BOLETÍN INFORMATIVO

INCIBE –INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 13 de enero de 2017.- 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 6 y el 12 de enero de 2017.

Borrar tu identidad online no es imposible

Por lo general no somos conscientes de la gran cantidad de información personal que circula por la red. Borrar esa información puede convertirse en un problema pero es posible eliminar esta información. Esta semana ofrecemos los pasos a seguir para eliminar la información concreta de un sitio, eliminar una cuenta o eliminar nuestra identidad completa. Borrar nuestros datos de Internet puede ser más simple o complejo en función de nuestra actividad o el tipo de información y los sitios donde se encuentre alojada, pero el derecho al olvido está para defendernos cuando pueda afectarnos de forma negativa.

Aumenta la protección de tu cuenta de Google con la llave de seguridad

Usar la “verificación en dos pasos” de Google implica añadir más seguridad a tu cuenta, y por extensión, a todos los servicios que esta nos ofrece, tales como el correo Gmail, Youtube, etc. Además de hacer uso de los códigos de verificación a través del móvil, puedes añadir una capa extra de protección activando una llave de seguridad y así garantizar al máximo la integridad de tu cuenta. ¿Sabes cómo obtener una llave de seguridad y cómo añadirla a una cuenta de Google?

comunicacion@incibe.es

www.incibe.es

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

¿Cómo nos engañan por correo electrónico?

La herramienta digital de trabajo más utilizada por las pymes y autónomos es el correo electrónico, con el fin de comunicarse con clientes, empleados y colaboradores. Muchos de los incidentes que sufren las empresas tienen su origen en los engaños que utilizan técnicas de ingeniería social a través de este medio de comunicación. Pero ¿cómo consiguen engañar al usuario a través del correo electrónico? En primer lugar intentando confundir al usuario para que crea que el correo procede de alguien de confianza, posteriormente pueden o bien conseguir que se haga clic en un enlace con destino malicioso o se descargue un fichero que lleva malware.

Consejos para hacer un uso seguro del correo corporativo

En un correo malicioso tanto el remitente como el asunto, el cuerpo, los adjuntos o los enlaces que contiene, pueden estar diseñados para engañarnos. Por esto es importante, estar atentos a ellos, utilizar el sentido común y analizarlos de forma crítica para evitar caer en su trampa. Prestar atención al remitente, el asunto, los elementos que hay en el cuerpo del mensaje, si lleva adjuntos o no y el tipo de enlaces que se emplean son algunas de las cosas que debemos tener en cuenta para identificar si un correo electrónico lleva un fraude detrás o no.

Actualización de seguridad de WordPress

WordPress ha publicado esta semana una nueva versión de su gestor de contenidos que, aparte de corregir varios errores de código, soluciona varios problemas de seguridad que afectan a las versiones anteriores. Para solucionar posibles problemas de seguridad, se recomienda tener siempre actualizado todo el software a las últimas versiones. Antes de realizar ninguna actualización del gestor de contenidos, se recomienda realizar una copia de seguridad de la base de datos y de todos los ficheros que componen el sitio web. También es importante comprobar que la copia se ha realizado correctamente y que podemos recuperarla.

Expertos alertan de un ataque masivo a MongoDB

La bitácora de ciberseguridad de INCIBE ha recogido esta semana el ataque masivo de ransomware a servicios con bases de datos

comunicacion@incibe.es
www.incibe.es
Av. José Aguado 41 / 24005 León
T. (+34) 987 877 189 / F. (+34) 987 261 016

MongoDB. Debido a una incorrecta configuración de MongoDB, los atacantes pudieron conectarse a las bases de datos expuestas en Internet y robar o bloquear el acceso a las mismas, pidiendo un rescate en bitcoins a los responsables de las bases de datos. Las estimaciones de los expertos calculan más de 27.000 servidores con MongoDB afectados.

Para más información en materia de Ciberseguridad visite INCIBE www.incibe.es, Protege tu Empresa https://www.incibe.es/protege-tu-empresa 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