El CCN-CERT publica su informe de Buenas Prácticas CCN-CERT BP-03/16 con un decálogo de seguridad con los principales puntos a tener en cuenta

Cómo usar nuestro móvil de forma segura y evitar ciberataques

- **España, uno de los países con una mayor penetración de teléfonos inteligentes, es uno de los más afectados por el creciente número de ataques, cada vez más complejos y sofisticados.**

- **El documento ofrece un conjunto de pautas y recomendaciones para mitigar posibles ataques, dando a conocer las técnicas y los recursos más utilizados por los atacantes para conseguir infectar un dispositivo móvil u obtener información personal de la víctima.**

Madrid, 20 de octubre de 2016.- Actualizar siempre el sistema operativo y las aplicaciones del dispositivo móvil (que deberían descargarse siempre de fuentes de confianza), realizar copias de seguridad periódicas del contenido que se desea proteger, evitar conectarse a redes Wi-Fi públicas abiertas y rechazar permisos innecesarios en las *apps* son algunas de las principales recomendaciones que el Centro Criptológico Nacional (CCN) realiza en su Informe **CCN-CERT BP-03/16 Buenas Prácticas en Dispositivo móviles** recién publicado.

"Los dispositivos móviles son utilizados tanto en las comunicaciones personales, como en las profesionales, privadas y relevantes, y para el almacenamiento e intercambio de información sensible"

El documento, el segundo de una serie de informes destinados a un público general que busca concienciar y facilitar el uso seguro de las tecnologías de la información y las comunicaciones, se centra precisamente en uno de los segmentos en los que se observa un mayor incremento en el número de ataques y de robo de información y, por el contrario, menor percepción de peligro tienen sus usuarios. Máxime, teniendo en cuenta que los dispositivos móviles son utilizados tanto en las comunicaciones personales, como en las profesionales, privadas y relevantes, y para el almacenamiento e intercambio de información sensible.

La mayor parte de los ejemplos del Informe hacen referencia a las dos plataformas más utilizadas en estos momentos: Android (Google) e iOS (Apple) y en él se pueden encontrar epígrafes dedicados a la pantalla de bloqueo, las comunicaciones a través de USB, la actualización del sistema operativo y de las aplicaciones, el cifrado del dispositivo móvil, las copias de seguridad o la gestión remota del dispositivo.

El **CCN-CERT BP-03/16** incluye además un apartado sobre las capacidades de comunicación inalámbricas, las aplicaciones móviles (apps) u otras recomendaciones de

seguridad de carácter genérico (tanto desde el punto de vista corporativo como personal) junto con un decálogo de recomendaciones.

	Decálogo de seguridad de los dispositivos móviles
1	El dispositivo móvil debe de estar protegido mediante un código de acceso robusto asociado a la pantalla de bloqueo (o en su defecto, una huella dactilar digital). El código de acceso debe ser solicitado inmediatamente tras apagarse la pantalla, que debería de bloquearse automáticamente lo antes posible si no hay actividad por parte del usuario. No se debe dejar el dispositivo móvil desatendido sin bloquear.
2	Se debe hacer uso de las capacidades nativas de cifrado del dispositivo móvil con el objetivo de proteger todos los datos e información almacenados en el mismo.
3	El sistema operativo del dispositivo móvil debe estar siempre actualizado, al igual que todas las aplicaciones móviles (*apps*).
4	No conectar el dispositivo móvil a puertos USB desconocidos y no aceptar ninguna relación de confianza a través de USB si no se tiene constancia de estar conectando el dispositivo móvil a un ordenador de confianza.
5	Deshabilitar todos los interfaces de comunicaciones inalámbricas del dispositivo móvil (NFC, Bluetooth y BLE, Wi-Fi, servicios de localización, etc.) que no vayan a ser utilizados de forma permanente por parte del usuario. Deberían habilitarse únicamente cuando vayan a ser utilizados, y volver a deshabilitarse al finalizar su uso.
6	No conectar el dispositivo móvil a redes Wi-Fi públicas abiertas (o *hotspots* Wi-Fi) que no implementan ningún tipo de seguridad.
7	No instalar ninguna aplicación móvil (*app*) que no provenga de una fuente de confianza, como los mercados oficiales de *apps* (Google Play, App Store, etc.).
8	Se recomienda no otorgar permisos innecesarios o excesivos a las *apps*, limitando así los datos y la funcionalidad a la que éstas tendrán acceso.
9	Siempre que sea posible se debe hacer uso del protocolo HTTPS (mediante la inserción del texto "https://" antes de la dirección web del servidor a contactar). Nunca se debería aceptar un mensaje de error de certificado digital inválido.
10	Se deben realizar copias de seguridad (*backups*) periódicas, y preferiblemente automáticas, de todos los contenidos del dispositivo móvil que se desea proteger y conservar.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

20 de octubre de 2016

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/