BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 16 de diciembre de 2016.- 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 9 y el 15 de diciembre de 2016.

Confirmado un nuevo robo de datos en Yahoo. Cambia tu contraseña

Yahoo ha lanzado un comunicado en el que informa que los datos de más de 1.000 millones de cuentas de usuario fueron robados, por lo que se recomienda cambiar la contraseña y la pregunta/respuesta de seguridad. El pasado mes de septiembre INCIBE ya informó sobre un incidente similar en la misma compañía.

Emails fraudulentos que suplantan al Banco Santander

Se ha detectado una campaña de phishing a través de correos electrónicos fraudulentos que simulan proceder del Banco Santander, con el objetivo de obtener las claves de acceso a la banca online e información bancaria de las víctimas.

Si el usuario ha sido víctima de este fraude, el primer paso es modificar inmediatamente su contraseña de acceso al área de clientes del Banco Santander y contactar con su oficina bancaria para informarles de lo sucedido con su cuenta online y con los datos de su tarjeta de crédito.

Antes de ver las fotos analiza los archivos, podrían infectarte

Detectada una campaña fraudulenta que intenta infectar el equipo mediante un archivo adjunto que aparenta ser una fotografía. Si un usuario recibido el correo pero no ejecuta el archivo adjunto, su equipo no se habrá infectado. No obstante, conviene permanecer atento, eliminando os emails con asuntos similares al descrito, no

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

descargando o ejecutando posibles ficheros adjuntos y realizando copias de seguridad frecuentes.

Un nuevo phishing a Apple que quiere robarte tu ID y tu tarjeta de crédito

Desde los sistemas de detección de INCIBE se ha identificado una campaña de phishing que suplanta a Apple con la intención de obtener información personal y bancaria de la víctima. El correo electrónico advierte al usuario que la información de su cuenta es incorrecta o incompleta y que debe solucionarlo.

El phishing ya es detectado por los navegadores de PC avisando al usuario que está accediendo a un sitio posiblemente fraudulento, pero en las versiones de Chrome y Safari para smartphone no lo advierten, por lo que el usuario podría caer en la trampa.

El carro de Navidad gratis que te llega al móvil te puede salir caro, muy caro

Han sido detectados mensajes SMS fraudulentos “Smishing” que comunican al receptor que su número de teléfono ha sido elegido para obtener un “Carro de Compra Navideña” valorado en 1000€. En el SMS invita al usuario a que llame a un número de tarificación especial 806, supuestamente para obtener el premio. La recomendación es que nunca se llame a este tipo de teléfonos para solicitar o responder a ofertas de productos comerciales. Para evitar que hagan cargos elevados en tu factura telefónica si por error, despiste o desconocimiento accedemos a las peticiones del SMS, la recomendación es contactar directamente con la operadora y solicitar el bloqueo a los números de tarificación especial.

Nuevo Servicio Antiransomware, recupera el control de tu información

INCIBE pone a disposición de los usuarios el nuevo Servicio Antiransomware con el que cualquier víctima de este tipo de malware podrá contactar con expertos que intentarán solucionar su problema.

El ransomware es un tipo de malware que “secuestra” el equipo al que afecta impidiendo su uso normal. Este tipo de malware lo que hace es bloquear el ordenador al que infecta o impedir el acceso a los recursos (archivos, fotos, vídeos, etc.) cifrándolos. El objetivo de los ciberdelincuentes es totalmente económico, si la victima quiere volver a recuperar el control de su equipo tiene pagar un “rescate”, que por otro lado, no es ninguna garantía.

BOLETÍN INFORMATIVO

Configurando tu privacidad en Windows 10

El blog de la Oficina de Seguridad del Internauta (OSI) recoge esta semana un artículo que acerca al usuario las distintas opciones para configurar en el sistema operativo Windows 10 uno de los principales aspectos de la ciberseguridad, la privacidad.

El objetivo del texto es mostrar al usuario cómo minimizar al máximo la recogida de información personal en Windows 10, lo que podría afectar a algunas funcionalidades por lo que siempre debe ser el usuario quien decide qué información compartir y cuál no hasta llegar al equilibrio entre funcionalidad y privacidad.

Películas y series para hablar de Internet con niños y adolescentes

En ocasiones hay temas que resultan difíciles de explicar a los niños y adolescentes. ¿Por qué no utilizar películas y series para hablar de cuestiones como ciberacoso, sexting o protección en Internet? Esta semana proponemos algunos contenidos audiovisuales para trabajar los riesgos de Internet de forma dinámica y atractiva para menores de todas las edades, materiales a nuestro alcance para favorecer el buen uso de Internet entre niños y adolescentes.

Prevención de ciberriesgos laborales en el puesto de trabajo

¿Las empresas hacen lo necesario para prevenir los ciberriesgos a la hora de contratar a un nuevo empleado? Si una empresa utiliza en mayor o menor medida internet o las tecnologías de la información y comunicación, es decir, ordenadores, tabletas, móviles, etc., parece lógico que sea también necesario concienciar a los empleados sobre los ciberriesgos, para él y para la empresa, y de cómo evitarlos. No menos importante es que conozcan los mecanismos de seguridad (cifrado, autenticación, *backup*, etc.) y cómo aplicarlos.

¿Estás preparado para hacer frente a un ciberincidente?

Saber qué hacer en caso de incidente va suponer una diferencia importante en cuanto a las pérdidas económicas y de imagen de una empresa. Si está preparada, podrá frenar el incidente y recuperarse antes. Así sus consecuencias serán menores. Algunas preguntas que tendrá que hacerse si quiere estar preparada para responder a incidentes pasan por saber qué elementos tiene que proteger o tener un listado de posibles incidentes, saber quién se va a hacer cargo de las decisiones que hay que tomar, entre otras.

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

BOLETÍN INFORMATIVO

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