



TOTALSEC NEWSLETTER – INFOSEC MX

BOLETIN No. 10

ABRIL 23 – Mayo 01

Elaboración: Mayo 02,
2016

FINANZAS

**En este número
encontrarás noticias
sobre:**

- Finanzas
- Gobierno
- Tecnología

Bancos deben invertir en capacitar a usuarios para evitar cibercrimen

por ABRIL 19 2016 / EL FINANCIERO

Expertos en seguridad y del sector bancario, coincidieron en que además de adoptar nuevas tecnologías e invertir en seguridad como se ha hecho hasta el momento, se deben dirigir recursos para concientizar al usuario para el manejo de la misma.

Estamos entrando al sistema electrónico, al home-banking y al autoservicio, debido a que no hay otra manera para hacer estas transacciones, y las personas de mayor de edad son las más débiles en el sistema bancario.

Los bancos tienen equipos que analizan el comportamiento de sus clientes, pero aún se siguen dando casos en que se usan nips muy vulnerables o los usuarios comparten sus códigos de seguridad.

Y ahora las aplicaciones tienen acceso a nombre y tarjetas de crédito del usuario, por lo que se ha vuelto un blanco para los ciberdelincuentes.



Fuente: <http://www.elfinanciero.com.mx/tech/bancos-deben-de-invertir-en-capacitar-a-usuarios-para-evitar-cibercrimen.html>

GOBIERNO

Diputado promueve hasta 12 años de cárcel por usurpación de identidad

por ABRIL 26, 2016 / NOTICIAS TERRA MEXICO

El vicepresidente de la Mesa Directiva del Senado, Arturo Zamora Jiménez, presentó la iniciativa que busca tipificar y sancionar con 5 a 12 años de prisión a quien “fuera de normatividad, por cualquier medio y por cualquier causa obtenga, posea, use, transmita, retenga, controle, adquiera, transfiera, publique, difunda, distribuya, acepte, compre, venda u ofrezca en venta, gestione o almacene, bancos de información que contengan datos específicos y/o sensibles respecto de la identidad de dos o más personas identificadas o identificables”.

Se busca castigar delitos como el “phishing”, el robo de datos de identidad, haciéndose pasar con la víctima como alguien confiable.

El “skimming” que es la clonación de tarjetas de crédito o débito por medio de un dispositivo instalado en cajeros automáticos o usado en establecimientos.

Los riesgos van desde compras en línea o pago de servicios con cargo a tarjetas alteradas; apertura de créditos con cargo a la víctima; transmisión ilícita de propiedades inmobiliarias; altas de personas en el Servicio de Administración Tributaria (SAT) para responsabilizar a la víctima de evasión de impuestos.

Fuente:

<http://noticias.terra.com.mx/mexico/politica/diputado-promueve-hasta-12-anos-de-carcel-por-usurpacion-de-identidad.c1932611a194ca07994f350eaf014583g20fjh21.html>

SAT lanzará solución para alertar sobre correos falsos

por ABRIL 26, 2016 / EL UNIVERSAL



El Servicio de Administración Tributaria (SAT), está trabajando en una solución tecnológica que permitirá a los contribuyentes verificar si el correo electrónico que recibieron es falso, para evitar fraudes, robo de identidad y robo de datos personales.

Estas consultas se podrán realizar en un estimado de dos meses en lo que se termina el proyecto.

El jefe del SAT, Aristóteles Núñez mencionó que por lo pronto están haciendo públicos los correos apócrifos con el ánimo de que la gente los identifique y tome sus precauciones.

Se ha visto que los correos vienen de servidores que se encuentran en Europa y Sudamérica, por lo que se está trabajando de manera conjunta con otras instituciones como la Policía Cibernética.

Fuente:

<http://www.eluniversal.com.mx/articulo/cartera/2016/04/26/sat-lanzara-solucion-para-alertar-de-correos-falsos>

TECNOLOGÍA

Amazon desmiente a Movimiento Ciudadano: No hubo hackeo del padrón electoral

por ABRIL 28, 2016 / SOPITAS

Hace unas horas, Dante Delgado, dirigente del partido, dijo que habían puesto la información en Amazon y ahí fue donde un hacker atacó. Por lo que Amazon salió a desmentir la versión del dirigente.

El especialista en seguridad cibernética de Amazon Chris Vickery, dijo que el Movimiento Ciudadano está mal informado o está mintiendo, la explicación más probable es que la compañía que contrataron para almacenar los datos cometió un error, por lo que están tratando de cubrirlo alegando que se trató de un hackeo u otro método ilegal, pero simplemente no había una contraseña u otra protección resguardando la base de datos.

Agregando "Es decepcionante que un partido político no tenga la integridad para admitir que se cometió un error, y en lugar de eso, intenten acusar que se cometió un hackeo".

Fuente: <http://www.sopitas.com/609240-padron-ine-amazon/>

Policía del futuro: Vida digital, clave contra el crimen

por ABRIL 21, 2016 / EXCELSIOR

El oficial de cibercrimen de la Organización Internacional de Policía Criminal (Interpol), Adrián Eduardo Acosta, indicó que se requiere una evolución de los miembros policiales, así mismo de una gran coordinación con las tecnológicas.

Ya que compañías como Facebook, Google o Microsoft, se enteran primero de los nuevos métodos de ataque, al recibir las quejas de los usuarios y al acercarse a las víctimas.

Ahora los narcotraficantes, u otros delincuentes utilizan las redes sociales o aplicaciones para planear cómo atraer víctimas. Por lo que las fuerzas policiales deben prepararse y comenzar a atraer talento especializado, así como firmar alianzas con empresas del sector tecnológico, ya que las áreas de investigación de estas instituciones se verán rebasados ante los cibercriminales, ejemplos de ello son: el abuso infantil y la distribución de videos o fotografías en internet; la sextorsión, que ha provocado varios suicidios o el uso de ransomware para extorsionar a las víctimas.

Fuente:

<http://www.excelsior.com.mx/hacker/2016/04/21/1087927>



En cuatro años, el robo de identidad aumentó 519%

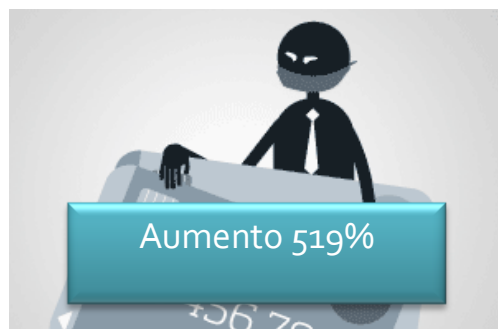
por ABRIL 19, 2016 / EL FINANCIERO

En cuatro años las reclamaciones por robo de identidad aumentaron 519% en México.

Por lo que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) pidió al Congreso poder tener facultades para cooperar con otras autoridades en la persecución de este delito y no sólo prevenirlo, así mismo es necesario que la persecución y la sanción de este delito sea a nivel federal, y con ello evitar disparidades regulatorias que existen en los estados que sí lo tipifican penalmente.

Mientras el proyecto de la Ley General de Protección de Datos Personales está siendo analizado en el Congreso de la Unión, las reclamaciones por robo de identidad, en el primer semestre de 2011 fue de cuatro mil 564. En el primer semestre de 2015 fueron 28 mil 258. La cifra se multiplicó seis veces.

Fuente: <http://www.elfinanciero.com.mx/nacional/en-cuatro-anos-el-robo-de-identidad-aumento-519.html>



Los edificios seguirán estando bajo riesgo de ciberataques, según nueva investigación

por ABRIL 20, 2016 / SEGURIDAD UNAM



Cualquier objeto conectado a internet y hasta los autos modernos son un potencial blanco de ataque. También los edificios inteligentes son cada vez más susceptibles a ser atacados ya que se siguen presentando fallas de seguridad básicas.

Se calcula que el número de edificios conectados, entre ellos hospitales, centros de investigación e iglesias, se aproximan a los 50.000 a nivel mundial, y 2.000 de ellos no tienen protección por contraseñas implementada.

Incluso Google, tuvo un incidente en el 2013, en donde dos investigadores de seguridad de Estados Unidos accedieron al sistema de administración de un edificio de oficinas de esta empresa en Sidney, Australia. Los ciberataques a edificios son constantes.

Fuente: <http://www.welivesecurity.com/la-es/2016/04/20/edificios-riesgo-ciberataques/>

Microsoft trabaja en el combate al cibercrimen en México

por ABRIL 27, 2016 / MUNDO CONTACT

En México, los incidentes reportados a la Policía Federal se incrementaron un 30%; y lastimosamente tiene el segundo lugar mundial en distribución de pornografía infantil. Los ciberataques son dirigidos a entidades educativas con 39%, el sector gobierno 31% y el sector privado 26%. Microsoft ha creado una unidad dedicada a combatir el crimen digital en el Cybercrime Center, en la ciudad de Redmond. Es operada por expertos especializados en el combate a la ciberdelincuencia.

Así mismo ha desarrollado el sistema PhotoDNA, un software que detecta imágenes con contenido ilegal, que es utilizado en plataformas como Facebook, Twitter y Google de forma licenciada, además de organizaciones como el FBI. Gracias a esta herramienta han sido retiradas más de 50 millones de imágenes en la red. A la fecha el centro ha logrado colaborar ante 14 tipos de malware, a través de una metodología que desenmascara el código fuente para comprender su funcionamiento y generar un escudo.

Fuente: <http://mundocontact.com/microsoft-trabaja-en-el-combate-al-cibercrimen-en-mexico/>

RansomWhere te ayuda a detectar el ransomware en tu Mac

por ABRIL 22, 2016 / PARENTESIS

Las infecciones por ransomware, se han elevado en computadoras Mac orillando a desarrolladores a crear soluciones. Una de ellas es el RansomWhere, un software creado por Objective-See que se encarga de alertar al usuario ante posibles amenazas de ransomware estando activo de manera permanente.

Aunque no es infalible, ayuda ante procesos maliciosos que tratan de cifrar archivos de una Mac.

Fuente:

http://www.parentesis.com/noticias/software_aplicaciones/RansomWhere_te_ayuda_a_detecer_el_ransomware_en_tu_Mac



México, rezagado en ciberseguridad

por ABRIL 20, 2016 / NTRZACATECAS

Jay Bavis, presidente y CEO de EC-Council, organización internacional certificadora de profesionistas en seguridad de la información, aseguró que en México las empresas sólo invierten del 3 al 6% del presupuesto en seguridad informática, mientras que el promedio a nivel mundial es del 15 al 18%, por lo que las hace "blancos" de ciberataques.

Agregó que un gran error que cometen las mismas, es que pensando que teniendo a un encargado de la seguridad informática evitarán sufrir ciberataques, siendo que todo el personal debe ayudar para contrarrestarlos y evitarlos. Recomendó que las universidades en México deben de proponer cursos y diplomados enfocados a la seguridad informática para ofrecer más especialistas del tema al mercado.

Fuente: <http://ntrzacatecas.com/2016/04/20/mexico-rezagado-en-ciberseguridad/>





TOTALSEC NEWSLETTER - INFOSEC

BOLETÍN No. 10

23 ABRIL – 01 MAYO, 2016

Elaboración: MAYO 02, 2016.