba las tres páginas web y redirigieron el tráfico hacia páginas de registro falsas, diseñadas para recoger datos personales de víctimas inocentes. Esto les permitió recolectar un número no revelado de números de tarjetas de crédito y pins, junto con otra información personal de los clientes.

En junio de 2018, los hackers llevaron a cabo un ataque de spoofing de DDoS de dos días contra la página web de la aseguradora médica americana, Humana. Durante el incidente, que se dijo que había afectado a al menos 500 personas, los hackers consiguieron robar historiales médicos completos de los clientes de Humana, incluidos los datos de su estado de salud, tratamientos recibidos y los gastos relacionados.

En 2015, hackers no identificados usaron técnicas de spoofing de DNS para redirigir el tráfico desde la página oficial de Malaysia Airlines. La nueva página de inicio mostraba la imagen de un avión con el texto "404- Avión No Encontrado" sobre la pantalla. Aunque no robaron datos ni los pusieron en peligro durante el ataque, se bloqueó el acceso a la página web y el estado de los vuelos durante varias horas.

CAPÍTULO SEPTIMO

FRAUDE INFORMÁTICO EN LA CIUDAD DE CHIHUAHUA

Durante el periodo comprendido del 2020 al 2021 el fraude informático en la ciudad de Chihuahua, se investigaba en la Unidad de Delitos Patrimoniales, ubicada en la fiscalía zona centro, en esta unidad se recibían las querellas de personas titulares de una cuenta bancaria de una institución financiera, y que habían sido víctimas de un fraude informático en cualquiera de las siguientes modalidades:

7.1 fraude informático (compra desconocidas en su cuenta y/o tarjeta)

en esta modalidad el titular de una cuenta bancaria de una institución financiera la cual tenía asignado un número de cuenta y un número de tarjeta, en una sucursal y a través de un ejecutivo, le fue cambiado el plástico de dicha tarjeta, sin haber sido solicitado ni realizado por el titular y a partir de dicho cambio de tarjeta fue pues que se hicieron cargos a la cuenta en mención, mismos que él no reconoció y de los cuales se percató, al verificar sus estados de cuenta en donde se refleja que existen varios cargos, por lo que solicita vía telefónica que su cuenta sea bloqueada, proporcionándosele un número de folio, posteriormente presenta su queja en la institución financiera, sin embargo, posteriormente, es emitida por el banco una resolución en la que se le informa que su queja es improcedente, por lo que presenta su querella en la Unidad de Delitos Patrimoniales.

7.2 fraude informático (extracción de información por medio de llamada telefónica- spoofing)

en esta modalidad el titular de una cuenta bancaria de una institución financiera la cual tenía asignado un número de cuenta y un número de tarjeta y una persona que parece del banco, pero no lo es, le indica que se trata de una llamada de su banco, es decir en su teléfono aparece el número que utiliza el banco, recordemos que para hacer que sus llamadas falsas parezcan más reales, los spoofers también han empezado a usar software para falsear la identificación de llamada, acto llamado spoofing de número de teléfono y, al responder, la operadora del otro lado de la línea le explica que fue recibido en su banco, una alerta de que se ha realizado un movimiento inusual en su cuenta bancaria, la victima confía en la operadora, pues se escucha entre la llamada la grabación con promociones del banco y en el menú de opciones, además de que le dice que proporcione sus datos personales, tales como NIP, número de cuenta, número de tarjeta y al obtenerlos fes pues que se hicieron cargos a la cuenta de la víctima, mismos que no reconoció y de los cuales se percató, al verificar sus estados de cuenta en donde se refleja que existen varios cargos, haciendo la reclamación a su institución financiera, sin embargo, posteriormente, es emitida por el banco una resolución en la que se le informa que su queja es improcedente, por lo que presenta su querella en la Unidad de Delitos Patrimoniales.

7.3 Fraude informático a través de la banca en línea.

en esta modalidad el titular de una cuenta bancaria de una institución financiera la cual tenía asignado un número de cuenta y un número de tarjeta y que a su vez es usuario de la banca en línea, el cual a través de su celular ingresa a la banca web de Scotiabank siendo la siguiente: www.scotiabank.com.mx/ y al ingresar todo parecía normal, entonces en dicha página agrega todos sus datos sobre su cuenta a efecto de

realizar una inversión con su tarjeta de débito y en su cuenta en la cual tenía un monto de $8,574.58.00 pesos, luego le apareció un mensaje de texto del teléfono 55-5728-1900 de que había generado una clave para retiro de efectivo sin tarjeta en Scotia móvil por los $8,000.00 pesos; al ver este mensaje de inmediato se dirigió al cajero de Scotiabank más cercano y observa que sus $8000.00, habían sido retirados de su cuenta, la víctima llama al número de aclaraciones de Scotiabank y la operadora que le atendió bloqueo la cuenta inmediatamente, y le solicitaron hacer una carta a mano que manifestara lo que me había ocurrido para después escanearla y mandarla al correo: tramitescc@scotiabank.com.mx; así mismo le generaron un folio de aclaración posteriormente presenta su queja en la institución financiera, sin embargo, posteriormente, es emitida por el banco una resolución en la que se le informa que su queja es improcedente, por lo que presenta su querella en la Unidad de Delitos Patrimoniales.

En esta misma modalidad, pero en diverso caso, el titular de una cuenta bancaria de una institución financiera la cual tenía asignado un número de cuenta y un número de tarjeta y que a su vez es usuario de la banca en línea, ingresa como habitualmente lo hace, al sistema web de Scotiabank denominado Scotiaweb, para verificar sus cuentas, de las cuales tiene tres con esa institución y una tarjeta de crédito, al ingresar al sistema Scotiaweb, es decir dentro de la página del banco, se le solicita que realice una actualización requiriéndole su correo electrónico, celular y teléfono fijo, posteriormente el e. Llave, no permitiéndole el acceso, por lo que se comunica con un asesor que le recomienda acudir a su sucursal en la ciudad de Chihuahua, Chih., la víctima acude y se entrevista con la gerente quien le informa que habían sido vaciadas sus tres cuentas, y que le habían abierto una línea de crédito por la cantidad $250,000.00 pesos, ,la víctima no reconoce haber realizado dichos movimientos, documentados por la institución bancaria, haciendo por escrito la inconformidad para que de manera interna la institución bancaria pudiera darle el seguimiento

correspondiente; sin embargo, posteriormente, es emitida por el banco una resolución en la que se le informa que su queja es improcedente, por lo que presenta su querella en la Unidad de Delitos Patrimoniales.

Las victimas en donde el modus operandi es similar al de este último ejemplo, Regularmente son micro y pequeños empresarios los cuales requieren de la banca en línea para realizar sus labores.

Estos delitos se encuentran previstos y sancionados en código penal del estado de chihuahua en capítulo IV , fraude en su Artículo 223. El cual señala que: A quien por medio del engaño o aprovechando el error en que otro se halle, se haga ilícitamente de alguna cosa u obtenga un lucro indebido en beneficio propio o de un tercero, se le impondrán:

I. De treinta a noventa días multa, cuando el valor de lo defraudado no exceda de cincuenta veces el valor diario de la Unidad de Medida y Actualización.

II. Prisión de seis meses a tres años y de noventa a doscientos cincuenta días multa, cuando el valor de lo defraudado exceda de cincuenta, pero no de quinientas veces el valor diario de la Unidad de Medida y Actualización.

III. Prisión de tres a seis años y de doscientos cincuenta a setecientos cincuenta días multa, cuando el valor de lo defraudado exceda de quinientas, pero no de cinco mil veces el valor diario de la Unidad de Medida y Actualización; y

IV. Prisión de seis a doce años y de setecientos cincuenta a mil doscientos cincuenta días multa, si el valor de lo defraudado excede de cinco mil veces el valor diario de la Unidad de Medida y Actualización. Cuando el delito se cometa en contra de dos o más personas, se impondrá además las dos terceras partes de las penas previstas en las fracciones anteriores.

El mismo Código Penal del Estado de Chihuahua en su Artículo 226 Bis, manifiesta que: Al que alcance un lucro indebido para sí o para otro, valiéndose de alguna manipulación informática, alteración de programas sistematizados, del empleo no autorizado de datos o artificio semejante, se le impondrá la punibilidad señalada para el delito de fraude.

Pero también el código penal federal en su Artículo 11 Bis. - Para los efectos de lo previsto en el Título X, Capítulo II, del Código Nacional de Procedimientos Penales, a las personas jurídicas podrán imponérseles algunas o varias de las consecuencias jurídicas cuando hayan intervenido en la comisión de los siguientes delitos:

X. De la Ley de Instituciones de Crédito, los previstos en los artículos 111; 111 Bis; 112; 112 Bis; 112 Ter; 112 Quáter; 112 Quintus; 113 Bis y 113 Bis 3;

A su vez el Delito innominado contenido en el artículo 113 bis de la ley de instituciones de crédito que a la letra dice: Artículo 113 Bis. - A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito o de los recursos o valores de estas últimas, se le aplicará una sanción de cinco a quince años de prisión y multa de quinientos a treinta mil días de salario.

Por lo que se tiene que este delito está previsto en una ley federal y resulta aplicable el principio de especialidad, de ahí que en el caso se actualiza la competencia prevista en el numeral 50, fracción I, inciso a), de la Ley Orgánica del Poder Judicial de la Federación, por lo que la Agente del Ministerio Público de la unidad especializada de delitos patrimoniales declino las carpetas de investigación al fuero federal, sin embargo, le fueron devueltas.

A pesar de que de lo anterior y de manera clara tenemos que existe un cliente de una Institución de Crédito mismo que relata hechos de los cuales fue víctima, en donde evidencia la intervención de un sujeto activo quien realizo un retiro de efectivo sin tarjeta de los recursos monetarios que la víctima tenía en su cuenta, el mismo se

realizó por el sujeto activo, sin derecho ni consentimiento del afectado, naciendo en este punto la disposición indebida; lo anterior fue logrado a través del cuadro emergente que apareció dentro de la página del banco, mediante el cual el sujeto activo se hizo de la información confidencial de la víctima y como consecuencia, el activo tuvo acceso a la cuenta bancaria del cliente y pudo disponer de los recursos depositados en ella. La conducta descrita encuadra en el tipo penal y especial previsto y sancionado en el numeral 113 Bis de la Ley de Instituciones de Crédito en razón de que el mismo establece: "A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de recursos o valores de los clientes de las instituciones de crédito, se le aplicará una sanción de tres a diez años de prisión y multa de quinientos a treinta mil días de salario. Lo anterior es así aún y cuando la víctima, quien al encontrarse en la idea de que navegaba de forma segura dentro de la página de su institución bancaria e ignorando las argucias de las cuales el sujeto activo se estaba valiendo, proporciona datos confidenciales, así pues, como haya sido el modo en que el sujeto activo se hizo de la información de la víctima (engaño), el detrimento patrimonial no fue al momento de proporcionar la información, pues esto no implicó la entrega directa e inmediata de una cantidad de dinero por parte de la víctima, sino de información confidencial que podía o no, ser utilizada; luego entonces la conducta delictiva en el presente caso, inicia cuando con posterioridad el sujeto activo hace uso de la información confidencial tal como token y/o contraseñas y dispone de manera indebida de los recursos de un cliente de una institución de crédito, siendo precisamente esta conducta un elemento fundamental que se recoge en los hechos,

por otorgar amplitud típica mayor, pues esos recursos del cliente son el bien jurídico tutelado por la norma especial, surtiéndose así uno de los requisitos de especialidad, pues si el hecho y/o delito de que se trata está previsto en una ley federal como lo es la de Ley de Instituciones de Crédito en su numeral 113 Bis, resulta aplicable el principio de especialidad por ser recursos o valores de un cliente de una Institución Bancaria, de tal manera que la conducta desplegada en los hechos en estudio encuadra en el tipo penal descrito en el artículo referido, y por consiguiente actualizándose la competencia prevista en el numeral 50, fracción I, inciso a), de la Ley Orgánica del Poder Judicial de la Federación. Lo anterior encuentra sustento en la exposición que hace Jesús Zamora Pierce en su obra Transferencia Ilícita de Recursos, paginas 43, 44 y 45, pues el mismo señala la interpretación que debe dársele precisamente a dicho numeral, y explica que: "el verbo típico disponer, pues cuando aún y el legislador menciona también los verbos utilizar, obtener o transferir ellos son mejores ejemplos de disposición y lo que a última instancia sanciona es cualquier forma de disponer. El bien jurídico tutelado es el patrimonio de los clientes de las instituciones de crédito, mas no todo su patrimonio, sino únicamente aquella parte de que se manifiesta bajo la forma de recursos o valores depositados en dichas instituciones. El sujeto activo es indiferente, puede serlo cualquiera, pero si es un funcionario o empleado de las instituciones de crédito o un tercero ajeno, pero con acceso autorizado por estas a los sistemas de las mismas, ello da lugar a un tipo de penalidad agravada. El sujeto pasivo son los clientes de las instituciones de crédito. La conducta de quien se hace de la firma electrónica de un cliente del sistema

financiero y mediante el uso de esa firma, dispone de los recursos depositados en la cuenta bancaria de ese cliente, queda perfectamente tipificada por el delito del artículo 113 Bis de la Ley de Instituciones de Crédito. Este artículo no menciona entre los elementos del tipo, el acceso a los sistemas o programas de informática del sistema financiero, ni es necesario que lo haga, puesto que se enmarca dentro de una forma verbal de mucha mayor amplitud "disponer de cualquier forma", que engloba y comprende todos los medios, incluyendo, el acceso a los sistemas. De la misma forma procede el legislador cuando tipifica el homicidio como el delito que comete quien priva de la vida a otro, sin preocuparse por enumerar los múltiples y muy diversos medios por los que el activo puede lograr este fin". Adminiculado a lo anterior tenemos las siguientes tesis con los datos de identificación que al efecto se precisan: Sexta Época, Registro 257498, Instancia: Pleno, Fuente: Semanario Judicial de la Federación, Volumen CXXXIV Primera Parte: Materia Penal, Pagina 22, bajo el título y texto: "instituciones de crédito, delitos previstos en los artículos 153 bis y 153-1, de la ley general de competencia juez federal instituciones de crédito, delitos previstos en los artículos 153 bis y 153 bis-i, de la ley general de. competencia del juez federal. Los Jueces del orden común están imposibilitados para conocer de los delitos previstos en la Ley General de Instituciones de Crédito y Organizaciones Auxiliares, porque es una ley federal, en la que se prevén delitos especiales y de los que solamente pueden conocer las autoridades judiciales federales, con arreglo a lo dispuesto en la Ley Orgánica del Poder Judicial de la Federación. De no ser así, se incurriría en el absurdo de que los Jueces del orden común podrían conocer de hechos no tipificados en las

leyes expedidas en el Estado y de acuerdo con su régimen soberano, violándose con ello lo dispuesto por el artículo 104 de la Constitución General de la República. Por tanto, cuando no se trata de controversias que afecten a intereses particulares, sino que por tratarse de hechos tipificados como delitos, son de orden público, los Jueces y tribunales del orden común no tienen competencia para conocer de ellos, porque con arreglo a lo dispuesto por el artículo 12 del Código Federal de Procedimientos Penales, en materia penal no cabe prórroga ni renuncia de jurisdicción. Competencia 126/67. Suscitada entre el Juez de Distrito del Estado de México y el Juez Primero de lo Penal en Almoloya de Juárez, Estado de México. 13 de agosto de 1968. Unanimidad de diecisiete votos. Ponente: Abel Huitrón y Aguado.

Novena Época, Registro: 163662, Instancia: Tribunales Colegiados de Circuito, Tesis Aislada, Fuente: Semanario Judicial de la Federación y su Gaceta XXXII, octubre de 2010, Materia(s): Penal, Tesis: I.3o.P.90 P Página: 2972.

conflicto competencial por razón de fuero en atención al principio de especialidad, se surte la competencia a favor de un juez de distrito y no de uno del orden común, cuando se actualiza el delito previsto en el artículo 113 bis, párrafo primero, de la ley de instituciones de crédito y no el descrito en el numeral 336, fracción VII, del código penal para el distrito federal.

Si a un procesado se le dictó auto de formal prisión por estimar que prestó ayuda al autor material del delito, ya que recibió el dinero en efectivo solicitado por el sujeto activo, quien anterior a ese acto se hizo pasar por cuentahabiente de una institución bancaria, realizó una operación y utilizó para ello la llave de acceso (NIP de atención telefónica) de una cuenta de cheques -que estaba cancelada-, y precisó que dicho numerario debía ser entregado al imputado en un lugar determinado, obteniendo en forma indebida recursos de un cliente de una institución de crédito, como se advierte de la escritura pública respectiva, es inconcuso que de ese ilícito corresponde conocer a un Juez de Distrito, atento a que se colma el hecho que prevé el artículo 113 bis, párrafo primero, de la Ley de Instituciones de Crédito y no la hipótesis normativa del precepto 336, fracción VII, del Código Penal para el Distrito Federal, pues si el delito de que se trata está previsto en una ley federal resulta aplicable el principio de especialidad, de ahí que en el caso se actualiza la competencia prevista en el numeral 50, fracción I, inciso a), de la Ley Orgánica del Poder Judicial de la Federación. TERCER TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO. Competencia 2/2010. Suscitada entre el Juzgado Sexto de Distrito de Procesos Penales Federales y el Juzgado Sexagésimo Noveno Penal, ambos del Distrito Federal. 18 de marzo de 2010. Unanimidad de votos. Ponente: Homero Ruiz Velázquez. Secretaria: María Imelda Ayala Miranda.

CONCLUSIONES

A pesar de que este delito es investigado en la Unidad de Delitos Patrimoniales, esta unidad no cuenta con las herramientas necesarias para la investigación, pues a pesar que se tiene a la policía cibernética y a la Dirección general del centro de información, análisis y estadística criminal, que se subdivide en Dirección de integración y evaluación de información delictiva, Dirección de análisis de evidencia digital e informática forense, dirección de centro de control, comando, comunicación y cómputo, y de la dirección de estadística criminal, y de que se emite un dictamen después de que es analizado el equipo de cómputo y que se solicita información a las diversas áreas de fiscalía y a la comisión nacional bancaria y de valores, lo cierto es que las víctimas de fraude informático en cualquiera de las modalidades no reciben justicia, pues es muy limitada la información que aportan las diversas áreas y de que los hackers desconocidos realizan sus ataques,, por medio de spoofing, hackean los servidores de proveedores de internet, redirigen el tráfico hacia páginas de registro falsas, diseñadas para recoger datos personales de víctimas inocentes. Esto les permite recolectar números de tarjetas de crédito y PINS, junto con otra información personal de las víctimas.

Por lo que es fundamental limitarse a utilizar fuentes de confianza para las aplicaciones móviles e instalar únicamente aplicaciones de buena reputación, descargadas directamente del sitio del proveedor, jamás de ningún otro sitio.

El fraude Informático es cada vez son más frecuente y el detrimento causado a las víctimas no es reparado. La ciberdelincuencia está en todas partes, las personas y empresas están constantemente siendo atacadas por los delincuentes en busca de datos confidenciales y debilidades de sus sistemas.

Se requiere más capacitación de los operadores jurídicos en esta materia, pues la marcada carencia de herramientas de investigación y la falta de coordinación que existen dentro de los sistemas de impartición de justicia mexicanos y específicamente los de la ciudad de Chihuahua, Chihuahua, quienes no han tenido la capacidad de definir si le corresponde la investigación de los hechos delictivos a los ministerios públicos del fuero común o a los ministerios públicos del fuero federal, deriva en la vulneración de los derechos de las víctimas.

REFERENCIAS BIBLIOGRÁFICAS

¿Qué es el Covid-19? (unam.mx)

Wang, C., Horby, P. W., Hayden, F. G., & Gao, A novel coronavirus outbreak of global health concern. The Lancet [Internet]. 2020 [citado 18 mar 2020]. 35(10223). Disponible en: URL doi:10.1016/s0140-6736(20)30185-9

A. Du Toit, Outbreak of a novel coronavirus, Nat. Rev. Microbiol.[Internet] 2020 [citado 19 mar 2020] 18 (123) Disponible en: URL https://doi.org/10.1038/s41579-020-0332-0.

L.L. Ren, Y.M. Wang, Z.Q. Wu, Z.C. Xiang, L. Guo, T. Xu, et al., Identification of a novel coronavirus causing severe pneumonia in human: a descriptive study, Chinese Med J [Internet] 2020 [citado 10 mar 2020] 30 (5). Disponible en: URL https://doi.org/10.1097/CM9.0000000000000722.

Who.int. World Health Organisation. 2020. [actualizado 12 enero de 2020, citado 19 mar 202]. Disponible en: URL https://www.who.int/csr/don/12-january-2020-novel-coronavirus-china/en/

C. Huang, Y. Wang, X. Li, L. Ren, J. Zhao, Y. Hu, et al., Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China, Lancet [Internet]. 2020 [citado 19 mar 2020] 395 (10223). Disponible en: URL 497–506, https://doi.org/10.1016/S0140-6736(20)30183-5.

Lu, H. (2020). Drug treatment options for the 2019-new coronavirus (2019-nCoV). BioScience Trends.[Internet] 2020 [citado 18 mar 2029] 14 (1). Disponible en: URL doi:10.5582/bst.2020.01020

Rothan H., Byrareddy S. The epidemiology and pathogenesis of coronavirus disease (COVID-19). outbreak. Journal of Autoimmunity.[Internet] 2020 [citado 19 mar 2020] 17 (1). Disponible en: URL https://doi.org/10.1016/j.jaut.2020.102433

Wang, W., Tang, J., & Wei, F. (2020). Updated understanding of the outbreak of 2019 novel coronavirus (2019-nCoV) in Wuhan, China. Journal of Medical Virology.[Internet] 2020 [citado 19 mar 2020] 20 (3). Disponible en: URL doi:10.1002/jmv.25689

First Case of 2019 Novel Coronavirus in the United States. Holshue M,. The New England Journal of Medicine. [Internet] 2020 [citado 19 mar 2020] 382 (4). Disponible en: URL https://www.nejm.org/doi/full/10.1056/NEJMoa2001191

20minutes.fr. Francia. Provenzano, Elsa. Coronavirus: Que sait-on du cas détecté à Bordeauz?. [actualizado en 17 enero 2020, citado 18 mar 2020] . Disponible en: URL: https://www.20minutes.fr/bordeaux/2703783-20200126-coronavirus-sait-cas-detecte-bordeaux

Trabajos citados

(s.f.).

CHINA, U. (17 de FEBRERO de 2020). UNAM CHINA . Obtenido de UNAM CHINA : ¿Qué es el Covid-19? (unam.mx)

oracle. (2022). oracle. Obtenido de oracle: https://www.oracle.com/es/database/security/que-es-el-spoofing.html