Septiembre 2014

CIBERDELINCUENCIA UN MAL QUE AFECTA A LA SOCIEDAD ACTUAL

MSc. Emilio Javier Flores Villacrés
Magíster en Educación Superior por la Universidad de Guayaquil. Ingeniero en Sistemas Administrativos Computarizados. Catedrático de la Universidad de Guayaquilemilio_flores_2009@hotmail.com
MSc. María Isabel Asanza Molina
Magíster en Educación Superior por la Universidad de Guayaquil. Economista. Catedrática de la Universidad de Guayaquil
maria-isabel-asanza@hotmail.com
Ing. Marcelo Berrones Miguez
Ingeniero Industrial por la Universidad de Guayaquil. Catedrático de la Universidad de Guayaquil
marcelo_berrones67@hotmail.com

Resumen

Esta investigación trata acerca de la ciberdelincuencia, es un tipo de delito que afecta a la sociedad en la actualidad debido a los avances tecnológicos y la poca costumbre de revisar o eliminar la información de las cuentas de banco, dejar de aceptar a todas las personas que no conoce en las redes sociales y no abrir todos los correos electrónicos que reciben por que pueden tener virus, si no se toman las precauciones adecuadas se deja una puerta abierta para que cualquier persona con un conocimiento de ciertos programas o mediante el uso de virus pueden engañar para tener acceso a la información personal y financiera pasando a ser víctimas de estos delincuentes.

Ciberdelincuencia - Sociedad - Redes Sociales - Correos Electrónicos - Programas

Abstract

This investigation treats about the ciberdelincuencia, it is a type of crime that fond of the society at present due to the technological advances and the little custom of revising or eliminate the information of the accounts of bench, stops to accept to all peoples that does not understand the social nets and does not open all e-mails they receive for that can have virus, if not take the appropriate precautions leave an open door in order that any person with a knowledge of certain programs or by means of the use of virus can deceive to have access to the personal and financial information victims of these criminals.

Ciberdelincuencia - Society - cast a net social - e-mails - program

1. INTRODUCCIÓN

TICS

Es la sigla de Tecnologías de la Información y la Comunicación. El concepto se utiliza para nombrar a las técnicas vinculadas a la gestión y la difusión de información. La telefonía, Internet, los videojuegos, los reproductores digitales y la informática forman parte del campo de las TIC.[1]

Los avances de la tecnología han permitido que las transacciones que se tenían que realizar personalmente y llevaban mucho tiempo ahora se las puede realizar de manera rápida pero a veces este proceso no es tan fácil como suena, hay tener un poco de conocimiento sobre el manejo de un navegador y tener en mente lo que desea hacer a veces se suelen abrir varias pantallas con múltiples opciones, las cuales sino se cierran adecuadamente dejan la información abierta y alguien puede accesar a la información.

Lo más importante es que actualmente hay que tener mucho cuidado con los datos que se envían por email o cualquier medio electrónico, debido a que pueden contar con información importante en donde tal vez existan datos importantes con datos personales y de cuentas financieras.

Sociedad[2]

Sociedad es un grupo de seres que viven de una manera organizada. La palabra proviene del latín "societas", que significa asociación amistosa con los demás.

Los miembros de una sociedad pueden ser de diferentes grupos étnicos. También pueden pertenecer a diferentes niveles o clases sociales. Lo que caracteriza a la sociedad es la puesta en común de intereses entre los miembros y las preocupaciones mutuas dirigidos hacia un objetivo común.

La sociedad está compuesta por hombres y mujeres de todas las edades que muestran la gran riqueza personal que compone la estructura social puesto que la diferencia generacional es positiva.

Hay personas que debido a la diferencia generacional se les hace difícil adaptarse de manera rápida a los avances tecnológicos, es por eso que se presentan varios problemas en el manejo de correos electrónicos,

Delincuencia organizada

Las definiciones de delincuencia organizada varían ampliamente de un país a otro. Las redes organizadas suelen participar en distintos tipos de actividades delictivas que afectan a varios países. Entre ellas se pueden contar la trata de personas, el tráfico de armas y drogas, los robos a mano armada, la falsificación y el blanqueo de capitales. En realidad, casi todos los ámbitos delictivos que se combate en INTERPOL presentan un aspecto organizativo.[3]

Pero uno los puntos que se pueden ver en diferentes países son los actos delincuenciales que se están dando como el hackeo de una cuenta de email o de una cuenta en redes sociales, hasta un clonación de un numero de celular.

Seguridad[4]

---

[1] Definición de tic - Qué es, Significado y Concepto. Disponible en: http://definicion.de/tic/#ixzz3DhgOUJmh.

[2] Definición de Sociedad, 2011. Disponible en http://definicion.mx/sociedad/

[3] Delincuencia organizada, Disponible en: http://www.interpol.int/es/Criminalidad/Delincuencia-organizada/Delincuencia-organizada

[4] Concepto de seguridad, Definición, Significado y Qué es , Disponible en: http://definicion.de/seguridad/#ixzz3DhsaxL59

El término seguridad posee múltiples usos. A grandes rasgos, puede afirmarse que este concepto que proviene del latín securitas hace foco en la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza.

En informática se habla de dos tipos de seguridades, la física (barreras físicas que impiden el paso al sistema de cualquier persona no acreditada. Se realiza a través de aplicaciones y procedimientos específicos que tienen el objeto de bloquear el acceso a dichos individuos) y la lógica (las formas en las que se desempeña este tipo de seguridad es a través de encriptación de códigos, de modo que no puedan ser leídos o traducidos por los intrusos que pudieran sobre pasar las barreras físicas, códigos de autenticación y antivirus o pared de fuego, en el caso de usar un sistema operativo como Windows). A la hora de elaborar un diseño, ya sea de página web o de espacio en la red de cualquier tener en cuenta ambos tipos de seguridad es fundamental.

Cabe destacar que existen conceptos mal establecidos: que son Hacker y Cracker.

Hacker

Es un individuo que se encuentra buscando siempre la forma de vulnerar las barreras de seguridad de los sistemas de información a fin de obtener algún tipo de información confidencial. El objetivo fundamental del verdadero hacker es aprender y satisfacer la curiosidad y creatividad, no busca hacer daño. El afán es crear, no destruir. Es un verdadero geek (alguien obsesionado y enamorado de la tecnología en general y de la informática en particular).

Cracker

Es aquel que tiene capacidades semejantes a la de un hacker pero que las utiliza con objetivos maliciosos. La razón de toda la investigación es destruir sistemas, borrar o robar datos y hacer daño por el solo hecho de divertirse.

Virus

Es un programa de computadora que tiene la capacidad de causar daño y la característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora. [5]

Ingeniería social [6]

Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

El principio que sustenta la ingeniería social es el que en cualquier sistema los usuarios son el eslabón débil. En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas “cadenas”, llevando así a revelar información sensible, o a violar las políticas de seguridad típicas.

[5] Ángel Fire. ¿Qué es un virus? Disponible en: http://www.angelfire.com/dragon2/ilovebsb/pagina7.html

[6] Expresión Binaria. Ingeniería Social. Disponible en: http://www.expresionbinaria.com/glosario/ingenieria-social/

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco- en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

Ciberdelincuencia

Comprende cualquier acto criminal que utilice ordenadores y redes. Además, la ciberdelincuencia también incluye delitos tradicionales realizados a través de Internet. Por ejemplo: los delitos motivados por prejuicios, el telemarketing y fraude de Internet, la suplantación de identidad y el robo de cuentas de tarjetas de crédito se consideran ciberdelitos cuando las actividades ilegales se llevan a cabo utilizando un ordenador e Internet.[7]

2. CONTENIDO

Delincuencia Informática

La delincuencia informática mundial tiene un costo de 114 mil millones de dólares anuales, se determinó que más de dos tercios de los adultos en línea (69%) han sido víctimas de la ciberdelincuencia alguna vez en la vida. Cada segundo, 14 adultos son víctimas de un crimen cibernético, lo que deja como resultado más de un millón de víctimas del cibercrimen todos los días. El 10% de los adultos en línea han experimentado la ciberdelincuencia en los teléfonos móviles el Symantec Internet Security Threat Report revela que en 2010 hubo un 42% más de vulnerabilidades móviles en comparación con la cantidad reportada en 2009. El número de nuevas vulnerabilidades de sistemas operativos móviles aumentó de 115, en 2009, a 163, en 2010. [8]

Como se puede observar cada día aumentan las víctimas de esta forma de delincuencia debido en parte a los avances tecnológicos y la falta de conocimiento del uso apropiado de estas nuevas herramientas, los smartphones han servido para agilizar procesos que solo se podían realizar en una computadora, ahora desde un teléfono puede conectarse al internet y de ahí conectarse a las cuentas bancarias, muchas de estas instituciones han sacado múltiples aplicaciones conocidos como app donde el manejo es más sencillo, que cuando se tratan de conectar desde la computadora, pero de igual forma en ambos casos deben tomarse precauciones y seguridades.

Se debe cuidar todo tipo de información que se suba, debido a que existen virus que lo pueden engañar haciéndolo creer que se cayó la conexión y usted trata de conectarse al sitio de nuevo volviendo a ingresar los datos pero lo que en realidad hace es que la información es enviada a otro sitio para que luego la persona que envió ese virus pueda ver los datos y usarlos para realizar compras, estafas, sacar dinero, entre otros.

Ejemplos de ciberdelitos[9]

Que afectan principalmente a redes o dispositivos informáticos serían:

- Malware y código malintencionado
- Ataques de denegación de servicio
- Virus informáticos

Malware y código malintencionado[10]

---

[7] Informe de Cibercrimen de Norton 2011. Disponible en: http://www.computerworldmexico.mx/Articulos/18883.htm

[8] Ciberdelincuencia: ¿qué es?, Disponible en: http://www.bullguard.com/es/bullguard-security-center/internet-security/security-tips/cybercrime.aspx

[9] Informe de Cibercrimen de Norton 2011. Disponible en: http://www.computerworldmexico.mx/Articulos/18883.htm

El malware es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra malware proviene del término en inglés malicioso software, y en español es conocido con el nombre de código malicioso.

Existen diferentes clasificaciones de código malicioso:

- Virus.
- Caballos de Troya (troyanos).
- Puertas traseras (backdoors).
- Gusanos de Internet (worms).
- Bots.
- Spyware.
- Adware.

Todos estos códigos maliciosos pueden ser modificados por ciberdelincuentes y usarlos como un medio para robar dinero y en algunos casos copiar información que tengan derecho de propiedad intelectual tanto a particulares como a empresas.

Ataques de denegación de servicio

(Denial of Service, DoS). En seguridad informática, un ataque de denegación de servicio, es un ataque a una red o a un sistema, que causa que un servicio o recurso sea inaccesible.[11]

Este tipo de virus ocasiona una pérdida de la conectividad de la red debido a que genera un consumo del ancho de banda de la red ocasionando muchos problemas o la sobrecarga de los recursos del sistema, produciendo que la maquina este ocupada con múltiples procesos y no se pueda realizar los trabajos, en algunos casos muchos usuarios llegan a pensar que la computadora está dañada.

En un ataque DDoS típico el hacker (o si lo prefiere cracker) empieza buscando una vulnerabilidad en un sistema informático y creando un master para el DDoS. Desde este master el sistema identifica y se comunica con otros sistemas que pueda utilizar. El atacante usa las herramientas de cracking disponibles en internet sobre cientos o miles de equipos. Con un solo comando el atacante puede controlar todas estas máquinas para que lancen un ataque simultáneo sobre un objetivo concreto. La avalancha de paquetes provoca el error de denegación de servicio.[12]

Otros dispositivos también pueden llegar a tener este problema, todo esto se debe a que muchas veces las personas abren información sin tener el cuidado adecuado.

Virus informáticos[13]

---

[10] Eduteca. ¿Qué es el malware?. Disponible en: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=193

[11] ALEGSA. Definición de Ataque de denegación de servicio Disponible en: http://www.alegsa.com.ar/Dic/ataque%20de%20denegacion%20de%20servicio.php#sthash.WPBkYLE0.dpuf

[12] Techtarget. Ataque de denegación de servicio (DDoS). Disponible en: http://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

[13] PSAFE. ¿Cuáles son los tipos de virus que existen? Disponible en: http://www.psafe.com/ayuda/cuales-son-los-tipos-de-virus-que-existen/

Worms o Gusanos

Son variantes de los virus, una subclase particularmente nociva de los virus que se distingue por ser capaz de ser distribuir sin acción humana, utilizándose de todas las capacidades de comunicación disponibles en un PC/dispositivo para ser auto distribuido. Otra diferencia excepcional entre virus y worms es que los worms se replican dentro de un PC/dispositivo infectado, creando miles de copias de sí mismo, con el objetivo de ser distribuido más rápidamente y evitar que un antivirus remuévalo antes de causar daños e infectar otros dispositivos y usuarios conectados a el PC/dispositivo infectado. Worms también son utilizados para abrir puertas en el PC/dispositivo del usuario infectado, permitiendo el total control remoto por un hacker de todos los recursos disponibles en el PC/dispositivo infectado. Ese tipo de worm es normalmente llamado de Back Door (puerta trasera).

Trojan Horse (Caballo de Troya)

Es tan desleal cuanto el homónimo de la mitología griega. Un trojan normalmente disfrazase de un aplicativo normal y bueno mientras la instalación. Usuarios que reciben los trojans son convencidos a instalarlos y ejecutarlos por tenerlos recibido de una fuente confiable (un amigo, pariente o a través de e-mail disfrazado de una institución comercial con la cual el usuario se relaciona - bancos, oficinas de gobierno, entre otros). Una vez que es ejecutado, un trojan puede causar serios perjuicios, como robo de contraseñas bancarias, datos de tarjetas de crédito, contraseñas de redes sociales, etc. Muchos trojans abren puertas en el PC/dispositivo infectado - la llamada back door (puerta trasera) - permitiendo el control remoto del hacker o grupo de hackers liados en el ataque al equipo. Diferente de los virus y worms, trojan no se distribuyen infectando otros archivos ni si reproducen a si propios.

Blended Threats (Amenazas Compuestas)

Son caracterizadas por la combinación de múltiples códigos maliciosos en un sólo ataque e son consideradas las más peligrosas y devastadoras amenazas digitales que existen hoy. Combinando lo que existe de peor en virus, worms y trojans, una amenaza compuesta distingues por atacar múltiples aspectos de un sistema (PCs, smartphones, tablets, etc) al mismo tiempo en que infecta la red de datos en la cual el dispositivo está conectado. Así, ella ataca cualquier otro PC/dispositivo o servidor conectado por la red local mientras se reproduce como los worms. Ella también se distribuye no sólo a través de los contactos de e-mail, sino también por cualquier otro mecanismo disponible (redes sociales, chats, SMS, etc) en el dispositivo infectado. O sea, una amenaza compuesta damnifica simultáneamente múltiples áreas del sistema operacional del dispositivo infectado, dificultando lo trabajo del antivirus instalado. Este tipo de amenaza no requiere ninguna intervención humana para ser propagada y la naturaleza nociva combinada a la habilidad de rápida propagación hace de ella la peor amenaza digital que existe hoy.

Otros tipos de virus

Que simplemente utilizan redes o dispositivos informáticos serían:

- Ciberacoso
- Fraude y suplantación de identidad
- Estafas de phishing y Guerras de información

Ciberacoso

Amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación, es decir: Internet, telefonía móvil, videoconsolas online, etc.[14]

Fraude y suplantación de identidad

El "phishing" es una modalidad cuyo objetivo es la estafa por medio de la obtención de información de un usuario como son: datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Luego con estos datos utilizarlos de forma fraudulenta.

El phishing puede producirse de varias formas, desde un simple mensaje al teléfono móvil, una llamada telefónica, una web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico.

Pueden existir más formatos pero en estos momentos solo mencionan las más comunes:

- SMS (mensaje corto); La recepción de un mensaje donde le solicitan los datos personales.

- Llamada telefónica; Pueden recibir una llamada telefónica en la que el emisor suplanta a una entidad privada o pública para que usted le facilite datos privados.

  Un ejemplo claro es el producido estos días con la Agencia Tributaria, ésta advirtió de que algunas personas están llamando en su nombre a los contribuyentes para pedirles datos, como su cuenta corriente, que luego utilizan para hacerles cargos monetarios.

- Página web o ventana emergente; es muy clásica y bastante usada. En ella se simula suplantando visualmente la imagen de una entidad oficial, empresas, etc pareciendo ser las oficiales. El objeto principal es que el usuario facilite los datos privados.

  La más empleada es la "imitación" de páginas web de bancos, siendo el parecido casi idéntico pero no oficial. Tampoco olviden los sitios web falsos con señuelos llamativos, en los cuales se ofrecen ofertas irreales y donde el usuario novel facilita todos los datos, un ejemplo fue el descubierto por la Asociación de Internautas y denunciado a las fuerzas del Estado: Web-Trampa de recargas de móviles creada para robar datos bancarios.[15]

En Latinoamérica, hubo un incremento de 135% en el número de fraudes en línea y 80% de los casos de fraude del 2008 fueron mediante phishing.[16]

Se puede resumir de forma fácil, engañando al posible estafado, "suplantando la imagen de una empresa o entidad pública", de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.

Programas maliciosos para Móviles

Algunos de los virus más conocidos son: Spyeye y Zeus (también conocidos como Spitmo y Zitmo) atacan a los usuarios que visitan los sitios web configurados por los creadores del malware, los

[14] Aftab Parry. Guía práctica sobre Ciberbullying. Disponible en: http://www.ciberacoso.net/definicion.html

[15] Luque Guerrero José María, Comisión de seguridad en la red. Disponible en: http://seguridad.internautas.org

[16] Ciberdelincuencia en Ecuador, avanza sin parar, 2014. Disponible en:http://www.itecuador.com/2009/09/ciberdelincuencia-en-ecuador-avanza-sin-parar/

patrocinadores o los socios. Si el usuario que visita el sitio malicioso utiliza un navegador web de Windows, el sitio pone en marcha la versión para Windows del malware. Si el usuario visita un sitio web malicioso desde un navegador para móviles, el malware pone en marcha las versiones para móviles de Zeus o Spyeye.[17]

Spyeye

Es una nueva versión de un caballo de Troya el cual no sólo le roba el dinero, a continuación, ofrece una falsa confianza que todavía está allí.

Cuando vea el estado de cuenta de su banco en línea no habrá rastro de las transacciones que los ciberdelincuentes están utilizando para vaciar su cuenta bancaria. Lo más grave es que en su pantalla usted no podrá darse cuenta de nada y estará bien confiado de que todo está bien.

La base de todo esto es que los ladrones tengan más tiempo para usar los datos de la tarjeta de débito en transacciones fraudulentas sin que lo sepan. La próxima vez que la víctima visita el sitio de banca en línea, el programa malicioso oculta las transacciones fraudulentas y le muestra un balance del estado de cuenta falso. La nueva versión de SpyEye está dirigido a los bancos en los EE.UU. y el Reino Unido.

Zeus[18]

Se trata del malware Zeus, uno de los troyanos más peligrosos. Cuando Zeus infecta una máquina, se mantiene latente hasta que accede a la cuenta bancaria de la víctima, entonces roba las contraseñas y los datos de acceso. Tras descubrirse el año pasado que se valía de Facebook para infectar ordenadores, ahora el virus ataca usando la aplicación WhatsApp.

Estos virus son capaces de ingresar al celular con el solo hecho de recibirlos en el mismo, otras de las variantes de estos virus es que pueden ser por SMS promocionando tarifas o promociones especiales o diciendo que los mensajes son ilimitados y de manera gratuita para que los instalen, cuando en realidad son programas maliciosos que están recopilando la información para poder enviarlas a un servidor en la red para que la personas que los creo reciba esta información.

El virus Zeus, uno de los troyanos más peligrosos, aunque es antiguo todavía se propaga a través de la red. Cuando Zeus infecta una máquina, se mantiene latente hasta que accede a la cuenta bancaria de la víctima, entonces roba las contraseñas y los datos de acceso. Ahora ha regresado con una nueva estrategia: utiliza Facebook para infectar ordenadores, según la página Techspot.com. El virus provoca que el ordenador del usuario no se apague una vez activado.

Según algunos informes, el virus se adjunta en enlaces falsos de Facebook y cuando se entra en el vínculo, el usuario es re direccionado a una página pidiendo que se descargue un software común. Tras ser descargado el virus se activa. A partir de ese momento, cada vez que un usuario acceda a las cuentas bancarias, está en peligro. Zeus, también conocido como ZBOT, es tan poderoso que puede incluso sustituir a la página principal de la institución financiera con el fin de engañar a la gente para que entregue los datos.

Las cuentas de correo electrónico

Con las cuentas de email hay que tener un gran cuidado debido a que pueden llegarnos emails de diferentes personas que no se los conoce, pero debido a que en esta época casi toda la mayoría de información se envía y se recibe por email, muchos llegan a pensar que todo lo que les llega al correo deben abrirlo o son de personas que quizás conozcan. Es muy importante que las contraseñas que usen contengan letras en mayúsculas, números, caracteres especiales y combinarlos, además no es recomendable que pongan un nombre o fecha conocida por que existen programas que utilizan los nombres comunes y fechas para poder accesar.

[17] SOPHOS, Cuando el malware llega a los dispositivos móviles, Disponible en: http://www.sophos.com/es-es/company.aspx

[18] RT. Zeus, el virus que roba información personal y bancaria, 'asalta' WhatsApp. Disponible en: http://actualidad.rt.com/ciencias/view/117303-zeus-virus-roba-informacion-bancaria-whatsapp

Por eso se habrá dado cuenta que en algunas instituciones financieras les ponen un máximo de 3 intentos y de ahí se bloquea la cuenta en otros se bloquea la cuenta hasta que hable con ellos.

En las cuentas de correo electrónico le piden que ingrese un correo alterno o número de teléfono para enviar la clave en caso de que se olvide, actualmente les piden que usen de 3 a 5 preguntas secretas para validar que usted es el usuario de esa cuenta.

Prácticas que te permitirá mantener la seguridad de tu cuenta de email.[19]

1. Si te llegan mails de remitentes desconocidos con archivos adjuntos, no los abras.

2. No hagas clic en los links que vienen en los correos de remitentes que no conoces

3. No des información confidencial: Los bancos generalmente no piden a los clientes datos privados por email por lo que si recibes uno que te solicita información confidencial, duda.

4. Habilita el filtro anti-spam

5. Créate diferentes cuentas de correo electrónico: De esta forma, en una de ellas podrás recibir promociones y otras informaciones de baja importancia y reservar otra para los mails más relevantes.

6. Usa contraseñas seguras: Para garantizar la seguridad de la misma debes incluir mayúsculas, minúsculas, números y ser mayor a los diez caracteres.

7. No accedas a tu cuenta desde equipos públicos

8. Ten cuidado a la hora de usar redes públicas de Wi-Fi: Puede haber alguien que esté queriendo descifrar tu contraseña.

9. Utiliza la opción de copia oculta:Será bueno que la uses cuando debas enviar un mismo material a varios destinatarios y para que no queden visibles las direcciones.

10. Infórmate sobre seguridad informática

Spam

Se llama spam o correo basura a los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestosos.

Todos aquellos que tienen una dirección de correo electrónico que se recibe a diario varios mensajes donde aprecen anuncios y propagandas que no se han solicitado sobre cosas que no son importantes. Actualmente, se calcula que entre el 60 y el 80% de los mails (varios miles de millones de mails por día) que se envían son no solicitados, es decir, spam.

Por lo general, las direcciones son robadas, compradas, recolectadas en la web o tomadas de cadenas de mail. Aunque hay algunos spammers que envían solamente un mensaje, también hay muchos que bombardean todas las semanas con el mismo mensaje que nadie lee.

La mayoría de las veces si uno contesta el mail pidiendo ser removido de la lista, lo único que hace es confirmar que la dirección existe. Por lo tanto, es conveniente no responder nunca a un mensaje no solicitado.

Se recomienda nunca hacer caso a los correos no deseados o que llegan con publicidad, simplemente elimínelos. Si usted visita las webs que se publicitan por spam estaría ayudando a los que spammers (los que distribuyen spam).

[19] Eset. Decálogo de buenas prácticas que te permitirá mantener la seguridad de tu cuenta de email. Disponible en: http://www.muyinteresante.es/

En algunas ocasiones también entran a la bandeja de spam de los correos electrónicos, ciertos email de algunas personas dependiendo si han sido enviados con demasiadas imágenes, también los de las tarjetas de crédito o de la institución financiera que debido a la modernización los estados de cuenta son digitales, debe revisar con precaución esta bandeja y eliminar los que no conozca.

Las Redes Sociales

Navegar en una red social no va a infectarme, lo que sucede es que los nuevos virus diseñados por los hackers maliciosos o por crackers utilizan diferentes técnicas para llegar a un ordenador y hay personas que por el hecho de tener una red social aceptan a todos los que le manden una solicitud deben cuidarse y seleccionar muy bien que aceptan o no.

Además deben configurar las cuentas para que tengan cierto tipo de seguridad un ejemplo es que las fotos o información la pueda ver todo mundo o que la puedan ver los amigos de los amigos es así como se deja una puerta abierta por donde alguna persona mal intencionada intente ingresar a su cuenta y tal vez en algún momento usted lo permita sin darse cuenta.

En estos momentos la ingeniería social en redes sociales es una técnica utilizada por muchos hackers malintencionados que pretenden averiguar los datos personales de todas las cuentas, sobre todo la contraseña, conociendo al máximo la información personal y utilizando la confianza que genera una "cuenta amiga".

El caso más común lo componen aquellos mensajes que se recibe de contactos asegurando de que se puedan hacer cosas como "averiguar quién los han excluido del messenger o de Facebook", ganar dinero de alguna manera, entrar en el sorteo de iPods o iPhones... o incluso aquellos mensajes que aseguran que tienen una foto nuestra.[15]

Uno de los virus de redes sociales: KoobFace[20]

Es un "gusano" que posee un radio de ataque muy amplio y que tiene diversas variantes para atacar en muchas redes sociales como por ejemplo: Facebook, MySpace, Twitter, Hi5, Bebo, myYearBook, NetLog, Fubar y Tagged.

Un usuario normal puede utilizar las primeras tres o cuatro y, en ellas, la mayoría utiliza las mismas claves o incluso también en el e-mail. KoobFace integra al ordenador en un “ejército” de ordenadores conectados a la red, que le permiten al desarrollador del virus enviar spam a todos ellos, enviar e-mails, entre muchas otras acciones más.

Actualmente lo único asegurado sobre este virus es que ataca de la forma que se mencionó y que se auto-envía a todos los contactos mediante la misma forma que lo infectaron.

Estos son los nombres con los que hasta el día de hoy puede conocerse:

- Net-Worm.Win32.Koobface.a (ataca MySpace).
- Net-Worm.Win32.Koobface.b (ataca Facebook).
- WORM_KOOBFACE.DC (ataca Twitter).
- W32/Koobfa-Gen (ataca Facebook, MySpace, Twitter, Hi5, Bebo, myYearBook, NetLog, Fubar y Tagged).

Es necesaria la colaboración de los usuarios es fundamental, ya que si todos colaboran será más fácil detectar estas prácticas y bloquearlas antes de que miles de usuarios se contagien, algo rápido y con tiempo suficiente hasta que la red social lo detecte por sí sola en muchos casos.

[20] Cosmomedia. Virus en redes sociales: consejos para prevenir infecciones o desinfectar nuestro perfil. Disponible en:http://www.cosmomedia.es/seguridad-informatica/466-virus-en-redes-sociales-consejos-para-prevenir-infecciones-o-desinfectar-nuestro-perfil.html

¿Cómo prevenir una infección de virus en las redes sociales?[15]

Es un error abrir mensaje de contactos que se conocen y que están escritos en inglés, a pesar de que la persona habla en español: quizás ni el amigo/a sabe que ese mensaje ha sido enviado, así que por favor, no abrir mensajes sospechosos.

Ante la duda no hay nada mejor que preguntarle a la persona misma si ese mail lo ha enviado el mismo. Si no se confía en el mensaje que les ha llegado, mejor no abrirlo. Lo mismo ocurre para los programas: si no se confía en el programa lo mejor es que no lo instalen.

Para eliminar los virus de redes sociales que ya han llegado al equipo ante todo se debe actualizar el antivirus, una vez hecho esto se debe escanear completamente todas las unidades y utilizar alguna herramienta de limpieza para eliminar los datos temporales, cookies, carpetas temporales de Windows.

Recomendaciones contra los ciberdelincuentes

Se debe tratar de verificar que la pagina donde se conecte tenga las protecciones debida antes de ingresar datos personales o datos que tengan cuentas financieras, como medio de protección no solo hay que usar un simple antivirus o un programa de seguridad de internet (Internet Security), debe usarse un conjunto de diferentes tipos de herramientas de seguridad, como malware o aplicaciones que protegen las contraseñas que se utilizan, además tiene que borrar de los navegadores que utiliza las contraseñas y paginas recientes de navegación.

En estos momentos los celulares han ganado un gran mercado debido a que tienen la capacidad de navegar por la internet solo que la mayoría jamás borra el historial de navegación, además cuando ingresan las claves le pregunta si quiere guardar la contraseña y muchas veces le ponen que sí, de esta forma si alguien llega a tener acceso a este celular pueden accesar a las cuentas que el equipo tenga almacenado.

En la actualidad muchas de las personas están acostumbrados a recibir múltiples mensajes por medio del celular desde un correo electrónico, mensajes de texto y mensajes multimimedias, algunas veces los mensajes que llegan son información de propagandas e información que no tiene relevancia alguna para determinadas personas.

Dentro de los emails pueden también escondidos algunos virus que pueden dar acceso a su información a otras personas.

Por ello es recomendable solo abrir email de personas conocidas, además jamás de información a nadie sobre la entidad financiera aunque le digan que necesitan solicitar la contraseña, números de tarjeta de crédito o cualquier información personal por correo electrónico, por teléfono o SMS.

Estas instituciones ya tienen los datos, en todo caso es usted el que los puede solicitar por olvido o pérdida y ellos se lo facilitarán.

Cuando se visiten sitios Web, teclee la dirección URL en la barra de direcciones del navegador, aunque algunas instituciones financieras cuando ustedes accesan a las páginas le recomiendan que navegador deberían usar, jamás por enlaces procedentes de cualquier sitio.

Las entidades bancarias contienen certificados de seguridad y cifrados seguros, algunas instituciones le proveen un servicio de protección en el momento de ingresar claves.

Recomendación al momento de ingresar datos para una compra por internet revisar que tengan las seguridades correspondientes y que sea confiable la página, también para evitar problemas en algunas páginas le piden que ponga la dirección, teléfono.

Pero de los datos que están registrados en la tarjeta, algunos cometen el error de poner la dirección donde se encuentran en ese momento y no la dirección que pusieron cuando saco la tarjeta y que todavía este en vigencia.

No aceptar mensajes o archivos de desconocidos, sobre todo enviados a través de Bluetooth.

Desactivar el Bluetooth cuando no lo use. Por defecto está activado puede correr riesgos alguien se podría conectar al teléfono y obtener algún tipo de información importante.

Debería bajar aplicaciones para proteger las fotos o archivos a los cuales solo ingresara con clave.

No realice transacciones, ni consultas privadas desde el móvil en redes de WIFI públicas.

3. CONCLUSIONES

La ciberdelincuencia es un gran problema en esta época moderna, donde el medio más rápido para hacer compras ya sea dentro o fuera del país, es por medio de una transacción digital o el uso de tarjetas es recomendable tomar siempre las precauciones pertinentes para evitar algún transacción no autorizada.

Muchas veces las personas por desconocimiento creen que por que una página esta en internet es segura y no hay problema cuando en realidad esto no es así, hay que ver bien dónde y cómo se ingresan los datos porque hay virus que permiten ver la página tal cual como la original solo que no es así, lo que hace este virus es hacer creer que se cayó la señal emulando lo que en algunas veces a la mayoría de las personas les pasa, es ahí donde deben tener mucho cuidado al ingresar los datos personales porque la información puede ser enviada a otra persona en cualquier lugar del mundo.

Hasta los mensajes de texto pueden contener algún tipo de virus, los virus también pueden afectar a un celular pero muchos creen que solo los virus son para las computadoras. Los principales métodos para obtener dinero de los usuarios desprevenidos: programas maliciosos bancarios y estafas a través de mensajes SMS de tarifas especiales.

La información es muy importante, debe protegerla usando aplicaciones que existen en el mercado o debe tener cuidado como, donde y cuando se brinda información podrían resultar siendo víctimas de este delito.

4. Referencias Bibliográficas

Definición de tic - Qué es, Significado y Concepto. Disponible en: http://definicion.de/tic/#ixzz3DhgOUJmh.

Definición de Sociedad, 2011. Disponible en http://definicion.mx/sociedad/

Delincuencia organizada, Disponible en: http://www.interpol.int/es/Criminalidad/Delincuencia-organizada/Delincuencia-organizada

Concepto de seguridad, Definición, Significado y Qué es, Disponible en: http://definicion.de/seguridad/#ixzz3DhsaxL59

Ángel Fire. ¿Qué es un virus? Disponible en: http://www.angelfire.com/dragon2/ilovebsb/pagina7.html

Expresión Binaria. Ingeniería Social. Disponible en: http://www.expresionbinaria.com/glosario/ingenieria-social/

Informe de Cibercrimen de Norton 2011. Disponible en: http://www.computerworldmexico.mx/Articulos/18883.htm

Ciberdelincuencia: ¿qué es?, Disponible en: http://www.bullguard.com/es/bullguard-security-center/internet-security/security-tips/cybercrime.aspx

Informe de Cibercrimen de Norton 2011. Disponible en: http://www.computerworldmexico.mx/Articulos/18883.htm

Eduteca. ¿Qué es el malware?. Disponible en: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=193

Alegsa. Definición de Ataque de denegación de servicio Disponible en: http://www.alegsa.com.ar/Dic/ataque%20de%20denegacion%20de%20servicio.php#sthash.WPBkYLE0.dpuf

Techtarget. Ataque de denegación de servicio (DDoS). Disponible en: http://searchdatacenter.techtarget.com/es/definicion/Ataque-de-denegacion-de-servicio

Psafe. ¿Cuáles son los tipos de virus que existen? Disponible en: http://www.psafe.com/ayuda/cuales-son-los-tipos-de-virus-que-existen/

Aftab Parry. Guía práctica sobre Ciberbullying. Disponible en: http://www.ciberacoso.net/definicion.html

Luque Guerrero José María, Comisión de seguridad en la red. Disponible en: http://seguridad.internautas.org

Ciberdelincuencia en Ecuador, avanza sin parar, 2014. Disponible en:http://www.itecuador.com/2009/09/ciberdelincuencia-en-ecuador-avanza-sin-parar/

Sophos, Cuando el malware llega a los dispositivos móviles, Disponible en: http://www.sophos.com/es-es/company.aspx

RT. Zeus, el virus que roba información personal y bancaria, 'asalta' WhatsApp. Disponible en: http://actualidad.rt.com/ciencias/view/117303-zeus-virus-roba-informacion-bancaria-whatsapp

Eset. Decálogo de buenas prácticas que te permitirá mantener la seguridad de tu cuenta de email. Disponible en: http://www.muyinteresante.es/

Cosmomedia. Virus en redes sociales: consejos para prevenir infecciones o desinfectar nuestro perfil. Disponible en:http://www.cosmomedia.es/seguridad-informatica/466-virus-en-redes-sociales-consejos-para-prevenir-infecciones-o-desinfectar-nuestro-perfil.html