BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 12 de junio de 2015.- 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 5 y el 11 de junio de 2015.

Aviso de app fraudulenta para usuarios de Apple

La ingeniería social es utilizada por los delincuentes para intentar engañarnos de muchas formas diferentes con el objetivo de acceder a información privada, infectar el ordenador con algún tipo de virus, robar datos bancarios, etc. En esta ocasión, un fallo de seguridad en la aplicación Mail puede ser utilizado por ciberdelincuentes para enviar correos maliciosos capaces de hacer creer a los usuarios, que es necesario que introduzcan su nombre de usuario y contraseña de iCloud. Es posible ver un vídeo ilustrativo de cómo el fallo podría ser utilizado con intenciones maliciosas:

El email contiene código especialmente diseñado para mostrar un cuadro de diálogo que solicite al usuario diferentes credenciales de acceso como por ejemplo, para acceder al servicio iCloud.

Cuando el usuario introduce los datos, pueden enviarse a una web (un servidor web) completamente ajeno a Apple, de modo que ser pierde el control sobre los mismos y pueden ser utilizados por los ciberdelincuentes para llevar a cabo conductas maliciosas (robo de identidad, robo de información, entre ellas). Incluso, el ataque puede desarrollarse de manera que el usuario reciba un mensaje de confirmación después de introducir su contraseña en el cuadro de diálogo aparecido en el correo electrónico, y así le haga creer que todo va bien.

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

BOLETÍN INFORMATIVO

Oleada de falsas facturas con malware

Se ha identificado una campaña activa de correos fraudulentos que utilizan la ingeniería social para instalar malware en los ordenadores de los usuarios que sean víctimas del engaño. Esta vez, como en otras ocasiones, el pretexto utilizado por los ciberdelincuentes es el envío de una supuesta factura que bajo su inocente apariencia esconde malware.

Si has recibido un correo de estas características y has descargado y ejecutado el fichero, es posible que el ordenador se haya infectado con un malware. Es importante analizarlo con un antivirus para comprobar si estás infectado y de ser así, poder desinfectarlo lo antes posible para evitar problemas de seguridad.

El riesgo de andar escaneando códigos QR cómo locos

Los códigos QR son esos recuadros con manchas negras que tras escanearlos con la cámara de un smartphone o tableta, nos llevan hasta una página web. En ocasiones, son muy útiles, pero es necesario conocer previamente los riesgos a los que nos expone.

Ya estamos acostumbrados a ver códigos QR en muchos sitios: carteles informativos, billetes de avión, entradas de un evento, revistas e incluso en invitaciones de boda para que los amigos y familiares visiten la página web que los novios han creado con todos los detalles de la boda. La verdad es que, gracias a los teléfonos móviles que manejamos hoy en día (smartphones), todo parece que es mucho más fácil, ¡ya no es necesario ni tener que teclear una URL en el navegador del teléfono! Escaneando un código QR con una simple aplicación móvil, accedemos directamente a la página web.

¡Sigue sin actualizar y mira lo que te puede ocurrir!

Una de las medidas básicas en la seguridad de nuestros dispositivos es mantenerlos actualizados. Si no lo hacemos, las consecuencias pueden ser graves para nuestra información. Conciénciate, protégete de riesgos innecesarios y actualiza.

Lo hemos escuchado infinidad de veces, debemos mantener nuestros dispositivos actualizados. Aun así, a veces no lo cumplimos por diferentes motivos: falta de tiempo, pereza, que el equipo se

ralentiza cuando instalamos las actualizaciones, que ocupan mucho espacio… En definitiva, siempre encontramos alguna excusa para no tener nuestros dispositivos actualizados.

¿Tienes una tienda online? Conoce las claves para detectar una compra fraudulenta

¿Quién no conoce los beneficios del comercio electrónico? Total disponibilidad horaria, 24 horas al día durante los 7 días de la semana, la posibilidad de trasladar el alcance del negocio de un ámbito local a uno global, entre otros muchos. Los mercados se han transformado en globales y digitales en poco tiempo. Las antiguas reglas, las leyes y las normas se quedan escasas y es necesario reformularlas. Las fronteras se están difuminando, aparece el «prosumidor» (productor-consumidor) y las iniciativas crowd (crowdsourcing, crowdfunding,...), cambia la preocupación por la privacidad, etc. El mercado ha evolucionado, se ha hecho 3.0.

¿Qué factores pueden amenazar la reputación online de nuestra empresa?

¿Hay datos, imágenes, registros, noticias o comentarios sobre tu empresa en Internet? Todo el conjunto de este tipo de información es definido como identidad digital corporativa y conforma una descripción de la organización desde los puntos de vista humano, de negocio y digital.

Pero dentro de este conjunto de información sobre nuestra empresa ¿hemos analizado valoración que hacen los usuarios? Es decir, ¿sabemos lo que opinan los usuarios sobre nosotros en Internet? ¿Conocemos nuestra reputación online?

Tan importante es la investigación (qué ocurrió) como la monitorización (qué está ocurriendo) sobre nuestra reputación. Debemos gestionar nuestra reputación online para hacer frente a las diferentes amenazas que pueden generar impactos negativos en la imagen de la compañía.

BOLETÍN INFORMATIVO

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