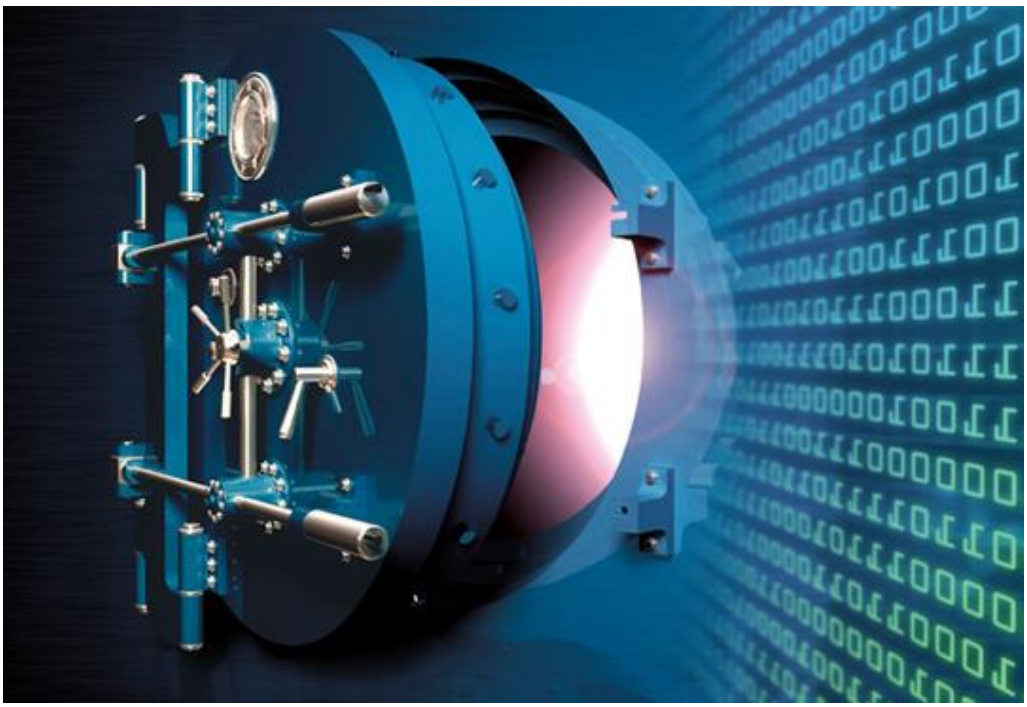

TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN No. 11

ABRIL 30 – Mayo 08

Elaboración: Mayo 09, 2016

GOBIERNO

En este número encontrarás noticias sobre:

- Gobierno
- Finanzas
- Tecnología

Legisladores piden fortalecer estrategias contra el robo de identidad

por ABRIL 14 2016 / CAMARA DE DIPUTADOS

La Comisión de Seguridad Pública de la Cámara de Diputados, aprobó el dictamen en el que se solicita a las autoridades correspondientes promover y fortalecer estrategias en contra del robo de identidad, en especial los casos de correo electrónico, redes sociales y banca electrónica.

El llamado es a Comisión Nacional de Seguridad (CNS), Bancaria y de Valores (CNBV), y para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), a las procuradurías General de la Republica (PGR), Federal del Consumidor (Profeco), y de la Defensa del Contribuyente (Prodecon).

Fuente:
http://www5.diputados.gob.mx/index.php/camara/Comunicacion/Boletines/2016/Abril/14/1329-Comision-de-Seguridad-Publica-aprueba-solicitar-a-Segob-que-refuerce-seguridad-en-penitenciarias

Policía Federal y Google México establecen alianza en materia de capacitación sobre Seguridad Digital

por MAYO 04, 2016 / EL UNIVERSAL

Comunicado de Prensa No. 308

La División Científica de la Policía Federal estableció una alianza de cooperación y capacitación con Google México para sumar acciones de prevención del delito y concientización de la ciudadanía en el uso de internet. Integrantes de la Coordinación de Delitos Cibernéticos e instituciones policiales de 11 estados de la República tomaron un curso con expertos de Google.

Se impartieron sesiones con temas relativos al uso responsable de la Red, engaños virtuales, interacción en redes sociales, seguridad de dispositivos móviles, ciudadanía digital, así como medidas preventivas para evitar daños al patrimonio, datos personales e integridad de las personas al usar Internet.

Fuente:
http://www.eluniversal.com.mx/articulo/techbit/2016/05/5/policia-federal-y-google-mexico-crean-alianza

Comunicado del IMSS sobre página web apócrifa

por ABRIL 29, 2016 / IMSS

El IMSS emitió un comunicado urgente que dice lo siguiente:

"A todos nuestros usuarios del portal IMSS DESDE SU EMPRESA (IDSE), se les informa que el día de 29 de abril del año en curso se identificó la existencia de una página web apócrifa pretendiendo suplantar dicho portal. La citada página aloja aplicaciones que contienen malware, esto es, software que tiene como objetivo dañar o extraer información de los equipos de cómputo.

Derivado de lo anterior y con la finalidad de prevenir cualquier tipo de intrusión, así como salvaguardar su información, les recordamos que la única vía de acceso al portal IDSE es http://idse.imss.gob.mx"

Fuente: **http://www.imss.gob.mx/patrones/idse**

¿Por qué la Seguridad de la Información es relevante en campañas políticas?

por MAYO 02, 2016 / WE LIVE SECURITY

Esto a raíz de los sucesos recientes como el del hacker Andrés Sepúlveda que afirmó haber participado en las últimas elecciones presidenciales alterando el curso de las campañas por medio del uso de malware, bots o ciberespionaje. Así mismo, la filtración del padrón electoral del INE con los datos de 93 millones de electores. Se le está prestando atención a las campañas políticas que están por venir, esto debido a la ausencia de medidas de protección, o el mal manejo de los datos, que puede perjudicar a todos.

La ciberseguridad debe formar parte de las estrategias de campaña de los candidatos para evitar algunos ataques como ataques publicitarios, espionaje o minimización de la participación de un adversario político, por ejemplo, comprometiendo sus cuentas. Así como la sustracción de información sensible como discursos políticos, reuniones, programas y estrategias de campaña.

Fuente: **http://www.welivesecurity.com/la-es/2016/05/02/seguridad-informacion-relevante-politicas/**

FINANZAS

Ciberataques y crudo ponen nerviosa a la banca: E&Y

por ABRIL 28, 2016 / EL FINANCIERO

Anthony Caterino, líder global de Servicios Financieros de EY e Ignacio Aldonza, socio líder del Sector Financiero de la firma en México, aseguraron que el fraude mundial es intensivo y está creciendo, los ataques a la banca están al alza, pero la industria está desarrollando prácticas para combatirlo. El robo de identidad a través del sistema financiero mexicano es un problema grave y está en ascenso, por lo que la preocupación es la evolución al mundo digital, mejorar los canales, construir arquitectura multicanal para reducir costos y ampliar la capacidad.

Además de verse amenazada por ciberataques y el robo de identidad, también está el problema de los bajos precios del petróleo que seguirán en el mediano plazo, alertó Ernst & Young (EY), la caída del precio del combustible desde el 2014, preocupa por la exposición en créditos con empresas del sector con problemas financieros, y porque los proyectos se detienen y no requieren financiamiento.

Fuente: **http://www.elfinanciero.com.mx/economia/ciber-ataques-y-crudo-ponen-nerviosa-a-la-banca-e-y.html**

Moneta ATM Guard, nuevo escudo de protección para cajeros automáticos

por ABRIL 26,2016 / PR NEWSWIRE

Moneta Technologies, informó que desarrolló en conjunto con otras instituciones financieras el sistema Moneta ATM Guard, para proteger cajeros automáticos de ataques de seguridad a través de dispositivos externos y la alteración del hardware o software del ATM, impidiendo la intromisión a los cajeros e inyectarles malware desde un dispositivo USB o CD, impedir que alguien tenga acceso a los datos de transacciones que viajan por red, además de proteger el software de las aplicaciones bancarias del propio disco duro del cajero.

México tiene más de 50,000 cajeros con sistemas legados que pueden estar expuestos; por lo que esta solución garantiza el cuidado de los cajeros ante cualquier intrusión física manteniendo un monitoreo permanente de cualquier anomalía o ataque de software o hardware.

Fuente: **http://www.prnewswire.com/news-releases/moneta-atm-guard-nuevo-escudo-de-proteccion-para-cajeros-automaticos-577150541.html**

TECNOLOGÍA

Adiós al botón de huella digital del teléfono

por MAYO 02, 2016 / EXCELSIOR

LG planea quitar el botón del sensor de huella digital en sus próximos teléfonos inteligentes. Haciendo que toda la pantalla del móvil se convirtiera en un sensor de huella digital para desbloquear el dispositivo, por lo que adelgazó 0.01 pulgadas la cubierta de cristal en la parte baja del teléfono, estando el sensor en el mismo lugar, pero lo suficientemente cerca de la superficie para leer las huellas digitales.

El sensor estaría protegido del agua y ralladuras. Hasta podría instalarse en cualquier sitio debajo de la pantalla del dispositivo. La empresa dijo que la tecnología de reconocimiento tiene una precisión similar a la que utiliza botón físico. La probabilidad de que el sensor acepte una huella errónea es del 0.002%. Aún no hay fecha de lanzamiento, pero LG ya hay pláticas con clientes para la obtención del mismo.

Fuente:
http://www.excelsior.com.mx/hacker/2016/05/02/1090121

BlackBerry invierte mil mdd para reforzar Seguridad

por ABRIL 30, 2016 / EXCELSIOR

Las empresas necesitan ocupar más recursos para mitigar riesgos de ataques por parte de los ciberdelincuentes en sus dispositivos móviles, impidiendo a los empresarios instalar oficinas móviles. Por lo que BlackBerry invirtió mil millones de dólares comprando cinco empresas dedicadas a la ciberseguridad, permitiendo así a diversas organizaciones gubernamentales o privadas transferir datos y hacer transacciones económicas libres del temor de ser atacadas.

Con la empresa SECUsmart, se pueden cifrar todas las datas, Movirtu, firma dedicada a la administración de carriers, permite tener hasta dos números telefónicos independientes en el mismo SIM y protege los datos del usuario. Con WatchDocx, se impide la fuga de información al controlar el ciclo de vida de un documento y tener control de este, sin importar si éste es compartido o fotografiado, con Good, se cifran los datos de voz evitando el espionaje telefónico. La seguridad también se enfoca a los usuarios de dispositivos, por ello se adquirió AtHoc, que permite mandar alertas masivas en caso de alguna eventualidad, ya sea mediante notificaciones o mensajes bidireccionales.

Fuente:
http://www.excelsior.com.mx/hacker/2016/04/30/1089841

Inmadurez en ciberseguridad

por ABRIL 13, 2016 / EXCELSIOR

La ciberseguridad en México se encuentra en un estado "inmaduro", ya que las empresas no invierten en sistemas de protección, hay un mayor número de víctimas y se está en el segundo lugar como el país más atacado en América Latina. Además, 27 millones de mexicanos sufrieron un ataque o robo de información en el 2015.

Agregando que al país el problema de ciberseguridad le costó el año pasado cerca de tres mil 900 millones de dólares y las empresas sólo están invirtiendo para protegerse 680 millones de dólares. Por lo que las empresas ya se están dando cuenta de los verdaderos efectos del robo de información o un ataque cibernético, ya que éstos significan gastos, pérdida de credibilidad, de reputación y de clientes.

Fuente: **http://www.excelsior.com.mx/hacker/2016/04/13/1086250**

Karspersky Lab descifra el ransomware CryptXXX

por MAYO 03, 2016 / BLOG KARSPERSKY

Kaspersky Lab, desarrolló una nueva herramienta que recupera los archivos secuestrados por CryptXXX, esto sin pagar el rescate de hasta 500 bitcoins exigido por el ransomware. Además de encriptar los archivos, el malware era capaz de navegar por el sistema buscando contraseñas y datos sensibles.

Los expertos determinaron que la encripción RSA-4096 era falsa por lo que crearon esta herramienta que es gratuita y para poder hacer la recuperación, necesitará al menos un archivo no encriptado que no haya sufrido el ataque del ransomware. Esta herramienta está disponible en la web de soporte de la compañía.

Fuente: **https://blog.kaspersky.es/cryptxxx-ransomware/8189/**

El MIT crea un sistema de IA capaz de detectar el 85% de ciberataques

por ABRIL 18, 2016 / WE LIVE SECURITY

El Computer Science and Artificial Intelligence Lab (CSAIL) del MIT, ha desarrollado un sistema llamado AI², que detectará si se están produciendo ciber-ataques, además reduce el número de falsos positivos de forma notable.

Los sistemas de seguridad operan de dos maneras: con personas, o con máquinas. La solución del MIT combina ambas operaciones y hace que los datos detectados por la máquina sean supervisados por analistas que los etiquetan y los revisan. Detectando el 85% de los ciberataques, haciendo suponer una detección tres veces mejor en comparación con otros sistemas, y reduciendo el número de falsos positivos en cinco veces. Entre más ataques sean detectados por el sistema, más información se obtendrá para mejorar la precisión de las predicciones siguientes.

Fuente: **http://www.welivesecurity.com/la-es/2016/04/19/inteligencia-artificial-predecir-ciberataques/**

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No. 11

30 ABRIL – 08 MAYO, 2016

Elaboración: MAYO 09, 2016.