TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN 6

MARZO 26 – ABRIL 03

Elaboración: Abril 04, 2016

TECNOLOGÍA

En este número encontrarás noticias sobre:
- Tecnología
- Gobierno
- Negocios
- Fuentes Informales de Redes Sociales

Advierte INAI de control criminal de redes públicas de internet

por MARZO 26, 2016 / EL SOL DE MÉXICO

El INAI dio una serie de recomendaciones para que los vacacionistas no sean víctimas de los ciberdelincuentes, alertando con no visitar sitios dudosos o no reconocidos al buscar promociones de viajes por Internet, evitar hacer clic en ventanas emergentes o anuncios que ofrecen productos gratis o con promociones dudosas, no aceptar descargas de archivos de esos sitios y por ningún motivo dar información personal.

Así mismo se recomienda evitar mantener siempre activa la conexión Wi-Fi/Bluetooth, además de no conectarse a redes o dispositivos públicos ya que pueden estar siendo controlados por los ciberdelincuentes para el robo de información. No publicar fotografías, videos o ubicación en tiempo real en redes sociales que puede ser utilizada en contra del patrimonio, familia o persona. Pedir a algún vecino o persona de confianza recoger la correspondencia mientras se encuentran ausentes, esto para evitar el robo de información.

Estar pendiente de la tarjeta bancaria al hacer pagos, cuando se use una terminal de cobro y si se hacen pagos en línea. Llevar consigo, el número telefónico del banco, para comunicarse en caso de necesitar alguna aclaración y evitar tener el dispositivo móvil sin seguridad.

Fuente: http://elsoldemexico.com.mx/mexico/160596-advierte-inai-de-control-criminal-de-redes-publicas-de-internet

Por bandas extranjeras, crece robo de identidad en México

por MARZO 26, 2016 / MILENIO

El robo de identidad creció de manera alarmante en México por la operación de bandas criminales centroamericanas y europeas, e incluso la mafia rusa. El modus operandi de estas bandas es tener a gente buscando en la basura estados de cuenta y tarjetas bancarias para robar identidades, y también rastros de operaciones bancarias en los equipos de cafés internet.

Según el presidente de la Condusef, Mario di Costanzo, el monto defraudado por este delito pasó de 110 millones de pesos en 2014 a por lo menos 250 millones en 2015. Por lo que pidió al Congreso de la Unión tipificar y homologar el delito de robo de identidad a nivel federal ya que sólo en la Ciudad de México, Estado de México, Colima y Tabasco se ha definido esta conducta como ilegal.

Fuente: http://www.milenio.com/politica/Condusef-robo_de_identidad_0_707929207.html

Ciberataques, por qué no debemos pagar para descifrar nuestros archivos

por MARZO 23, 2016 / PYMES AUTÓNOMOS

Al sufrir un ataque de un virus que cifra los archivos, tanto empresas o particulares tienen que seguir las instrucciones de los atacantes para realizar un pago y que sus datos sean descifrados, pero no existe una garantía de que la información sea descifrada e intacta, una de las dudas de esto es que el pago se hace por medio de criptomonedas y de manera anónima, alentando a que el ciberdelincuente siga haciendo sus fechorías nuevamente al ver que ha logrado su cometido.

Por lo que es recomendable utilizar la copia de seguridad para recuperarlos si se tiene sospecha de que un correo o una aplicación está instalando algo que no debe, se debe desconectar el ordenador de la red, apagarlo y llamar al servicio técnico para minimizar los daños.

Fuente: http://www.pymesyautonomos.com/tecnologia/ciberataques-por-que-no-debemos-pagar-para-descifrar-nuestros-archivos

Seguridad informática enfrenta escasez de talento en México

por MARZO 22, 2016 / SEGURIDAD EN AMÉRICA

De acuerdo con Brett Kelsey, vicepresidente y CTO para Américas de Intel Security, el sector de la ciberseguridad sufre de escasez de talento, ya que las empresas carecen de personal especializado y tardan meses en cubrir las posiciones.

Así mismo comentó que el reto del cuidado de la información de las organizaciones ha cambiado a causa de la enorme dispersión de usuarios móviles, remotos y corporativos, la multiplicación de dispositivos, la acumulación de información en la nube y factores como BYOD (Bring Your Own Device).

El directivo agregó que se están buscando herramientas y conocimientos para identificar, cazar, evaluar y priorizar los riesgos que no se clasifican simplemente en "malos" o "buenos"; ya que algunos ataques se desarrollan lentamente, y ya cuando el sistema está comprometido, la organización tiene poco tiempo para detectar y contener el incidente antes de que los datos se filtren u ocurran grandes daños.

Fuente: http://www.seguridadenamerica.com.mx/noticias/de-consulta/secciones-revist-seguridad-en-america/noticias-sobre-redes-e-infraestructura-ti/21565-seguridad-informatica-enfrenta-escasez-de-talento-en-mexico

Hackers roban datos de clientes de Verizon

por MARZO 25, 2016 / WEBADICTOS

Por vulnerabilidad en la seguridad, ciberdelincuentes accedieron y robaron datos de contactos de empresas clientas de la compañía estadounidense Verizon.

La compañía asegura que el problema fué resuelto, y que el material robado corresponde sólo a información de contacto, que no incluye datos como la duración o número de destino de las llamadas realizadas. Pero no especificó el número de afectados.

El periodista y bloguero especializado en ciberseguridad Brian Krebs aseguró haber visto en un foro "de cibercriminales" en internet un anuncio en el que se ofrecía la información de contactos de un millón y medio de clientes de Verizon.

Dijo que la información se vendía en un paquete por 100.000 dólares, y en partes con los datos de 100.000 clientes por 10.000 dólares cada una.

Fuente: https://webadictos.com/2016/03/25/hack-verizon/?wa_count=5

¿Qué países de América Latina tienen estrategias contra ciberataques?

por MARZO 14, 2016 / CIOAL

Un informe evalúa la situación de 32 países en cuanto a seguridad informática en función de indicadores de política y estrategia, cultura y sociedad, educación, marco legal y tecnología. Además, analiza la situación de las legislaciones y la

Estas medidas han sido adoptadas por Brasil, Colombia, Jamaica, Panamá, Trinidad y Tobago y Uruguay, mientras que Argentina, Antigua y Barbuda, Bahamas, Costa Rica, Dominica, El Salvador, Haití, México, Paraguay, Perú y Surinam, están en proceso de articular una estrategia.

Sólo uno de cada cinco países está preparado, y en 30 de los 32 estudiados, los ciudadanos no están bien informados de los riesgos de privacidad y seguridad en el ciberespacio, según el presidente del BID, Luis Alberto Moreno.

Los riesgos se multiplicarán con el "Internet de las cosas", donde estarán interconectadas máquinas y sensores inteligentes, controlando virtualmente todo lo que se usa a diario.

Fuente: http://sanluis24.com.ar/index.php?option=com_content&view=article&id=65087:ique-paises-de-america-latina-tienen-estrategias-contra-cyber-ataques&catid=60:tecnologia&Itemid=59

GOBIERNO

El Sector Energético es el objetivo principal de los cibercriminales

por MARZO 22, 2016 / FORBES MÉXICO

El sector energético influye tanto en la economía de un país y una región, por lo que los cibercriminales tienen como objetivo los SCADA (Centros de control de procesos industriales a distancia). Esto para espionaje de empresas a sus competidores o de gobiernos nacionales a compañías estatales de otros países. DNV GL destaca las diez amenazas digitales principales a las que están expuestas estas organizaciones:

1. La falta de conciencia sobre la seguridad cibernética y la formación entre los empleados.

2. El trabajo a distancia durante la operación y mantenimiento. Hay que proteger los dispositivos que utilizan los empleados estén conectado a la red.

3. El uso de productos de TI estándar con vulnerabilidades conocidas en el entorno de producción.

4. Una cultura de seguridad cibernética limitada entre los vendedores, proveedores y contratistas. La mejor estrategia de seguridad digital, al igual que en la vida "offline", es el uso del sentido común y la precaución.

5. Separación insuficiente de las redes de datos.

6. El uso de dispositivos móviles y unidades de almacenamiento, incluyendo teléfonos inteligentes.

7. Las redes de datos entre instalaciones dentro y en alta mar.

8. La seguridad física insuficiente de las salas de datos, armarios, etc.

9. software vulnerable.

10. Los sistemas de control que han sido superados y el envejecimiento en las instalaciones.

Fuente: http://www.forbes.com.mx/sector-energetico-objetivo-principal-los-cibercriminales/

Gmail te avisará si eres un objetivo del gobierno

por MARZO 27, 2016 / DIGITAL TRENDS ES

Entre los cambios que ha hecho Google se encuentra la expansión de las notificaciones de "navegación segura", que indican cuando se va a abrir un enlace de un correo electrónico sospechoso.

Estas advertencias se mostrarán cuando se haga clic en el vínculo, pero antes de que este enlace se abra, mostrará también una opción para retirarse en lugar de visitar la página.

Ya que antes sólo había una advertencia antes de hacer clic sobre el vínculo sin opción de bloqueo.

Además, Google también está luchando contra los ciber ataques del gobierno, mostrando un aviso cuando piensan que están en la mira de un hacker de alguna instancia del gobierno.

En un blog la empresa afirma que menos del 0.1 % de los usuarios de Gmail recibirá esta advertencia.

Fuente: http://es.digitaltrends.com/internet/gmail-fbi-ciber-ataques-advertencias/

NEGOCIOS

México, el tercer país más propenso a fraudes corporativos

por MARZO 24, 2016 / PLANO INFORMATIVO

Con un aumento en el fraude empresarial del 5% y con afectaciones como el robo de activos (23%), el fraude de vendedores, proveedores o adquisiciones (23%) y el robo, ataque o pérdida de información (17%), México e India son de los países que sufren más fraudes a nivel corporativo en el mundo, ya que 80% de sus empresas fueron víctimas de algún incidente de fraude durante los últimos 12 meses, según la firma Kroll.

El tema de fraude a nivel nacional es complicado, porque no solo afecta a la economía sino también se encuentra relacionado con la corrupción en las empresas, comentó Brian Weihs.

Fuente:
http://planoinformativo.com/nota/id/450177/noticia/mexico,-el-tercer-pais-mas-propenso-a-fraudes-corporativos.html

FUENTES INFORMALES/REDES SOCIALES

Hackean página web de Cultura de la CDMX

por MARZO 31, 2016 / EL UNIVERSAL

La página web de la Secretaría de Cultura del Gobierno de la Ciudad de México fue intervenida al parecer por el grupo Anonymous Venezuela poco después de la medianoche.

En lugar del menú con la agenda cultural del gobierno capitalino, en portada aparecía una pantalla negra con una leyenda donde se leía: "¡Alto a la violencia contra las mujeres!".

Así mismo el mensaje: "Nos encontramos en momentos de cambios sociales importantes, pero parece ser que hemos olvidado el más importante: Nuestras mujeres, debemos levantar la voz, debemos impedir que sigan sufriendo víctimas del maltrato psicológico o físico." Aproximadamente a las dos de mañana el sitio no mostraba irregularidad alguna.

Fuente:
http://eluniversal.com.mx/articulo/metropoli/cdmx/2016/03/31/hackean-pagina-web-de-cultura-de-la-cdmx

TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No.6

26 MARZO – 03 ABRIL, 2016

Elaboración: ABRIL 04, 2016.