BOLETÍN INFORMATIVO

INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 03 de junio 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 27 de mayo y el 02 de junio de 2016.

Falsa factura electrónica de Endesa intenta infectar tu equipo

La Oficina de Seguridad del Internauta ha detectado una campaña fraudulenta de tipo phishing que suplanta la identidad de Endesa, cuyo propósito es instalar malware en el equipo de la víctima. Es importante aclarar que se trata de una suplantación que utiliza la imagen de la empresa para cometer el fraude y, en ningún caso, afecta a la seguridad de los servicios de la entidad.

Para eliminar la infección se puede utilizar cualquier antivirus o antivirus auto-arrancable actualizado, pero dependiendo de la importancia de los datos perdidos y si se va a realizar denuncia, es recomendable realizar un clonado previo de los discos (copia de la información del disco duro en otro soporte) ya que se podrían eliminar archivos que pudiesen ser necesarios para una investigación.

Detectados correos de phishing que suplantan a Banco Popular

Los correos electrónicos detectados en esta ocasión, tienen como asunto «Mensaje seguridad!» y simulan proceder del Banco Popular. Éstos, tienen un documento adjunto llamado «Verificacion321312.html».

En el mensaje, se indica al usuario que se ha detectado actividad sospechosa en una de las cuentas y que ésta será suspendida a no ser que se complete el formulario adjunto.

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

Al descargar y ejecutar el documento adjunto, se abre en el navegador una página que suplanta a la del Banco Popular en la que solicita diversa información: nombre de usuario, contraseña, número de tarjeta, fecha de caducidad, código CVV y número PIN.

El ransomware, cada vez más peligroso. Protégete

Un ordenador infectado funciona de manera incorrecta, pero actualmente, hay malware que realiza acciones más peligrosas como el cifrar los ficheros y bloquear dispositivos. A este tipo de malware se le denomina ransomware, ¿sabes cómo protegerte?

El ransomware es un tipo de malware que “secuestra” el ordenador, smartphone o los ficheros que contiene, pidiendo un “rescate” para permitirnos usar de nuevo el dispositivo o que podamos recuperar los ficheros.

Estamos ante la amenaza más importante para nuestros ficheros, y los “malos” lo saben, por lo que no se espera que este tipo de malware cese, así que debemos de tener mucho cuidado, hay que tener muy presentes las medidas de seguridad y sobre todo, no olvidarse de las copias de seguridad en soportes o dispositivos que no estén conectados al ordenador de forma permanente.

No permitas que los datos de tu "androide" se pierdan

¿Quién es capaz de pasar un día sin su smartphone? Lo cierto es que probablemente, pocas personas ya que este pequeño dispositivo se ha integrado en nuestras vidas de un modo casi “inseparable”. Pero ¿sabemos cómo evitar una “separación” traumática?

Hoy día, la mayoría de los smartphones que usamos tienen información lo suficientemente importante como para que su pérdida o deterioro, nos suponga un problema. ¿Qué medios ponemos para evitarlo? Por un lado, tenemos en cuenta las buenas prácticas en la gestión de mensajería instantánea, correo electrónico, redes sociales, etc. y por supuesto, también instalamos software antivirus y mantenemos nuestros navegadores seguros.

BOLETÍN INFORMATIVO

Blog Menores OSI: ¡Oh, no!, me toca ser el coordinador TIC, ¿por dónde empiezo? (II). La red local

Hace unas semanas comenzábamos esta serie de contenidos tratando las cuestiones de la seguridad física, hoy continuamos adentrándonos en el mundillo de las redes locales.

Prácticamente todos los ordenadores del centro están en red, así se pueden conectar a Internet, compartir archivos entre sí, imprimir en la misma impresora, etc. Sin embargo, si no tenemos un mínimo cuidado en la configuración de la red, podemos dejar en manos de nuestros alumnos información sensible como por ejemplo notas, teléfonos de los profesores, etc.

Así pues, lo ideal es separar la red de nuestros centros entre los ordenadores de gestión (secretaría, dirección) y los de las aulas (aulas ordinarias, aulas de informática) de modo que no sea posible que se comuniquen entre sí.

Antes pyme con contraseñas fuertes que sencillas

Hay un proverbio árabe que dice: «La primera vez que me engañes, será culpa tuya. La segunda, será culpa mía». En cuanto a la seguridad de la información, y en el tema de las contraseñas, ya no podemos seguir echando balones fuera. Ya ha ocurrido antes, no dejaremos que siga pasando.

Sabemos que las credenciales de acceso (usuario y contraseña) son uno de los tipos de datos, junto con las cuentas bancarias y tarjetas de crédito, más demandados en los mercados negros de compra-venta de información. Para los cibercriminales, adivinarlas o craquearlas es un juego, cuanto más cortas y más sencillas mejor.

Precauciones al realizar una videoconferencia

¿Realizas videoconferencias de trabajo? ¿Utilizas las videoconferencias para comunicarte con tus clientes, proveedores y compañeros de trabajo? ¿Conoces algunas de las medidas de seguridad a tener en cuenta ante una videoconferencia?

El mercado ofrece multitud de herramientas y plataformas que ofrecen servicios de videoconferencias a la medida de las necesidades de las empresas. Pueden ser gratuitas o de pago, pueden permitir compartir documentos de trabajo, disponer de servicios añadidos como herramientas

de chat o pizarras virtuales, y se pueden realizar presentaciones de la misma forma que si estuviésemos en una sala de exposiciones.

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/