BOLETÍN INFORMATIVO

INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 8 de septiembre de 2023.- El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y empresas. Además, es un instrumento para la trasformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.

INCIBE centra sus esfuerzos en la prestación de servicios públicos de prevención, concienciación, detección y respuesta ante incidentes de seguridad, adaptándose a cada público específico (menores, ciudadanía y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

Cómo saber si una empresa está preparada para contratar servicios en la nube

Algunos factores clave y beneficios que una pyme puede adquirir a través de la contratación de servicios en la nube son la reducción de costes, mejor seguridad o acceso global, entre otros.

Existen 14 principios que permiten evaluar y seleccionar al proveedor más adecuado y seguro, como la protección de datos en tránsito, separación entre clientes o seguridad operativa. Este artículo da respuesta a las preguntas más relevantes a realizar antes de contratar servicios en la nube, teniendo en cuenta el grado de madurez actual de adopción de dichos servicios en España.

Más información: https://www.incibe.es/empresas/blog/

Caso real del 017: extorsión por un supuesto cliente insatisfecho, exigiendo un pago en bitcoines

El responsable de seguridad de una *start-up* se pone en contacto con el servicio Tu Ayuda en Ciberseguridad de INCIBE porque había recibido un correo electrónico de una persona que decía ser un cliente insatisfecho e intentaba extorsionarle solicitando un pago en bitcoines por el valor de 1500 euros. De lo contrario, realizaría acciones de difamación contra su empresa, afirmando que tenía la capacidad de publicar notas de prensa en los principales medios de comunicación de España.

Aunque el usuario trasladó que, desde un principio, no le había dado ninguna importancia, ni credibilidad al email, no era capaz de quitárselo de la cabeza, por lo que decidió escribir al 017 para preguntar si debía realizar algún tipo de acción al respecto.

Más información: https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales

BOLETÍN INFORMATIVO

El fraude del "sí" al contestar al teléfono

En esta era digital, donde la información personal está más expuesta que nunca, los ciberdelincuentes han encontrado en las llamadas telefónicas una oportunidad para engañar a personas desprevenidas. Actualmente, sigue siendo una forma común de comunicación e, independientemente de quiénes las realicen, es habitual responder con un simple "sí". Sin embargo, pocos son conscientes de los riesgos ocultos que pueden surgir al dar una respuesta tan aparentemente inofensiva.

Al grabar la voz, los estafadores la pueden utilizar para autorizar transacciones financieras, contratos o incluso falsificar la identidad. Además, las grabaciones de voz pueden ser manipuladas y utilizadas como evidencia en situaciones que podrían poner en riesgo la reputación. ¿Cómo podemos evitar ser víctimas de este engaño?

Más información: https://www.incibe.es/ciudadania/blog

INCIBE detecta una campaña de suplantación a la Policía Nacional para infectar los dispositivos con *malware*

Esta semana INCIBE ha identificado una campaña que suplanta a la Policía Nacional mediante la técnica de *phishing*. En el correo electrónico se menciona una citación judicial, debido a una denuncia interpuesta al usuario, con la finalidad de que la víctima descargue, a través del enlace, un archivo que ejecutará en su dispositivo un *malware* de tipo troyano.

En caso de haber caído en la trampa, se recomienda, entre otras cosas, desconectar el dispositivo infectado de la red del hogar para evitar que el *malware* se propague a otros dispositivos y realizar un análisis completo del sistema con el antivirus, asegurándonos de que esté actualizado.

Más información: https://www.incibe.es/ciudadania/avisos

Claves de la comunicación en Internet

La comunicación en línea es cada vez más habitual en la rutina diaria de los menores y posee multitud de beneficios, pero también pueden darse posibles malentendidos y problemas *online*. Algunos son el uso de un alias o de datos que no se ajustan a la realidad, ya que pueden generar una falsa sensación de anonimato o de que nadie, al otro lado de la pantalla, puede llegar a saber quiénes son. Además, puede provocar una falsa sensación de seguridad o impunidad, creyendo que sus acciones no pueden ser rastreables o castigadas.

Como adultos, debemos enseñarles a empatizar con el resto de las personas tanto en el entorno físico como en Internet, fomentar su pensamiento crítico y establecer unas pautas de uso y comunicación que sirvan de canal de ayuda, en caso de tener problemas en la Red.

Más información: https://www.incibe.es/menores/blog

BOLETÍN INFORMATIVO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TU AYUDA EN CIBERSEGURIDAD

017 Teléfono 017

WhatsApp 900 116 117

Telegram @INCIBE017

Formulario web

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia · España | digital 2026

Más información: https://www.incibe.es/

comunicacion@incibe.es
@incibe
017 TU AYUDA EN CIBERSEGURIDAD
www.incibe.es
Av. José Aguado 41 / 24005 León
T. (+34) 987 877 184