

## **INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD**

León, 17 de junio 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 10 y el 16 de junio de 2016.

### **Vulnerabilidad crítica sin parche en Adobe Flash Player**

La Oficina de Seguridad del Internauta (OSI) informa de un aviso de seguridad emitido por Adobe reportando la existencia de una vulnerabilidad crítica, del tipo 0day, en Adobe Flash Player.

Este fallo de seguridad no ha sido descrito completamente para no dar oportunidad a grupos de ciberdelincuentes a que se aprovechen de esta vulnerabilidad con propósitos maliciosos.

Sin embargo, lo que se conoce, es que a través de este nuevo fallo un atacante puede tomar el control remoto de un dispositivo y realizar cualquier acción como por ejemplo instalar malware.

### **Copias de seguridad en Windows, esas grandes desconocidas.**

En nuestro ordenador tenemos una serie de ficheros que no valoramos de forma adecuada hasta que los perdemos. Actualmente, con el ransomware llamando a nuestro email, día sí día también, las copias de seguridad no son una opción, son una necesidad.

Lo mismo que los smartphones contienen una gran cantidad de datos personales que nos importan, de igual modo ocurre con los ordenadores. En estos suelen convivir: ficheros personales, copias de seguridad de móviles, fotos de cámaras y en algunos casos ese ordenador contiene ficheros de trabajo. La pérdida de estos datos

podría traernos problemas serios por ello, las copias de seguridad son la única forma de garantizar que no se van a perder los datos.

### **Big Data: cómo afecta a los usuarios**

Cada día se habla más sobre el Big Data y lo beneficiosa que puede ser esta técnica de análisis de la información en diferentes aspectos de nuestra sociedad, pero ¿sabes cómo te afecta como usuario? Y ¿cómo minimizar su impacto?

Actualmente, en muchas empresas uno de los activos más valiosos que tienen es la información que poseen, ya que como dice la famosa cita de Francis Bacon «la información es poder» y las empresas son cada vez más conscientes de este hecho.

La llegada de Internet y la enorme cantidad de dispositivos que están continuamente conectados a la red ha ayudado a aumentar de modo exponencial el volumen de información que los usuarios generamos y esa información es realmente “el activo” del siglo XXI.

### **Historia real: “Pedí un préstamo a un falso banco, e intentaron estafarme hasta tres veces...”**

Daniel tenía un problema de liquidez, y decidió pedir un préstamo a un banco. Necesitaba 4000 € para reparar su camión, al ritmo que estaba trabajando lo podría devolver en 6 meses perfectamente. El inconveniente es que no disponía de bienes a su nombre, y como era autónomo tampoco tenía una nómina para avalarlo, de forma que buscó en Internet alguna otra opción para el préstamo.

Encontró varias personas que ofrecían préstamos personales en un portal de anuncios, así que se puso en contacto con el que mejores condiciones le ofrecía.

### **¡Oh, no!, me toca ser el coordinador TIC, ¿por dónde empiezo? (III), la red wifi**

Sí, tenemos Internet en el centro y podemos conectarnos vía wifi, pero ¿sabemos cómo configurar dicha red de manera segura?, ¿somos conscientes del riesgo que corremos si no lo hacemos así? En este artículo veremos paso a paso qué tenemos que hacer para disfrutar en el centro de una wifi sin problemas.

## 7 cuestiones para usar el móvil de forma segura en la pyme (1/2)

Los móviles y las tabletas no son más que ordenadores de pequeño tamaño que podemos llevar en el bolsillo. Han invadido nuestras vidas y han llegado para quedarse, tanto para su uso personal como profesional.

Como cualquier ordenador, puede contener información personal y de trabajo; nos da acceso a nuestras cuentas (correo, redes sociales, banca online, suscripciones,...) y ahora se está convirtiendo en un medio de pago. Nos permite navegar en internet y utilizar todo tipo de aplicaciones.

Pero, también, como cualquier ordenador, puede infectarse con malware (comúnmente conocido como virus) e incluso formar parte de una botnet. Te proponemos que te hagas las siguientes preguntas para hacer un uso inteligente de estos dispositivos.

## 7 cuestiones para usar el móvil de forma segura en la pyme (2/2)

En el post anterior planteábamos algunas cuestiones para verificar si utilizas el móvil para el trabajo de forma segura: ¿cómo tratas los dispositivos móviles?, ¿cómo configuras la seguridad del dispositivo?, ¿qué puedes hacer para proteger tu información del dispositivo móvil?, y ¿qué precauciones has de tomar cuando utilizas apps?

A continuación veremos los riesgos de utilizar algunas funcionalidades de los dispositivos móviles, la protección ante el malware y las precauciones cuando nos conectamos a wifis de dudosa seguridad.



Si tiene cualquier problema de seguridad, [INCIBE](http://www.incibe.es) y la Oficina de seguridad del Internauta [OSI](http://www.osi.es) 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](http://www.incibe.es) y OSI <http://www.osi.es/>