BOLETÍN INFORMATIVO

INCIBE – Instituto Nacional de Ciberseguridad

León, 26 de diciembre de 2014.- 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 19 y el 25 de diciembre de 2014.

Correos suplantan a Banesto para propagar malware

Gran cantidad de correos fraudulentos de tipo phishing, se están haciendo pasar por el banco Banesto para infectar con malware los ordenadores de los usuarios que caigan en la trampa. En esta ocasión, el pretexto utilizado es la confirmación de una transferencia.

Los correos electrónicos tiene por asunto "**El saldo de la cuenta en el archivo adjunto**". En el caso de que un usuario ejecute el fichero adjunto comprometerá su sistema con un virus conocido como **Bredolab**, el cual incluye funcionalidades para el robo de información privada.

Si has recibido un correo de estas características, y has ejecutado el fichero adjunto, realiza un análisis completo del sistema con tu antivirus.

Aunque el banco Banesto fue integrado en el grupo financiero Santander hace un año, los ciberdelincuentes siguen aprovechando su imagen para propagar malware.

Las ciberestafas también "vuelven a casa por Navidad"

Compras y reservas online, felicitaciones por correo electrónico, mensajería instantánea... en Navidad, usamos estos servicios más que el resto del año. Los ciberdelincuentes lo saben y aprovechan esta circunstancia para sus "ciberestafas navideñas".

Llega la época navideña y con ella, los regalos, los turrones, las uvas… ¡y las ciberestafas navideñas! Aunque hasta hace unos años estas últimas no

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

formaban parte de la Navidad, parece que tienen intención de convertirse en otro de los clásicos de estas fiestas.

En la infografía de nuestro post, te explicamos cuáles son las ciberestafas más comunes de la Navidad y cómo identificarlas para no caer en la trampa. ¡Qué no te amarguen la Navidad!

Las cinco medidas de ciberseguridad para esta Navidad en tu empresa

La Navidad es uno de los momentos del año con mayor «actividad online». Incremento de las compras por internet, felicitaciones navideñas que recibimos por correo electrónico de personas cercanas, clientes o proveedores, publicaciones en redes sociales. Los ciberdelincuentes conocedores de este incremento de actividad, también se aprovechan de ello para llevar a cabo acciones fraudulentas mediante campañas de SPAM con felicitaciones navideñas, falsas promociones publicadas en redes sociales, Phishing bancario o de tiendas de compra por internet, incluso enlaces a sitios fraudulentos que nos envían por mensajería móvil. Por eso, es imprescindible no bajar la guardia para que nuestra empresa no sea el regalo de ningún ciberdelincuente.

1. Durante estas Navidades ten precaución antes de descargar cualquier felicitación Navideña.
2. Garantiza que las felicitaciones navideñas digitales que envíes estén libres de virus.
3. Presta especial atención a la imagen y actividad de la página web de comercio electrónico de tu empresa.
4. Ten precaución con las compras online que realices para adquirir obsequios de regalo.
5. Analiza cuidadosamente cualquier obsequio de electrónica que adquieras que pueda afectar a la seguridad corporativa.

No todos los hackers son malos, aprende a diferenciarlos

¿Sabías que no todos los hackers son malos? En el mundo de la seguridad informática, existen los hackers buenos y los hackers malos. Hoy te explicamos cuál es la diferencia entre ambos tipos y cómo distinguirlos.

¿Has oído hablar de los hackers y los crackers? ¿De los buenos y los malos? ¿Son todos lo mismo? ¿Tienen las mismas intenciones? Con este artículo

vamos a aclarar todas estas dudas.

Durante muchos años, se ha utilizado la palabra hacker de forma general para hablar de cualquier persona que se dedicase a encontrar los puntos débiles o fallos de los sistemas informáticos con fines maliciosos. Sin embargo, como ya sabemos, nunca es bueno generalizar.

Dentro de la seguridad informática, existe una especialidad llamada "Hacking ético" en la que se estudia un sistema informático con el objetivo de asegurarlo y protegerlo, y aquí es donde encontramos a los hackers buenos. Este tipo de hackers también son conocidos como hackers éticos, de sombrero blanco o hackers blancos.

Disponibles los videos de CyberCamp 2014 de la sala Conferencias

Si quieres volver a ver las charlas de la sala Conferencias de CyberCamp 2014 ya los tienes disponibles en nuestro canal de YouTube en la sección de CyberCamp.

CyberCamp 2014, el primer foro internacional que tiene como objetivo captar talento e innovación en el sector de la ciberseguridad, cerró las puertas de su primera edición con cifras que superaron las expectativas marcadas por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información, SETSI, y el Instituto Nacional de Ciberseguridad, INCIBE.

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/