BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 22 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 15 y el 21 de abril de 2016.

Falsos vales descuento de Carrefour quieren robarte datos personales

La Oficina de Seguridad del Internauta ha detectado una nueva campaña fraudulenta que ofrece supuestos vales descuento de la cadena de supermercados Carrefour y cuyo objetivo es obtener datos personales de los usuarios.

Los mensajes de esta nueva campaña están llegando por correo electrónico, invitando a la víctima a realizar una falsa encuesta para entrar en el sorteo de un cheque regalo de la cadena de supermercados Carrefour.

Una vez se hace clic en el enlace que llega en el correo electrónico, el usuario es conducido a rellenar un formulario web en el que solicitan datos personales para poder participar en el sorteo del supuesto vale descuento.

Que no te engañen con las videollamadas de Whatsapp

La OSI también ha lanzado un aviso esta semana de una campaña que ofrece fraudulentamente un supuesto servicio de videollamadas para Whatsapp. Los mensajes de esta nueva campaña ofrecen a los usuarios activar videollamadas para este sistema de mensajería instantánea.

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

BOLETÍN INFORMATIVO

La promoción fraudulenta se propaga a través de redes sociales en teléfonos móviles (no es posible acceder a las mismas desde un ordenador), con mensajes que contienen un enlace que dirige a una web (wsx.xo) que trata de suplantar la identidad de Whatsapp.

Una vez en la web, si el usuario pincha en “Activar Videollamadas ahora”, aparecerán pantallas que simularán estar “verificando la versión de WhatsApp” del usuario o generando algún tipo de falsas actualizaciones.

Nuevo phishing: atento si eres usuario de ING Direct

Se ha detectado correos electrónicos que simulan proceder del banco ING Direct y están dirigidos a robar los datos de acceso de usuarios a la banca online de esta entidad.

Los mensajes de estas nueva campaña simulando proceder de ING Direct (phishing), indican a los usuarios que su última sesión en banca online no finalizó de manera correcta y solicitan que termine la sesión de inmediato. Para ello, deben pulsar sobre el enlace “entre aquí” incluido en el texto del correo electrónico.

PNFC: Posible Nuevo Fraude en "Credit Cards"

La tecnología NFC se está extendiendo en gran medida por la comodidad que supone para la realización de micropagos, por lo general cantidades de menos de 20/50€ pero ¿Conocemos los posibles riesgos de esta tecnología y cómo mitigarlos

En numerosas ocasiones os hemos informado acerca del uso seguro de las tecnologías inalámbricas que están disponibles en casi todos los smartphones y tablets cuando nos referimos a las conexiones wifi y bluetooth. Además muchos de los dispositivos también cuentan con otras tecnologías “sin cables” como es la NFC (Near Field Communication).

Ésta también se encuentra disponible en otro tipo de soportes, como las tarjetas utilizadas en diversos ámbitos: bonos de transporte, la versión 3.0 de nuestro DNI, acceso a servicios locales, y por supuesto, tarjetas de crédito.

BOLETÍN INFORMATIVO

Certificados electrónicos personales, esos grandes desconocidos

El uso de Internet genera una necesidad importante, identificar de manera inequívoca a la persona, de tal forma que una persona pueda demostrar su identidad y pueda firmar un documento con la misma validez legal que una firma manuscrita.

En la mayoría de servicios que usamos de Internet como es el caso del correo electrónico o las redes sociales, no es necesario identificarnos de forma real y, aunque no es lo que recomienda, esto provoca que algunos usuarios en sus datos de perfil pongan datos falsos: nombre, apellidos, dirección, fecha de nacimiento, etc.

Escuela Cibersegura: ¿Cómo detecto un caso de ciberacoso en clase?

Entre las diferentes consultas que nos hacen los profesores, ya sea por correo o en algún encuentro con ellos, destaca la necesidad de detección de problemas, especialmente en lo referido al acoso y ciberacoso. Por eso es necesario tratar el cómo saber si en nuestra aula hay algún caso de este tipo.

Hay diferentes publicaciones (muy completa y recomendable la Guía de actuación contra el ciberacoso) que ponen el foco en síntomas de diferente índole, incluyendo síntomas físicos que por norma general son psicosomáticos. Pero los que nos parecen más fiables siempre son los de comportamiento y relaciones, o al menos no centrarnos en los que aparentando ser síntomas físicos suelen estar muy ligados a otras situaciones y nos pueden llevar a confusión.

Historias reales: Fuga de información en un equipo de motociclismo

Alfonso gestiona un taller de motos donde hace todo tipo de reparaciones. A parte dirige una escudería de motos, aprovechando las instalaciones del taller para realizar el diseño y fabricación de las piezas de las motos de carreras.

Desde el año pasado ha estado investigando y desarrollando unas mejoras en el chasis de sus motos que les están permitiendo ganar muchas carreras esta temporada.

BOLETÍN INFORMATIVO

El trabajo de desarrollo de la mejora mecánica de sus motos los realiza, junto a su equipo de mecánicos, desde el ordenador de trabajo del taller. Aquí almacena toda la información del taller y de la escudería.

Con la movilidad y la nube, ¿dónde está el perímetro?

La transformación digital impone nuevas formas de interacción con los clientes y nuevas formas de trabajo para los empleados. Es habitual el uso de aplicaciones web, apps en dispositivos móviles y servicios en la nube para el desarrollo del negocio.

Llegamos a nuestros clientes por todos los medios a nuestro alcance, nuestra web o incluso una tienda online, las redes sociales, etc. Además, como para complicar más las cosas, los usuarios utilizan todo tipo de dispositivos (móviles, tabletas, smartwatches,…) y tienen «vida propia» comportándose de forma activa en la red con sus opiniones, descargas, valoraciones, etc.

En cualquier caso, se plantean nuevos desafíos a la hora de gestionar las identidades de acceso de los usuarios a los distintos servicios: los empleados y colaboradores a las aplicaciones de gestión y operación del negocio, y los clientes a los servicios/productos que ofrecemos.

incibe_ 2006-2016 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/