Boletín No. 2 /Abril 2016

BOLETÍN CELAES

Seguridad Bancaria

BOLETÍN CELAES
SEGURIDAD BANCARIA

ÍNDICE

2 Cibercrimen, Ciberseguridad Y Ciberataques

CUESTAN CIBERDELITOS 3 MIL MDD A EMPRESAS Y GOBIERNO: CEPAL

18-Apr-2016 18:35

Se multiplican las violaciones de datos con información personal, como números de tarjetas de crédito y ataques dirigidos a personas, organizaciones y robos bancarios.

El daño causado por los ciberdelitos a México alcanza los 3 mil millones de dólares anuales, de acuerdo con reportes de la Comisión Económica para América Latina y el Caribe (Cepal) y de la Organización de Estados Americanos (OEA), en donde el robo de información, la contaminación de equipos mediante correos spam para sustraer datos como números de cuentas o NIP, el robo de identidad, los programas maliciosos y los ataques a sitios web son las principales amenazas que van dirigidos al gobierno y corporativos.

En los últimos años los ciberdelitos han proliferado y se han diversificado aprovechando las vulnerabilidades de las instituciones para sustraer información. México se encuentra dentro del listado de principales países que son objetivo de estas amenazas, pues en robo de identidad ocupa el segundo lugar después de Brasil, al igual que en la infección de programas maliciosos.

En el rubro de ataques mediante correos no deseados, México se ubica en el séptimo lugar, mientras que en ataques a páginas web, se posiciona en tercer lugar dentro de un listado de 10 países, de acuerdo con el reporte "Del Internet del consumo a la Internet de la producción", elaborado por la Cepal.

Bajo este panorama, México aún debe mejorar diferentes rubros para fortalecer sus esquemas de seguridad en el ciberespacio, señala a su vez el reporte de Tendencias de Seguridad en América Latina y el Caribe, de la Organización de los Estados Americanos (OEA). En dicho estudio la institución elaboró un análisis con calificaciones del cero al cien, para evaluar la respuesta y las medidas adoptadas por varios países ante la inseguridad cibernética.

Las tareas pendientes.- En el reporte México observó una calificación de 32.4 sobre 100, lo cual implica que se encuentra 12.3 puntos por debajo del promedio global de 44.69 puntos. A nivel Latinoamérica, esto significa que México se encuentra por encima de países como Paraguay y Venezuela, pero muy por debajo de otros como Brasil, Uruguay, Argentina, Costa Rica, Chile y Colombia.

"Resulta de gran importancia comenzar con la pronta elaboración e implementación de estrategias y planes nacionales que agilicen la transición hacia un ciberespacio seguro en que sea posible aprovechar al máximo los enormes beneficios que generan estas nuevas tecnologías", indicó al respecto la consultoría The Competitive Intelligence Unit (CIU).

Señala que México registra bajos niveles en materia de marcos legales e instituciones encargadas de tratar la seguridad en línea, así como en programas de capacitación, certificación, desarrollo de profesionales y certificación de organizaciones de carácter público en esta materia. Este patrón se refleja nuevamente en una falta de mayor desarrollo en materia de marcos para cooperación nacional e internacional y redes de divulgación de información.

Dentro de las acciones que México debe emprender para mejorar la seguridad en el ciberespacio se encuentran la legislación y tipificación de "conductas delictivas" en internet, pero sin regular a estas tecnologías, ya que se trata de meras herramientas que son útiles para la sociedad, señaló Korina Velázquez, especialista en legislación y políticas públicas para la Sociedad de la Información, quien también es consultora para el Banco Mundial (BM) en la materia.

Las autoridades también deben tener preparación como peritos informáticos y capacitar a funcionarios públicos para que sepan la forma de operar de los delincuentes de internet y puedan hacer frente, de forma pronta y efectiva al crimen organizado on line, añadió la experta.

Afectaciones mundiales.- A nivel mundial los costos de los ciberdelitos ascienden en promedio a 113 mil millones al año, según datos de la firma de ciberseguridad Symantec.

Una encuesta realizada por la empresa señala que tan solo en 2013 el número de personas afectadas por este tipo de delito en todo el mundo fue del orden de 378 millones, con un costo promedio por víctima de 298 dólares, lo que representa un aumento del 50 por ciento respecto de los 197 dólares de 2012. El 83 por ciento de los costos

FUENTE: http://www.omnia.com.mx/noticias/cuestan-ciberdelitos-3-mil-mdd-a-empresas-y-gobierno-cepal/

¿CÓMO EVITAR QUE SU EMPRESA SEA VÍCTIMA DE CIBERATAQUES?

Tecnología - Abril 19 de 2016, 6:45 pm

Un experto en inteligencia y ciberseguridad explica algunas de las claves para evitar que las compañías sea hackeadas. Colombia es uno de los países más vulnerables en Latinoamérica.
Angélica Orcasitas M./NoticiasRCN.com

A propósito de la filtración de los 'papeles de Panamá', muchas empresas han replanteado su posición respecto a los peligros cibernéticos a los que se exponen. A pesar de ser una herramienta de desarrollo, la tecnología pone a las personas y compañías en situación de vulnerabilidad.

Félix Muñoz, experto en inteligencia y ciberseguridad y director general de seguridad del grupo español Entelgy, explica que a través de huecos de seguridad en los sistemas se puede entrar a la red de las compañías y sacar documentos sin que nadie los note.

Aunque se tiene conocimiento sobre el aumento de los casos de ataques cibernéticos en el mundo, no todas las compañías invierten ni le dan la importancia necesaria a estos hechos.

Los protocolos utilizados para proteger la privacidad en internet no son un garantía, pero tienen como objetivo hacer las redes lo más seguras posibles y la detección oportuna de cualquier ataque para poder detenerlo.

A pesar de ser muy cuestionado, uno de los métodos para evaluar la seguridad en internet es hacer pruebas con hackers, así identificar las falencias y hacer las respectivas correcciones. Las redes informáticas de una compañía tienen más posibilidad de ser penetradas debido a la cantidad de servidores activos.

Según Muñoz, Colombia es el tercer país de América Latina donde se presentan más casos de ciberataques.

Recomendaciones para evitar ataques cibernéticos:

El experto Félix Muñoz, que protege la información de al menos 400 entidades en el mundo, asegura que siguiendo algunos consejos básicos es menos probable que la privacidad sea vulnerada en internet.

1. **Utilizar contraseñas complejas, que contengan números, caracteres y letras, en todos los servicios de internet y cambiarlas periódicamente. Hay que evitar el uso de claves por defecto. Además cerrar sesión en cada oportunidad.**

2. **Mantener siempre el software, el sistema operativo del equipo y el antivirus actualizado, o configurarlo para que se actualice automáticamente.**

3. **Evitar descargar o abrir correos de dudosa procedencia, sospechosos, o que soliciten claves o información personal, sobre todo si terminan en la extensión ".exe". Es necesario tener en cuenta que el correo electrónico es una de las principales fuentes de entrada de virus a los computadores o dispositivos.**

4. Utilizar claves de ingreso para los dispositivos móviles, como prevención de protección de datos personales ante una posible pérdida o robo. También es recomendable usar antivirus en los celulares. Además, es fundamental conectarse a redes Wi-Fi de confianza.

5. **Limpiar el historial de navegación regularmente para dificultar la monitorización de los sitios por los que se navega.**

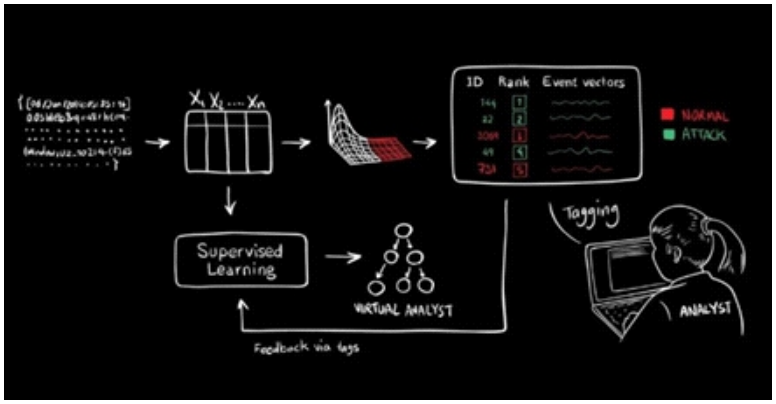
6. Utilizar un buen firewall, o red que bloquea el acceso no autorizado, y actualizarlo regularmente, para evitar modificaciones a datos o incluso a las páginas web.

7. Darle charlas reiteradas a los empleados sobre ciberseguridad y la importancia de tomar precauciones, de esta manera hay menos peligro de errores.

8. Evitar hacer compras por internet en sitios desconocidos e investigar antes de acceder a cuentas particulares. Por ejemplo, se recomienda nunca acceder a una web bancaria a través de un link de un e-mail sino hacerlo siempre introduciendo la dirección en el navegador.

http://www.noticiasrcn.com/tecnologia-tecnologia/evitar-su-empresa-sea-victima-ciberataques

Prevenir los ciberataques con inteligencia artificial es posible, y el MIT sabe cómo



Los ciberataques cada vez son más avanzados, y los hackers cada vez se las ingenian mejor para esquivar todo tipo de sistemas de seguridad. También es cierto que los sistemas cada vez son más complejos y las vulnerabilidades son más numerosas. Y por esto hay un universo sobre esto, donde se mueve mucho dinero tanto en un bando como en el otro.

El MIT quiere acabar de una vez por todas con estos ciberataques, para lo que han creado un sistema de inteligencia artificial que hará las cosas más difíciles todavía a los atacantes. Ha sido su equipo inteligencia artificial e informática (CSAIL) quien ha diseñado a AI², que se encargará de detectar los ciberataques bajo cualquier circunstancia.

Tiene una gran precisión de detección, y reduce bastante el número de falsos positivos. Sus desarrolladores nos ponen en situación, contándonos cómo funciona la detección de ciberataques hoy día. Se hace a través de personas o máquinas; los primeros se basan en reglas ya establecidas. Por eso, cuando se realizan ataques que no siguen estas reglas, pasan por alto y no se detecta nada extraño. Los segundos se basan en la detección de anomalías, donde aparecen muchos falsos positivos.

La alternativa que proponen en el MIT es combinar lo mejor de estos dos tipos, haciendo que los datos que identifica la máquina los revisen personas. A través de este sistema de aprendizaje, AI² va aprendiendo y le permite ir mejorando su inteligencia, llegando a resultados tan buenos como la detección del 85% de los ciberataques.

Estamos hablando de una mejora del triple respecto a los sistemas que existen hoy día, y una reducción de falsos positivos de hasta cinco veces. Para realizar estas pruebas se utilizaron 3.600 millones de líneas de registro, que fueron generadas por millones de personas en el transcurso de tres meses.

http://voltaico.lavozdegalicia.es/2016/04/prevencion-ciberataques-mit/

CIBERSEGURIDAD. UN NICHO PARA CRECER

El Incibe identifica los sectores y actividades en los que la industria del ramo debe buscar su desarrollo futuro. E l futuro se escribe con ciberseguridad, pero identificar los sectores y actividades concretas que requieren productos y servi-cios, y cuáles son los que demandan, son claves para que la industria tecnológica oriente su actividad a las necesidades del mercado. Y los futuros profesionales enfoquen su formación. El Incibe ha dibujado esas hojas de ruta industria, medio ambiente, movilidad, servicios, ciudadanía y gogernanza son los nichos de mercado

MARÍA J. MUÑIZ | LEÓN
19/04/2016

La ciberseguridad es la garantía del futuro digital, y las empresas y profesionales que enfoquen su actividad a este sector tienen ante sí previsiones de demanda y crecimiento de más de dos dígitos para los próximos años. Sin embargo, identificar correctamente las necesidades del mercado y enfocar la actividad a lo que se demanda realmente es imprescindible para aprovechar la oportunidad económica que plantean las vulnerabilidades de un entorno completamente interconectado. Dentro de su objetivo de impusar el talento y la industria relacionada con el sector, el Instituto Nacional de Ciberseguridad (Incibe) ha realizado un informe que servirá de base no sólo para que las empresas tomen sus decisiones, sino para que el propio instituto oriente las acciones que tiene encomendadas de apoyo a las empresas del sector. Un apoyo en el que la internacionalización y el mercado global tienen un papel protagonista.

El estudio Tendencias en ciberseguridad ha realizado "un análisis cruzado de las tendencias globales en la materia y las necesidades sectorializadas, lo que ha dibujado un mapa claro de tendencias", explica Alberto Hernández, director de Operaciones del Incibe. Estas tendencias se concretan en los sectores de industria y medio ambiente, movilidad, servicios, ciudadanía y gobernanza.

Por lo que se refiere a la industria y el medio ambiente, las redes de distribución inteligentes, la industria 4.0 y las infraestructuras críticas son, junto con las 'utilities'(servicios básicos como electricidad, agua y comunicaciones), las actividades en las que centrarse para el desarrollo de sistemas ciberresilientes, y seguridad en los sistemas de control industrial (Scada); además de los mecanismos de protección de las redes de distribución.

En cuanto a la movilidad, es uno de los sectores que se está desarrollando de forma más visible para los ciudadanos. La industria de la ciberseguridad tiene un importante nicho de actuación en los transportes, desde los coches inteligentes (en muy poco tiempo los vehículos estarán interconectados y serán por tanto más vulnerables) a la seguridad y protección de los vehículos aéreos no tripulados (drones) y la protección de las comunicaciones de los satélites.

En el campo de los servicios las finanzas y los seguros, sobre todo la banca on line, demandan mayores medidas de seguridad digital. A través del análisis de big data es necesaria la detección del fraude en banca y seguros; además de la gestión de la información en los eventos de seguridad, y la seguridad de los servicios FinTech.

Pero también los temas relacionados con la informatización de los datos de los ciudadanos implica la necesidad de nuevas medidas de protección, y por tanto la posibilidad de desarrollo de productos y servicio para garantizar esta seguridad. La

protección de los dispositivos médicos conectados y el cifrado para la investigación médica y farmacéutica, además del almacenamiento seguro y ubicuo de los datos médicos, son las principales líneas de actuación en este campo. Que se complementaría con la cibereducación y los laboratorios de ciberseguridad.

Tampoco la administración es ajena a las necesidades de seguridad cibernética, a través de las exigencias del eGovernment, la defensa y la participación ciudadana. Y un importante papel tienen también los ciberejercicios y la simulación de incidentes, para ejercitar la prevención de incidentes.

En cuanto a las propias necesidades del sector tecnológico, se concentran en las exigencias que tendrá la expansión del Internet de las cosas, los servicios de seguridad en la nube (la seguridad como servicio); el cifrado en tiempo real, el hacking ético y la certificación de confianza digital.

En total el estudio realizado por el Incibe identifica 30 grandes tendencias de ciberseguridad, de las que se han priorizado 20 en función de criterios como capacidad de penetración y desarrollo de oportunidades de negocio en España. En los primeros puestos de esta lista está el análisis de big data, los servicios de seguridad en la nube, la distribución de ciberinteligencia, los modelos de gestión de ciber-resiliencia, la protección de dispositivos conectados, el cifrado en tiempo real, la identificación biométrica, la cibereducación, la protección de los coches inteligentes o los sistemas de simulación de escenarios.

http://www.diariodeleon.es/noticias/innova/ciberseguridad-nicho-crecer_1062552.html

Bancos deben de invertir en capacitar a usuarios para evitar cibercrimen

A diferencia de otros países de la región, los bancos en México sí invierten en medidas de seguridad para evitar cibercrímenes, pero aún es necesario que enfoquen recursos para concientizar al usuario sobre el manejo de estas tecnologías, indicaron expertos del sector.
Jair López - 19.04.2016 Última actualización 19.04.2016
Expertos en seguridad y del sector bancario coincidieron en que las instituciones financieras en el país si bien están adoptando nuevas tecnologías e invierten en seguridad, deben de dirigir recursos en concientizar al usuario sobre el manejo de dicha tecnología.

"Se necesita invertir en que la gente conozca los riesgos que corre al usar internet y las nuevas tecnologías, así como en servicios electrónicos en materia de banca", consideró Adrián Acosta, director de crimen digital de la Interpol.

Acosta resaltó que a diferencia de otros países de la región, las instituciones bancarias en México sí invierten en medidas tecnológicas de seguridad para evitar los cibercrímenes, entre ellas el uso de chip, token y la adopción de equipos especializados en seguridad.

Sin embargo, el integrante de la Interpol señaló que es de suma importancia invertir también en la preparación de los clientes en el uso de nuevas tecnologías, entre ellas los pagos en línea.

Ciberdelincuencia acosa a 47% de usuarios Bancos en México pierden 93 mdd al año por fraudes en línea: IMEF Instituciones financieras reprueban examen para prevenir lavado de dinero"Te están introduciendo al sistema electrónico, al home-banking y al autoservicio porque ya no hay otra manera para hacer estas transacciones. Las personas mayor de edad también son una debilidad en el sistema bancario. Estas personas no saben de tecnología y están siendo obligados a utilizar este tipo de tecnología", señaló Acosta.

Javier Montaño, director general adjunto de riego operacional y tecnológico de la Comisión Nacional Bancaria y de Valores, coincidió en que si bien los bancos están preocupados por blindarse de los cibercriminales, muchas de las vulnerabilidades que sufren sus clientes son a partir de la falta de conocimiento.

Montaño destacó que hoy los bancos cuentan con equipos que diariamente analizan el comportamiento de sus clientes, sin embargo se siguen dando casos en donde se usan nips que son muy vulnerables o casos en donde los mismos usuarios comparten sus códigos de seguridad.

Rafael Valencia, coordinador del grupo de prevención de fraudes de la Asociación de Bancos de México, señaló que la tecnología abrió nuevas oportunidades de negocio, pero también aumentó las posibilidades de riesgo.

De acuerdo con Valencia, el que ahora una aplicación tenga acceso a nombre y tarjetas de crédito del usuario lo hace un objetivo importante para los atacantes.

En este sentido, dijo que lo usuarios deben de estar al tanto de la información que comparten con este tipo de nuevos servicios.

"Cualquiera información que se pueda capturar y que se pueda extraer el crimen organizado puede enviarse a cualquier parte del mundo y de forma rápida preparar y atacar", señaló.

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

3 Noticias de la Región

El costo de la seguridad de las tarjetas de crédito

Última actualización 14.04.2016

Aunque la mayoría de tarjetas de crédito en Estados Unidos contiene un chip para sumar seguridad, la mayor parte de las terminales de pago en comercios minoristas no puede leer la nueva tecnología. Y la situación no va a mejorar pronto.

Una mayoría de tarjetas de crédito en los Estados Unidos contiene ahora un chip diseñado para sumar más seguridad; sin embargo, la mayoría de las terminales de pago en los comercios minoristas no puede leer esa nueva tecnología. Y la situación no va a mejorar en un futuro inmediato.

Las redes de tarjetas de crédito comenzaron a promocionar hace años tarjetas con chip como protección contra falsificaciones, y se suponía que los comerciantes se sumarían a los bancos y los procesadores de pagos para el 1 de octubre, o asumirían la responsabilidad por cargos fraudulentos que ocurrieran en sus tiendas.

A fines del año pasado, sólo 20 por ciento de las terminales habían sido activadas para procesarlas, según Alex Johnson, director en la firma de investigación Mercator Advisory Group. En cambio, casi 60 por ciento de las tarjetas de crédito emitidas por los bancos tienen un chip incorporado.

Los gastos que implicaba y los tiempos más prolongados para las transacciones hicieron que muchos comerciantes esperaran para actualizar sus sistemas. Los minoristas, desde las grandes cadenas hasta las tiendas pequeñas, gastarán un total de 30 a 35 mil millones de dólares para pasar al EMV, según la Federación Nacional de Minoristas.

Ahora que tienen una idea de lo que significa cargar con los costos por fraude, los propietarios de tiendas están apresurándose a comprar, certificar y desplegar la tecnología, conocida como EMV -por Europay, MasterCard Inc. y Visa Inc., sus patrocinadores. No obstante, los comerciantes minoristas tienen que hacer cola ya que la demanda de dispositivos y servicios supera la oferta.

"Francamente, el mayor problema en la adopción de EMV es la cola", dijo en una entrevista Vin D'Agostino, vicepresidente ejecutivo del fabricante de terminales de pago VeriFone Systems Inc. La demanda creció considerablemente "porque están empezando a ver el cambio de responsabilidad".

D'Agostino no cuantificó el trabajo atrasado en VeriFone, con sede en San Jose, California, limitándose a decir que "hay muchos esperando" el software, la certificación y las pruebas y que la compañía espera terminar con su oleada actual de clientes este año.

Cuidado con las tarjetas adicionales y pre aprobadas

Arrecia competencia en la banca por clientes de tarjetas de crédito

El país donde ni los bancos aceptan efectivo

CERTIFICACIÓN

La cuestión no es solamente conseguir el hardware. Las tiendas deben probar su funcionalidad y recibir una certificación, y eso requiere un promedio de tres intentos para hacerlo bien, dijo Greg Burch, vicepresidente de iniciativas estratégicas en el fabricante de terminales Ingenico Group SA con sede en París.

Los comerciantes minoristas pueden, no obstante, aceptar transacciones con tarjeta de cinta magnética y no serán responsables de cargos fraudulentos si el consumidor todavía no recibió la tarjeta con chip. Normalmente, sería responsable el emisor de la tarjeta.

"Es un proceso complejo y a los comerciantes les lleva meses y meses realizar la certificación", dijo Derek Ross, responsable de ventas y desarrollo de negocios en ICC Solutions Ltd., una compañía con sede en el Reino Unido que contrata al procesador de pagos Vantiv Inc. para certificar a los comerciantes estadounidenses.

En otros países, el avance hacia la tecnología con chip comenzó hace más de dos decenios. En 2011, Visa anunció que el 1 de octubre de 2015 la responsabilidad pasaría a los comerciantes estadounidenses a menos que adoptaran EMV. Luego lo hizo MasterCard. Wal-Mart Stores Inc., mostrándose proactivo, comenzó a instalar equipos aptos para EMV en sus tiendas un decenio atrás.

http://www.elfinanciero.com.mx/economia/el-costo-de-la-seguridad-de-las-tarjetas-de-credito.html

LOS DISPOSITIVOS MÓVILES SON LOS PROTAGONISTAS DE LAS COMPRAS MÓVILES DURANTE 2016

Por Valeria Murgich 19-04-2016,

Un creciente numero de compradores online se están decantando por el uso del móvil o la Tablet cuando se trata de comprar en internet, lo que es una muestra de cómo están cambiando los hábitos de compra gracias a este tipo de dispositivos, que permite a los consumidores la adquisición de productos y servicios desde cualquier lugar y de forma rápida y simple.

Además, los dispositivos móviles se han convertido en imprescindibles cuando se trata de la comparación de precios, así como la investigación sobre productos antes de su adquisición o la búsqueda de cupones y descuentos; razones que les fortalecen como nuevo canal de compra.

"En 2016 se estima que en España las compras online hechas a través de ordenadores crecerán un 13%, sin embargo en los dispositivos móviles lo harán en un 51%, una cifra que lo sitúa entre los tres países que más crecerán junto con Italia (80%) y Holanda (57%). El dato de España está seis puntos por encima de la media de estimación de crecimiento en Europa (45%), y se sitúa muy por encima de países como Alemania (45%), Francia (44%) o Reino Unido (43%).

Los ingresos a través de dispositivos móviles para España en 2016 serán por valor de 2.260 millones de euros, dato que se ha multiplicado por seis desde 2013 (+511%), y todavía existe un gran potencial de crecimiento. Además, hay que señalar que 20 céntimos de cada euro (19,7%) de las ventas online en España en 2016 provendrán de los Smartphones y las Tabletas. Estas premisas confirman que las compras realizadas a través de dispositivos móviles son cada vez más populares, de hecho las que se harán a través de Smartphones crecerán un 59%, dato que se sitúa muy por encima de la media europea (42%), y supondrán unos ingresos de 1.240 millones de euros. En el caso de las Tablets este dato de aumento será del 42%, y supondrá unos ingresos por valor de 1.020 millones de euros."

Estos datos son resultado del más reciente estudio sobre eCommerce realizado por RetailMeNot, a través del Centre for Retail Research (Nottingham, Inglaterra), que ha analizado las cifras de ventas online en los ocho principales mercados europeos (Alemania, Francia, España, Italia, Países Bajos, Polonia, Reino Unido y Suecia), así como Estados Unidos y Canadá.

Sexta posición en el ranking de gasto medio

"Este año los compradores online españoles a través de sus dispositivos móviles harán once compras, lo que supone tres compras más respecto al año anterior. En cada una de ellas se gastarán una media 36,58 euros y el gasto medio total por comprador en 2016 será de 401 euros, 83 euros más que el año anterior. En este sentido hay que señalar que España se encuentra entre los seis países que más gastarán a través de los Smartphones y las Tablets. Reino Unido se posiciona a la cabeza del ranking de gasto por móvil con 1.074 euros; Alemania con 873 euros, Francia

con una cifra de 712 euros, Holanda con 525 euros y Suecia con 513 euros.
Asimismo, el informe señala que "tres de cada diez compradores online españoles ha comprado al menos un producto o servicio a través del móvil en el último año. A día de hoy España se encuentra por detrás de mercados maduros como Reino Unido o Alemania, donde esta cifra se sitúa en uno de cada dos usuarios online, pero muestra un gran potencial de crecimiento que mejora año tras año."
¿Qué métodos de pago prefieren los españoles?
"Una de los aspectos más valorados por los usuarios a la hora de comprar en internet es que las páginas ofrezcan varios métodos de pago. De esta forma los compradores no se sienten acorralados a la hora de pagar y pueden elegir el método que mejor les convenga en ese momento y el que más seguridad les de. En este ámbito, el 70% de los españoles prefiere pagar con tarjeta de crédito o débito en primer lugar, seguido por el pago contra reembolso (18%)y el pago por integradores (8%)."
En este sentido, Mike Lester, Vicepresidente y Director General de Nuevos Mercados de RetailMeNot cocluye que: "Existe una tendencia positiva en la compra por internet a través de dispositivos móviles ya que en 2015 más de una cuarta parte de los compradores online adquirieron al menos algún productor a través de sus dispositivos móviles, y esto representa al 10% del total de los españoles, por lo que los datos son muy alentadores. Tanto los comercios minoristas como las tiendas y las marcas continuarán mejorando la experiencia de compra, los métodos de pago o los descuentos en el ámbito de los dispositivos móviles".

http://www.merca20.com/los-dispositivos-moviles-son-los-protagonistas-de-las-compras-moviles-durante-2016/

Las "fintech" deben ofrecer seguridad y simplicidad para tener éxito

19/04/2016 19:43

Madrid, 19 abr (EFECOM).- Las empresas tecnológicas del sector financiero, conocidas como "fintech", tienen que ofrecer "seguridad, simplicidad y transparencia" para ganarse la confianza del usuario y así tener éxito, según los expertos de la aplicación para gestionar la economía personal Mooverang.

En un comunicado, dicho gestor identifica varios retos que deben superar las empresas del sector "fintech" para tratar de triunfar en el negocio, principalmente el de ganarse la confianza del usuario, clave en el mundo financiero.

Cada vez se hacen más compras por Internet, transacciones desde la web de un banco o la apertura de una cuenta corriente en un banco sin oficinas.
Para Mooverang la confianza del cliente se puede obtener gracias a la seguridad tecnológica y emocional, ya que los usuarios desconfían de lo nuevo y no basta con implementar altos niveles de seguridad sino que además hay que ser capaz de explicar al usuario los riesgos y qué se ha hecho para eliminarlos.

Por otro lado, la simplicidad también es un factor importante, puesto que los temas financieros son percibidos como algo complejo; los usuarios quieren servicios "simples, rápidos y adaptados a su modo de vida".

Asimismo, la transparencia es "fundamental", los productos deben ser fáciles de entender, sin letra pequeña, sin cláusulas abusivas, ni costes escondidos, y llegar al sector "fintech" con una marca desconocida es complejo.

Además, los bancos no deben estar reñidos con la tecnología y tienen que "acompañar al movimiento fintech de manera proactiva" y aprovecharse de las ventajas que trae consigo, añade Mooverang. EFECOM

http://www.lavanguardia.com/vida/20160419/401224156402/las-fintech-deben-ofrecer-seguridad-y-simplicidad-para-tener-exito.html

4 Cae organización trasnacional dedicada a la clonación de tarjetas crédito y débito

Los capturados están sindicados de violación de datos personales y hurto por medios informáticos

La Policía Nacional a través de la Dirección de Investigación Criminal e INTERPOL, en desarrollo de la operación 'Trópico' capturó en la ciudad de Bogotá a tres integrantes de una organización criminal trasnacional señalados de clonar tarjetas débito y crédito.

Un proceso investigativo adelantado en coordinación con la Fiscalía General de la Nación y el Grupo Americano de Unidades de Cibercrimen de INTERPOL permitió dejar al descubierto la existencia de una organización criminal que venía instalando dispositivos de clonado de tarjetas bancarias en cajeros electrónicos ubicados en países de centro y sur América como Chile, Ecuador, Honduras, Panamá, Guatemala, El Salvador y Colombia.

A nivel nacional esta organización delinquía en varias ciudades del territorio colombiano, especialmente en la costa Atlántica, en Bogotá actuaban en los sectores de Santa Isabel, Normandía, Park Way y en el norte de la ciudad.

Con base en denuncias y procesos investigativos originados en la pasada edición de la Copa América desarrollada en Chile donde se hallaron en poder de estas personas elementos para la obtención de claves bancarias,

en las últimas horas integrantes del Centro Cibernético Policial de la DIJIN adelantaron una operación en Bogotá donde fueron capturados los integrantes conocidos como 'ñaña', 'mamut' y 'la mona' de esta organización criminal trasnacional, por los delitos de concierto para delinquir, violación de datos personales y hurto por medios informáticos. Dos de los sindicados fueron detenidos en el Aeropuerto Internacional El Dorado cuando pretendían huir hacia Ecuador.

La red, integrada por tres personas, enviaba los datos de las víctimas a sus contactos en Ecuador desde donde se realizaban los retiros de dineros, afectando clientes de los bancos de la región.

Las víctimas, principalmente clientes de entidades bancarias de estos países eran objeto del hurto de fuertes sumas de dinero de sus cuentas, producto de modalidades empleadas por la estructura criminal como la clonación de tarjetas y el cambiazo.

Durante la acción policial fueron incautados los siguientes equipos y dispositivos usados por la red para acceder de manera ilícita a los datos de los tarjetahabientes:

- 40 Dispositivos de almacenamiento
- 39 Tarjetas bancarias
- 9 Protectores de contraseña falsos
- 8 Discos compactos con software para la magnetización
- 3 Relojes espía con cámara incorporada
- 2 Cajas magnetizadoras de tarjetas

http://portal.policia.gov.co/es-co/Noticias/Paginas/Delincuencia.aspx

5 Fuera de Nuestro Continente

PwC creates cyber security game to let board members play as hackers

Australia's biggest accounting firm PwC is rolling out a new way of teaching its clients about cyber security, creating a game in which senior executives and board members can play as the attackers and the defenders.

Game of Threats was developed by the firm's Washington DC office, in conjunction with PwC's Australian design team and will be launched locally through the Melbourne office this week and in Sydney next week.

PwC cyber partner Richard Bergman said Game of Threats was the first solution of its kind for PwC Australia's digital design team but it could be the first of many gamified education products.

"We're already looking at using gamification in other areas," he said" We're considering games for financial crime and also crisis management in general - anything such as a product recall or a natural disaster. It helps companies to understand how well prepared they are."

Based on real-life

Game of Threats was developed based on reallife situations PwC has experienced helping clients respond to cyber breaches.

The game is fast-paced and each team has 90 seconds per turn to decide how to respond to the other side's move.

Related Quotes
ASX ANNOUNCEMENTS

The attacking team, the hackers, always goes first and has the option of playing a card to launch an attack or to buy more capability to invest in better skills to attack with.

The defending team, which acts as the company in the situation, has to then make a decision whether to play a card that lets them invest in more technology to protect themselves, invest more in people capabilities, or to respond to an attack that the attackers have launched.

Mr Bergman said defensive teams usually won if they decided on a long term strategy and stick to it.

"But if the attackers launch a few successful attacks and they panic, then the attackers usually win," he said.

"There are companies out there which panic and then make poor decisions, which impacts on their brand and customer trust."

The game took about six months for the business to develop, although most of this time was spent nailing the concept.

It was first rolled out in the United States two years ago and hundreds of sessions have since been run, with some companies putting their top 500 employees through the game.

Gamification trend

It's one in a string of recent gamification products which have been launched by the major professional services firms.

Last week Deloitte farewelled standard question and answer psychometric testing in favour of a customised "game" which placed future graduates in real life work situations to test their problem-solving capabilities.

The cyber security industry has also started developing gamified technology. In August Symantec acquired Blackfin Security and its Hacker Academy to bolster its gamification-led training efforts.

In the lead up to the launch, PwC's Game of Threats was trialled by non-executive directors from 20 to 30 boards.

Telstra chief information security officer Mike Burgess oversaw one of the trial Game of Threats sessions and said it was a useful tool to bring cyber security to life for board members.

"Board members know how to do their job well, but the complication with cyber security is it's complicated and it's hard for non-technical people to wrap their head around," he said.

"It explains to them through the game what a denial-of-service attack is, what a penetration test is and it just takes them through the terminology while they interact with it - it's a powerful learning tool."

The cost of the game will vary depending on the client, but $40,000 will buy a company four sessions of Game of Threats and includes the preparation time and the work running the sessions.

http://www.afr.com/technology/web/security/pwc-creates-cyber-security-game-to-let-board-members-play-as-hackers-20160229-gn713x

CELAES 2016 XXXI CONGRESO LATINOAMERICANO DE SEGURIDAD BANCARIA

FIBA

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

CELAES 2016 reúne a los líderes expertos del sector financiero para proveer perspectiva sobre la industria, convirtiéndola en la conferencia más completa y confiable del mercado.

Agende su participación desde ya !!

3 - 4 octubre

INSCRÍBASE CON DESCUENTO
Antes del 1 de junio de 2016

Algunos Temas a tratar

- Ciberseguridad – Estamos preparados en América Latina y el Caribe
- Pensando la CiberSeguridad : Nuevos Desafíos para la Industria Financiera
- Seguridad en pagos con tarjetas
- Cómo la Digitalización está transformando los conceptos de Seguridad y Privacidad.
- Amenazas Internas
- Network: Computación en la Nube
- Ejercicio Práctico de Simulación de una Crisis ante un Evento de CiberSeguridad

Quienes ostenten Certificaciones de ISACA podrán obtener créditos CPE de acuerdo a las políticas certificación correspondiente (ISACA Certification holders who attend this Conference may claim CPE hours according to certification policy).

Hotel Trump National Doral, Miami, Fl

Mas Información en http://www.felabancelaes.com/