BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 27 de mayo 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 20 y el 26 de mayo de 2016.

El phishing, versión gráfica

Cada vez es más común comprar por Internet, pero debido a la gran cantidad de tiendas existentes, a veces se hace complicado distinguir una tienda legítima de otra que no lo es, por eso recomendamos seguir una serie de pautas antes de comprar.

La mayoría de los phishing, independientemente de la entidad a la que suplanten, se realizan normalmente por medio del correo electrónico o del SMS y, aunque los dos canales anteriores son los más comunes, en la actualidad también es posible recibir phishing en aplicaciones de mensajería instantánea.

La siguiente infografía muestra de forma gráfica los pasos que siguen los ciberdelincuentes a la hora de perpetrar su delito y cómo engañan a la víctima hasta que esta cae en su trampa.

Detectados correos de phishing que suplantan al Banco Sabadell

La Oficina de Seguridad del Internauta (OSI) ha detectado en circulación correos electrónicos que simulan proceder del Banco Sabadell y cuyo objetivo es robar los datos de acceso de usuarios al servicio de banca online de esta entidad.

Los mensajes de esta nueva campaña de correos detectada tienen como asunto: Seguridad BancSabadell. Alertan al usuario de varios

intentos de acceso incorrectos a su cuenta desde la sucursal virtual, para presionarle a pinchar en un enlace y confirmar sus datos lo antes posible por motivos de seguridad.

Es importante que tomes conciencia de que ningún banco envía por correo electrónico solicitudes de datos personales de sus clientes. Si recibes un correo en este sentido, no facilites ningún dato y contacta inmediatamente con él.

Instagram y menores: cómo usar la app de forma segura

En cada charla, taller o evento que realizamos con chavales siempre hay una aplicación que parece ganar por goleada en cuanto al uso por parte de los menores: Instagram. Además lo hace sin que importe la edad, en cuanto tienen un dispositivo móvil (e incluso sin tenerlo) se apuntan. Así que no queda otra que aprender qué riesgos puede haber y, sobre todo, cómo podemos hacer que lo usen de forma segura.

Entre los menores de edad hay algunas aplicaciones y servicios que son los más utilizados. Mientras los adultos seguimos con nuestro Facebook, Twitter no termina de engancharles y dan el salto a Snapchat y Periscope… la imagen y el video les tienen enganchados, y en ese aspecto para ellos Instagram es la aplicación reina.

Descubre por qué quieren atacar tu pyme

Las actividades malintencionadas que se hacían la red han dejado de ser meras cuestiones egocéntricas en busca de un reconocimiento público sobre los conocimientos técnicos a través de: infecciones masivas, bromas mostrando algún mensaje divertido en la pantalla del ordenador o que provocaban un mal funcionamiento del sistema dejando en evidencia a la entidad en cuestión, etc.

Ahora hablamos de auténticas organizaciones criminales que utilizan las nuevas tecnologías para «evolucionar» sus «actividades» hacía un mercado del cibercrimen.

¿Cómo lo consiguen? Entre otras, con programas para enriquecerse de forma ilícita: que roban datos bancarios, secuestran ordenadores (ransomware) para pedir un rescate, o convierten el ordenador infectado en parte de una red de ordenadores zombie (Botnet) que

es utilizada para el envío masivo de correos de spam o para realizar campañas de phishing.

5 consejos de seguridad para atraer clientes online

¿Qué hace interesante tu tienda online?, ¿los productos?, ¿las facilidades de pago y de envío o devolución? o ¿el marketing? ¿Qué hacemos para que los que entren compren? y ¿para que vuelvan?, ¿cómo nos hacemos competitivos en la red?

Todas estas preguntas están en la cabeza de todo gestor de una tienda online. Pero, en una página cuyo fin es realizar una transacción económica, en la que el cliente «expone» sus datos (dirección, tarjeta, correo), además de todo lo anterior tenemos que preguntarnos: ¿cómo hacemos que perciba nuestros desvelos por garantizar su seguridad?

Seguramente creamos que nuestra tienda no es interesante para los ciberdelincuentes. En este artículo trataremos de ver qué persiguen, qué tenemos que puedan utilizar, cómo actúan y cómo protegernos. Además veremos qué factores hacen que nuestra tienda sea atractiva para nuestros clientes en términos de seguridad.

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/