BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 15 de mayo de 2015.- El Instituto Nacional de Ciberseguridad (INCIBE) tiene como misión reforzar la ciberseguridad, la confianza y la protección de la privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, red académica, Administración, al sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general. INCIBE elabora para los medios informativos un boletín semanal de Seguridad, con el fin de colaborar conjuntamente en la difusión de la Seguridad de la Información.

Principales informaciones de INCIBE entre el 8 y el 15 de mayo de 2015.

Concurso: celebra el Día de Internet 2015 de una manera segura

Un año más, INCIBE se suma al **Día de Internet 2015**, una fecha celebrada a nivel mundial todos los 17 de mayo que pretende promover el uso de Internet y las nuevas tecnologías, especialmente entre los colectivos menos familiarizados con ellas.

Aprovechando esta fecha, INCIBE, en su objetivo por mejorar la ciberseguridad de los usuarios en Internet, recomienda en su página web seguir una serie de medidas para hacer un uso responsable de los dispositivos tecnológicos.

Por otra parte, se ha puesto en marcha el concurso **#NavegaConChaleco**, en su perfil de la red social Twitter, en el que cualquier usuario registrado en ella puede participar subiendo una foto de su mascota interactuando con algún dispositivo tecnológico. Para ello deberá seguir a **@INCIBE** en dicha red social y publicar un tweet con el hashtag de la campaña (#NavegaConChaleco) y la foto de su mascota. La imagen más ingeniosa, creativa, divertida y artística ganará el concurso.

Desde INCIBE os animamos a participar en esta iniciativa y así poder optar al premio del concurso, un iPad Mini 2 de 16 GB. Se pueden consultar las bases del concurso a través del siguiente documento.

comunicacion@incibe.es

www.incibe.es

Av. José Aguado 41 / 24005 León
T. (+34) 987 877 189 / F. (+34) 987 261 016

BOLETÍN INFORMATIVO

¡Aviso! Mucho cuidado con los tweets promocionados

Una vez más, la ingeniería social, está siendo utilizada para llevar a cabo acciones poco lícitas a través de las redes sociales, en este caso, en Twitter. Como indicábamos al comienzo del aviso, se han detectado varios tweets promocionados en la red social que bajo la excusa de conseguir un drone a 2 euros, están consiguiendo que los usuarios acaben suscritos a un servicio cuya cuota mensual es de 79,99 euros. Se trata de publicidad engañosa ya que durante todo el proceso que el usuario debe seguir para obtener el supuesto drone, se le indica que el coste es de sólo 2 euros en grandes banners, cuando en realidad, la "letra pequeña", recoge los detalles del pago de la cuota mensual. Por tanto, ya no estamos hablando de un drone a 2 euros.

¿Tienes dispositivos zombis en tu empresa?

¿Últimamente has notado que en tu empresa los ordenadores van más lento de lo normal, el ventilador hace mucho ruido aún cuando no lo estás utilizando y algunas aplicaciones han dejado de funcionar correctamente? Estos síntomas podrían ser debidos a que ese ordenador de tu empresa se ha convertido en un pc "zombi". ¿Eso qué significa? Que hay alguien, aparte de ti, que está controlando tu ordenador sin que seas consciente de ello, y esto supone un riesgo para tu principal activo: la información.

Esto quiere decir que alguien, sin estar físicamente delante de tu ordenador, y con los conocimientos técnicos suficientes, puede manejarlo a su antojo. Pero eso no es todo, si tu ordenador es un zombi, estará formando parte de una red zombi de ordenadores, más conocido por el término anglosajón botnet, que no es más que un gran número de ordenadores zombi, infectados con el mismo tipo de virus, que están controlados por una misma persona u organización criminal.

¿Qué es ese candado de la barra de direcciones?

Las páginas web representan a entidades oficiales o empresas reconocidas en las que confiamos. Pero en Internet no todo lo que vemos es lo que parece. Entonces, ¿cómo comprobar que la página que visitamos es realmente la que dice ser?

Del mismo modo que los documentos físicos contienen sellos o firmas que los autentifican como originales, las páginas web también

disponen de mecanismos que confirman su autenticidad. Entre estos mecanismos están los **certificados digitales**, archivos que las dotan de una seguridad adicional y proporcionan información veraz al visitante acerca de su origen.

¿Sabes lo que es el malvertising y cómo estar protegido frente a él?

Cada vez más los usuarios estamos al día en lo que a virus y formas de protegernos se refiere y por ello los atacantes se reinventan para seguir infectándonos. Así llegó el malvertising, ¿sabes cómo seguir protegido?

¿Qué es el malvertising?

El malvertising no es más que otra técnica para intentar infectar nuestros equipos. El nombre de esta práctica viene de las palabras "*malicious advertising*" (publicidad maliciosa) y lo que hace es esconder malware para infectar nuestros dispositivos en los espacios de publicidad de otras páginas webs, ahora veremos cómo funciona.

Pero para entender bien que es el malvertising debemos saber qué es el adware, que es su hermano mayor.

Correos y Telégrafos NO te ha enviado ninguna notificación

Debido a la gran cantidad de usuarios afectados por los correos fraudulentos que se hacen pasar por el servicio de Correos y Telégrafos, nos vemos en la obligación de alertar nuevamente de este problema con el fin de que el mayor número de personas esté informado. Es muy importante difundir este aviso de seguridad entre todos nuestros conocidos ya que de lo contrario, las personas que caigan en la trampa, además de infectar sus dispositivos con un malware, perderán toda la información que en ellos almacene, así como la de las unidades de red mapeadas, pendrives conectados, etc. Esta pérdida se produce ya que el malware cifra gran cantidad de ficheros como imágenes, documentos de ofimática, etc. de modo que en el caso de no disponer copias de seguridad almacenadas en dispositivos externos aislados, en la mayoría de los casos prácticamente imposible recuperar la información.

BOLETÍN INFORMATIVO

Si tiene cualquier problema de seguridad, INCIBE y la Oficina de seguridad del Internauta OSI le ofrecen los siguientes servicios gratuitos: boletines gratuitos de seguridad, el asistente de seguridad y el servicio de atención telefónica (901 111 121). Para más información en materia de ciberseguridad visite: INCIBE www.incibe.es y OSI http://www.osi.es/

comunicacion@incibe.es

www.incibe.es

Av. José Aguado 41 / 24005 León
T. (+34) 987 877 189 / F. (+34) 987 261 016