BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 08 de abril 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 01 y el 07 de abril de 2016.

Suplantan a Apple para intentar robarte credenciales y la tarjeta de crédito

La Oficina de Seguridad del Internauta (OSI) ha detectado una campaña de correos electrónicos fraudulentos (phishing) suplantando a la entidad Apple. El mensaje del email alerta a los usuarios que tienen 48 horas para verificar su información de iCloud o de lo contrario, su cuenta será cerrada. El objetivo es robar el usuario y la clave de acceso al servicio además de información personal y datos bancarios.

Si un usuario ha recibido un correo de estas características, ha accedido al enlace y facilitado su Apple ID y contraseña, debe modificar lo antes posible su contraseña de acceso al servicio de iCloud. En caso de haber introducido su información bancaria, debe contactar con tu banco para informarles de lo sucedido.

No es certificado bueno todo lo que reluce

Es importante cuando navegamos por Internet saber en qué web estamos, y eso, nos lo indica la URL. Pero a veces, no queda demasiado claro debido a que éstas son complejas. Entenderlas es muy importante ya que depende la seguridad de nuestros datos.

El número de internautas crece de forma constante, esto implica un crecimiento del número de usuarios de servicios que ofrece la red,

entre ellos: correo electrónico, redes sociales, servicios para dispositivos móviles, comercio electrónico, banca electrónica, etc. Todos ellos tienen en común el uso de nombres de usuario, contraseñas, datos personales y en algunos casos datos financieros (tarjetas de crédito, cuentas bancarias, medios de pago…).

Navegación anónima, ¿es posible?

Hablamos de navegación anónima a la posibilidad de acceder a sitios en Internet sin que se pueda identificar a la persona o dispositivo que está accediendo a los servicios que se conecta (webmail, páginas, etc.), no nos referimos a la privacidad en general, sino a la parte de identificación.

En España para cada línea de conexión hay identificado un titular. La legislación española obliga a ello a través de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (al igual que los registros de llamadas, conexiones a internet etc.). Esto implica que el ISP (Proveedor de Servicios de Internet) conoce el titular de cada línea.

Uso seguro de aplicaciones de gestión educativa, ¿qué debemos saber?

Las aplicaciones de gestión educativa son imprescindibles en la vida cotidiana de colegios e institutos. Las usamos en la sala de profesores, en casa, en el móvil… pero, ¿lo hacemos de manera segura?, ¿cuán importantes son los datos que gestionamos en ellas?

Quienes trabajan en educación saben perfectamente que el día a día de un centro educativo no es sólo dar clases y tener muchas vacaciones… Siempre hay cuestiones que tratar y necesidades que atender tanto a nivel académico, de convivencia, coordinación del profesorado, comunicación con familias, cumplimiento de requisitos de la administración educativa, gestión económica, mantenimiento… Afortunadamente contamos con la ayuda de alguna de las múltiples herramientas informáticas de gestión educativa que hay en el mercado.

BOLETÍN INFORMATIVO

Caso de éxito: un comercial de telefonía

Hoy te descubrimos el caso de un comercial que es consciente de la importancia de tener un entorno seguro de trabajo y de la necesidad de proteger su información de trabajo ante posibles imprevistos como la pérdida o robo de sus dispositivos.

Nuestro comercial está gran parte de su jornada laboral fuera de su oficina, viajando y asistiendo a reuniones de negocios con sus clientes. Está concienciado de los riesgos que supone trabajar de esta forma para sus dispositivos y la información de trabajo que maneja. Seguro que conoces a alguien que se ha dejado olvidado un móvil en un taxi o un portátil en el tren (o incluso que se lo han robado)

Por ello, nuestro comercial, ha puesto en práctica una serie de medidas destinadas a proteger sus dispositivos móviles de trabajo y la información que contienen.

Historias reales: ¡Mi nueva conexión de red va fatal!

Marisa es la dueña de una boutique de moda de gran éxito en su ciudad. Es un pequeño comercio familiar que ya regentaron su madre y su abuela con el mismo éxito.

Hace un tiempo decidió que era hora de modernizar su negocio introduciendo algunos cambios, como la implantación de un nuevo sistema de gestión de inventario. Para ello, adquirió unas tabletas para que los empleados pudieran leer el código de barras de las prendas y, así, acceder a toda la información referente a ellas en la aplicación centralizada de inventario.

incibe_
2005-2015
TRABAJANDO POR LA CONFIANZA DIGITAL

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