NEWSLETTER – INFOSEC MX

BOLETIN No. 40

Noviembre 19- 27

Elaboración: Noviembre 28, 2016

Ataca virus por Facebook Messenger

por NOVIEMBRE 24, 2016 / EL UNIVERSAL

Según PSafe Total, llega por medio de un mensaje de un contacto donde se invita al usuario a ver un video que contiene la imagen de un conocido, al dar clic, la víctima es redireccionada a un sitio de videos donde se le pide la descarga e instalación de un archivo zip. Ya instalado, el hacker tendrá acceso a los datos que se ingresan en el teclado, historial de internet incluidas las transacciones bancarias.

Se recomienda desinstalar la aplicación, cambiar la contraseña y descargar el antivirus PSafe Total, que además de realizar pruebas de antivirus regulares, ayuda a mantener el dispositivo optimizado para un mejor funcionamiento y entonces reinstalar Facebook, esto es porque cada vez que una aplicación se descarga, indicará si es segura o no, y evitará que éstas sirvan como medio de infección ya que siempre emitirá una alerta de lo que se está descargando.

Fuente:
http://www.eluniversal.com.mx/articulo/techbit/2016/11/24/ataca-virus-por-facebook-messenger

Google: Usuarios tienen que saber distinguir las noticias falsas

por NOVIEMBRE 23, 2016 / EXCELSIOR

Miguel Alva, director de Marketing para Latinoamérica de Google, dijo que son los propios usuarios los que tienen que aprender a discernir entre noticias veraces y falsas, Google se ha esforzado desde el inicio que el Internet sea democrático, habiendo contenido de todo tipo. La publicación de noticias falsas es parte del dinamismo del mercado y hay que dejar que el usuario sea quien decida y quien descarte el contenido.

La pasada campaña electoral estadunidense, donde salió vencedor Donald Trump, estuvo marcada por publicaciones de noticias falsas en redes sociales y buscadores. Una investigación de Buzzfeed encontró que las 20 noticias falsas más populares de los últimos tres meses obtuvieron más de un millón de interacciones más en Facebook que las principales historias de medios como The New York Times, The Wall Street Journal o CNN. Un segmento de la opinión culpa a Facebook de estos resultados electorales por haber permitido la publicación de bulos informativos ha influido en los electores.

Fuente:
http://www.excelsior.com.mx/hacker/2016/11/23/1129786

¡Cuidado! Este video deja inservible a tu iPhone

por NOVIEMBRE 23, 2016 / EXCELSIOR

Circula un video en redes sociales que dura cinco segundos y quien lo reproduce en su iPhone o iPad obliga a reiniciar el dispositivo ya que queda inservible. Lo alarmante, es que este video hace lento al sistema operativo hasta dejarlo inútil. Por lo que la víctima tendría que forzar el reset del iPhone pulsando prolongadamente los botones de bloqueo e inicio.

El video es un .MP4 que pesa aproximadamente 500 KB y está alojado en VK. Se puede compartir con un enlace a través de cualquier red social o hasta por mensajes y se desconoce si este archivo es un virus o qué cause este problema, en algunos blogs comentan que podría tratarse de un archivo corrupto que afecta a Safari.

Fuente: **http://www.excelsior.com.mx/hacker/2016/11/23/1129912**

Facebook crea software censurador para entrar en mercado chino

por NOVIEMBRE 23, 2016 / EL UNIVERSAL

No está siendo usado ni se ha ofrecido a las autoridades chinas. Este software impide que aparezcan ciertos contenidos en regiones geográficas determinadas, según fuentes que son empleados y ex empleados de Facebook. El objetivo de esta empresa no es censurar los contenidos por sí mismo, sino permitir a las autoridades chinas o a un eventual socio en China eliminar determinados temas o posts. Hay que recordar que China bloquea las redes sociales como Facebook, Twitter, YouTube o webs que critican la política de Pekín.

El programa solamente es una idea debatida para tener acceso a China. Algunas de las fuentes del diario están preocupadas porque este software resulte interesante para las autoridades en Estados Unidos tras la victoria de Donald Trump. Facebook ha limitado contenidos con base a leyes locales en Turquía, Pakistán o Rusia. En Alemania se eliminan contenidos como cruces gamadas o páginas en las que se niega el Holocausto.

Fuente:
http://www.eluniversal.com.mx/articulo/techbit/2016/11/23/facebook-crea-software-censurador-para-entrar-en-mercado-chino

Los hackers también pueden robar huellas dactilares

por NOVIEMBRE 22, 2016 / EXCELSIOR

Según Anil Jain, ningún sistema de seguridad es perfecto. A medida que bajan los precios y aumentan las capacidades de los sensores electrónicos y los microprocesadores, las empresas fabricantes de aparatos electrónicos empezaron a incorporar sistemas biométricos a sus productos. La investigadora demostró que es posible penetrar un teléfono que requiere las huellas dactilares para activarse, a pedido de la policía, Jain y dos colegas hicieron copias digitales de las huellas de un individuo que había muerto, las agrandaron y las imprimieron con una tinta especial que reproduce las propiedades conductivas de la piel humana.

Por otro lado, investigadores de la Universidad de North Carolina burlaron sistemas de reconocimiento de rostros usando fotos que encontraron en redes sociales y crearon imágenes tridimensionales empleando algoritmos de realidad virtual. No siempre funcionaron las imágenes, especialmente con aparatos que usan rayos infrarrojos. Expertos están preocupados de que los sistemas biométricos afecten derechos legales.

Fuente:
http://www.excelsior.com.mx/hacker/2016/11/22/1129750

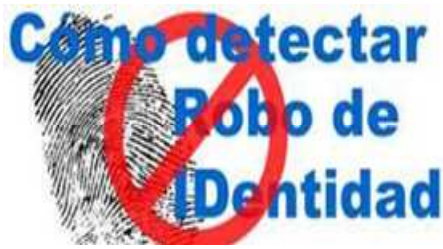
Buró de Crédito va contra el robo de identidad

por NOVIEMBRE 23, 2016 / EL ECONOMISTA

De acuerdo con la Condusef, en los primeros seis meses del 2016, se han reportado más de 32,000 casos de robos de identidad en productos bancarios. Por lo que el Buró de Crédito trabaja en herramientas de alertas, para avisar al usuario de servicios financieros desde el momento en que se consulta su historial, ya que podría ser un indicativo de intento de fraude. Las alertas son dos: Una de servicio gratuito con el que las personas reciben por correo electrónico un aviso de cualquier consulta o cambio en la información de su historial crediticio, detectando cualquier intento de robo de identidad, y otro denominado Alértame, que hace los mismo, pero con el plus de cuatro reportes con información del Buró con un costo de $232 pesos anuales.

Mauricio Gamboa director general de la sociedad de información crediticia, explicó que el Buró de Crédito ya trabaja también con la herramienta llamada Vigilante, la cual procesa cada solicitud de financiamiento a través de modelos matemáticos, realiza comparaciones, combina datos históricos considerando puntuaciones de scores de fraude, y analiza el comportamiento y la actividad delictiva conocida, alertando a las instituciones de crédito.

Fuente: **http://eleconomista.com.mx/finanzas-publicas/2016/11/23/buro-credito-va-contra-robo-identidad**



Boletín No. 2619. Conocen diputados dictamen sobre Usurpación de Identidad

por NOVIEMBRE 24, 2016 / CAMARA DE DIPUTADOS LXIII LEGISLATURA

El pleno de la Cámara de Diputados informó para trámite de publicidad el dictamen para castigar el delito de robo de identidad, que será votado en la próxima sesión, planta la adición del Artículo 430 al Código Penal Federal, para incluir un capítulo en materia de usurpación de identidad. "Se establece que comete este delito, el que por sí o por interpósita persona, usando cualquier medio lícito o ilícito, se apodere, apropie, transfiera, utilice o disponga de datos personales sin autorización de su titular o bien suplante la identidad de una persona, con la finalidad de cometer un ilícito o favorecer su comisión".

"Plantea imponer una pena de uno a seis años de prisión y de 400 a 600 días multa por el delito y, en su caso, la reparación del daño que se hubiera causado a los afectados. Las penas aumentarán hasta en una mitad, cuando el ilícito sea cometido por servidor público que, aprovechándose de sus funciones, tenga acceso a bases de datos o por quien se valga de su profesión para ello".

Fuente
http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Boletines/2016/Noviembre/24/2619-Conocen-diputados-dictamen-sobre-usurpacion-de-identidad

El 69.7% de datos en la nube están en un "limbo legal" sobre su propiedad

por NOVIEMBRE 17, 2016 / SILICON

La firma Skyhigh Networks ha estudiado el uso de datos en la nube de 30 millones de usuarios, y destaca que el 69.7% de las aplicaciones que gestionan datos de usuarios en la nube analizadas, no especifican quien es el dueño de esos datos una vez que son subidos por los usuarios. Implicando que muchos datos quedan en un 'limbo legal', algo que puede ser peligroso para las empresas entrando en vigor la nueva ley de protección de datos de la Unión Europea.

Asimismo, solo el 8.7% no compartirán con terceros los datos subidos por sus clientes, el 16% indica que borran todos los datos cuando finaliza el contrato con sus usuarios. En cuanto al bloqueo de las empresas a contenidos que se intentan subir a internet en sus redes, las conclusiones son: En el caso de los contenidos subidos a Instagram, a pesar de que las empresas estiman que logran bloquear el 43.7% de ellos, la realidad es que apenas consiguen hacerlo con el 6.4%. Si se trata de Facebook, tampoco tienen la eficacia de bloqueo que creen (63% contra 28.8% real), y Twitter es menor con (30.8% contra 12.6% real).

Fuente: **http://www.silicon.es/697-ciento-datos-la-nube-estan-limbo-legal-propiedad-2323262?utm_content=bufferfd9df&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Los ataques DDoS de más de 100 Gbps han aumentado un 138%

por NOVIEMBRE 18, 2016 / SILICON

El informe de Akamai sobre seguridad del tercer trimestre de 2016, comprueba que los ataques DDoS de más de 100 Gbps se han disparado, han crecido un 138% interanual. Además, habla de "dos ataques DDoS récord", ambos favorecidos por la botnet Mirai. Son los ataques DDoS más grandes con los que esta compañía se ha topado hasta ahora, con 555 Gbps y 623 Gbps, respectivamente. Los ataques DDoS han crecido 71% durante el tercer trimestre respecto al mismo periodo de 2015, pero no todas las amenazas lo han hecho por igual. Mientras los ataques a aplicaciones web han caído 18%, los de reflexión de DNS y de fragmentos de UDP se están generalizando, han crecido 4.5% y aglutinan ya un 44% de los vectores.

Martin McKeay, editor senior del informe dice que "La botnet Mirai" también ha puesto de manifiesto la realidad del temor imperante en el sector de que el Internet de las Cosas y otros dispositivos conectados a internet pueden constituir el medio para lanzar ataques DDoS y a aplicaciones web, así como la necesidad de que los fabricantes de dispositivos hagan mayor hincapié en la seguridad.

Fuente: **http://www.silicon.es/ataques-ddos-mas-100-gbps-han-aumentado-2323333?utm_content=buffer63190&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

Circula en WhatsApp y redes sociales mensaje falso de CFE

por NOVIEMBRE 16, 2016 / NETMEDIA

La Comisión Federal de Electricidad (CFE) alertó a los usuarios sobre mensajes apócrifos distribuidos a través de WhatsApp y redes sociales como Facebook y Twitter. Indicó que a través de un mensaje titulado "I.M.P.O.R.T.A.N.T.E" se invita a los usuarios de la CFE a oponerse al programa de sustitución de medidores. Al ingresar a la página www.monederocfe.com los usuarios se convierten en víctimas de un fraude cibernético.

La CFE señaló que es falso que estos medidores estén vinculados a cualquier programa de "Monedero CFE", y subrayó que dicho programa no existe en la empresa. Detalló que el programa de sustitución de medidores que impulsa es totalmente gratuito y tiene como objetivo modernizar los equipos de medición actuales por equipos electrónicos digitales. Por lo que ya interpuso las demandas correspondientes a la división de delitos cibernéticos de la Procuraduría General de la República (PGR).

Fuente: **http://www.netmedia.mx/b-secure/circula-en-whatsapp-y-redes-sociales-mensaje-falso-de-cfe/?utm_content=buffer73296&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer**

¡Alerta! Gmail podría sufrir un ciberataque respaldados por el gobierno

por NOVIEMBRE 24, 2016 / NOVENTA GRADOS

Usuarios de Twitter alertan sobre un supuesto ataque en sus cuentas de correo electrónico Gmail, donde les advierte que hackers respaldados por el gobierno están tratando de acceder a su cuenta. Google ha advertido a sus usuarios sobre estos ataques desde el 2012, en marzo, la compañía lanzó una página completa de advertencia, pero no especifica qué gobierno puede estar detrás de estos ataques. Con el siguiente mensaje alertan al usuario:

"Atacantes respaldados por el gobierno pueden estar tratando de robar tu contraseña. Existe la posibilidad que esto sea una falsa alarma, pero nosotros creemos que hemos detectado atacantes respaldados por el gobierno que están tratando de robar tu contraseña. Esto le pasa a menos del 0.1% de los usuarios de Gmail. No podemos revelar cómo nos dimos cuenta, porque esa información les serviría a los hackers para que cambien sus tácticas, pero si tienen éxito en algún punto ellos podrán accesar a su información o emprender otras acciones usando su cuenta. Para mejorar su seguridad, basado en su configuración actual nosotros recomendamos: Configurar una clave de seguridad o instalar una alerta de contraseña".

Fuente:
http://www.noventagrados.com.mx/tecnologia/alerta!-gmail-podria-sufrir-un-ciberataque-respaldados-por-el-gobierno.htm

Robo de identidad crece en México hasta 500 %; Chiapas reporta 325 en 2016

por NOVIEMBRE 24, 2016 / MERIDIANO POLITICO

Desde el 2011 a la fecha se han incrementado hasta en un 500% el robo de identidad en México; en Chiapas a finales del 2016 se estarían reportando cerca de 325 casos de esa índole. En México el 37% de estos casos ocurre a través del robo de carteras; el 33% por la pérdida de documentos oficiales y un 30% por la clonación de tarjetas bancarias, afirmó Miguel Ángel Marina Moreno, experto financiero.

Uno de los métodos más usados para conseguir los datos de una persona es el Dumpster Divingo o el buceo de basurero, que debido a la mala costumbre de desechar casi intactos los recibos o estados de cuenta, hace que cualquiera que inspecciona en la basura pueda encontrar algún documento con los datos. Se recomienda nunca perder de las tarjetas bancarias para evitar que estas sean clonadas; romper vouchers o estados de cuenta cuando estos sean desechados y asegurarse de que, al sacar copias de documentos oficiales, se saquen las que se necesiten evitando que el establecimiento se quede con alguno.

Fuente: **http://www.meridianopolitico.com/2016/11/robo-de-identidad-crece-en-mexico-hasta.html**

Cámaras son los dispositivos del IoT más peligrosos para las empresas

por NOVIEMBRE 18, 2016 / SEGURIDAD UNAM

Zscaler dice que las cámaras de seguridad en red son las que tienen más probabilidades de tener vulnerabilidades cuando se trata de proteger los dispositivos de Internet de las Cosas en la empresa. Por ejemplo, en la cámara de monitorización inalámbrica HD Flir FX, los investigadores encontraron que esta se comunicaba con la empresa matriz en texto plano y sin autenticación, el firmware que se estaba actualizando no estaba firmado digitalmente, por lo que los atacantes pueden introducir su propio firmware malicioso.

La cámara IP de Foscam, se conecta a un servidor web para transmitir video a los escritorios o teléfonos de los usuarios, pero las credenciales de usuario se transmiten en texto sin formato, a través de HTTP, directamente en la URL. Una cámara infectada puede hacer aún más daño, ya que los ciberdelincuentes podrán ver cuando las áreas en particular no están protegidas, para planificar ataques físicos o cibernéticos. Zscaler sugirió que las empresas restringieran el acceso a los dispositivos IoT tanto como fuera posible, bloqueando puertos externos o utilizar dispositivos de filtrado en redes aisladas, para evitar movimientos laterales. Cambiar las credenciales predeterminadas, y configurar un proceso para aplicar actualizaciones periódicas de seguridad y firmware.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3099&utm_content=buffera7f13&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Ransoc chantajea a víctimas con browser locker/ransomware

por NOVIEMBRE 18, 2016 / SEGURIDAD UNAM

Este malware apunta a usuarios que visitan sitios para adultos, y es distribuido vía malvertising afectando a usuarios Windows. Sin cifrar los archivos del usuario, amenaza con dañar la reputación del usuario. Cuando se ejecuta en el ordenador de la víctima, escanea nombres de archivos multimedia en busca de cadenas asociadas a pornografía infantil y archivos descargados vía torrent y corre múltiples rutinas para obtener información de las cuentas de Facebook, LinkedIn y Skype del usuario. Esta información es usada para personalizar un falso "aviso de penalidad" que es mostrado a la víctima y amenaza con exponer sus faltas con los derechos de propiedad intelectual y su sospechosa actividad en línea si no paga la multa, además es usada para chantajear de que todos en sus círculos profesionales y sociales podrían terminar escuchando acerca de ello.

Así mismo, el mensaje dice que el dinero que pague la víctima les será devuelto si no son atrapados de nuevo en los próximos 180 días. El pago se haría mediante tarjeta de crédito, mostrando que el delincuente está confiado de que el usuario no denunciará a las autoridades ya que tiene algo que ocultar. Este falso aviso aparece en una ventana en pantalla completa evitando que las víctimas puedan manipularla o accedan al sistema operativo. Ransoc detiene el proceso cada 100 milisegundos en regedit, msconfig y el taskmgr, matando los procesos antes de que la víctima pueda eliminar o deshabilitar el malware. El malware solo usa una llave de registro de autoarranque para asegurar persistencia, por lo que reiniciando la máquina en modo seguro debe permitir a los usuarios eliminar el malware.

Fuente:
http://www.seguridad.unam.mx/noticia/?noti=3098&utm_content=buffer05ab6&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

TOTALSEC NEWSLETTER – INFOSEC

BOLETÍN No. 40

Noviembre 19 - 27, 2016

Elaboración: Noviembre 28, 2016

totalsec