

2013-06-24

Ciber Seguridad # 6

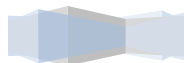


SCProgress

www.scprogress.com

ÍNDICE

1. Informe anual de seguridad FBI/IC3	03
2. Tu actividad en redes sociales puede poner en peligro un contrato de trabajo	04
3. Seguridad informática y los problemas con Corea del Norte	05
4. Se llevó a cabo con éxito el Seminario de Seguridad Informática Perimetral organizado por SCProgress	06



NOTICIA 1: Informe anual de seguridad FBI/IC3

El FBI y el Internet Crime Complaint Center (IC3) emitieron su informe anual [PDF] sobre el estado de la seguridad en Internet y cómo está creciendo los tipos de estafas y las nuevas tácticas de los delincuentes.

Mientras que las denuncias presentadas ante el IC3 se han reducido ligeramente respecto a los informes 2012 y 2011 (289.874 contra 314.246).

Overall Statistics

Total complaints received:	289,874
Complaints reporting loss:	114,908
Total Loss:	\$525,441,110.00
Median dollar loss for those reporting a loss:	\$600.00
Average dollar loss overall:	\$1,813.00
Average dollar loss for those reporting loss:	\$4,573.00

Las pérdidas monetarias por fraudes en línea han crecido más del 8%, superando los \$525 millones y con un promedio de U\$S 600 por persona.

Las quejas más comunes recibidas en 2012 incluyeron estafas de suplantación de correo electrónico, varios tipos de crímenes de intimidación y estafas y la utilización de scareware para obtener dinero de los usuarios.

Fuente: Segu-info.com



NOTICIA 2: Tu actividad en redes sociales puede poner en peligro un contrato de trabajo.

Las redes sociales tienen como función darnos la posibilidad de relacionarnos con personas que no podemos ver diariamente como familiares y demás. Según el enfoque o el uso que se le dé a una red social se le puede sacar más partido que el nombrado anteriormente.

Muy pocos son los jóvenes que tienen conciencia de que se puede perder la oportunidad de conseguir un empleo por los comentarios o fotos que dejan en sus perfiles. No son conscientes de que el uso de las redes sociales por parte de Recursos Humanos, para poder valorar si el candidato es adecuado, es una práctica que se usa habitualmente.

Un estudio realizado por Young People's Consumer Confidence (YPCC) ha relacionado el ámbito laboral con el entorno personal y ha analizado la repercusión que tienen las redes sociales en unos 6.000 casos, de jóvenes entre 16 y 34 años en más de cinco países diferentes, indicándonos que uno de cada diez jóvenes ha sido descartado para un trabajo por contenidos que no han agradado la empresa en sus perfiles.



Generalmente los jóvenes usan las redes sociales enfocadas a su vida personal para quedar bien y estar en contacto con sus amigos y no se preocupan por la imagen que puedan dar a alguna empresa u otras personas en general. Por otro lado ésta también, como nos quita, nos puede dar la oportunidad de conseguir un empleo si se realiza una buena gestión del mismo.

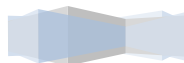
Son cientos las consecuencias que puede tener el hacer un comentario comprometido en la red

Como bien puede ser la nombrada con anterioridad, la pérdida de un empleo pero también puede llevarnos a malentendidos, dañar nuestra reputación on-line o incluso a que se nos llegue a interpretar como emisor de calumnias. Por este motivo es necesaria una mayor y mejor educación en el uso de las redes sociales.

Para poder mejorar nuestro propio perfil hemos de tener en cuenta varias cuestiones como por ejemplo el tener respeto hacia todas las personas, ya las conozcamos o no; no hacer retweets que puedan dañar la imagen o el honor de terceros, no publicar elementos difamatorios y sobretodo procurar no tener fotos o enlaces a las mismas de nosotros mismos en situaciones que nos pueda perjudicar a la hora que conseguir un trabajo.

Realmente está en nuestra mano el cuidado de nuestra reputación o imagen on-line a través de los perfiles de las redes sociales y es algo que debemos tener en cuenta ya que un trabajo nos puede cambiar la vida.

Fuente: delitosinformaticos.com



Noticia 3: Seguridad informática y los problemas con Corea del Norte

Las armas nucleares de Corea del Norte forman parte de los problemas internacionales que tienen en vilo al gobierno de los Estados Unidos. El presidente Barack Obama, y su homólogo chino Xi Jinping, coincidieron en que Corea debe renunciar a sus armas nucleares, pero no parece que vaya a haber una respuesta satisfactoria desde el país asiático en cuestión.

En la conferencia Obama y Xi tocaron diferentes temas, incluso realizaron una charla al aire libre que duró cerca de 50 minutos y una extensa discusión acerca de las medidas para moderar a Corea del Norte y evitar la escalada de conflictos. En los últimos meses los discursos de corte bélico de China han mantenido a los diferentes involucrados en seguridad internacional muy atento ante posibles movimientos.



Los presidentes de China y Estados Unidos acordaron que no aceptarán a Corea del Norte como una nación con potencia nuclear, y ante la negativa del país coreano también surgieron temáticas relacionadas con la seguridad informática.

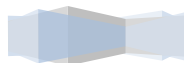
Los ataques de origen chino a diferentes empresas y sitios estadounidenses fueron otro de los puntos importantes al analizar la coyuntura política de ambas naciones.

Obama sostuvo que los ataques informáticos pueden ser muy malos para las relaciones económicas y políticas de ambas naciones ya que es imprescindible lograr cooperación y tolerancia entre ambas naciones.

Obama acerca directamente sus críticas a los ciberataques chinos, pero buscó mostrar una reunión cordial con el presidente chino de cara a mejorar la relación entre ambas naciones, que a menudo parecen distantes y frías.

Con la aparición de un enemigo en común que amenaza la paz del mundo con sus amenazas nucleares, la demostración de solidaridad y trabajo conjunto de Estados Unidos y China es una forma sólida de enfrentar el avance de los enemigos de ambas naciones.

Fuente: opensecurity.es



Noticia 4: Se llevó a cabo con éxito el Seminario de Seguridad Informática Perimetral organizado por SCProgress.

Este prestigioso evento, se llevó a cabo en las instalaciones del Hotel Sheraton el día miércoles 19 de Junio del presente año.

En el evento participaron los especialistas de EEUU Nisheet Davda Ingeniero Técnico y Jacob Thankachen Gerente de Tecnología de la empresa Cyberoam.

Los invitados al seminario eran los técnicos de las instituciones y empresas más importantes de nuestro país como las Fuerzas Armadas, S.P.P (Servicio de Protección Presidencial), Policía Nacional, CNT (Corporación Nacional de Telecomunicaciones), Ecuador Quality Systems, , UHY Ecuador Audit & Managment, la Escuela Politécnica del Ejército, entre otros.



Personal de SCProgress conjuntamente con los representantes de la empresa Cyberoam.

En la foto el ganador del premio mayor del Seminario de Seguridad Informática Perimetral, una Tablet de última tecnología.



Fuente: Marina Sabando Jefe de Marketing SCProgress.

