INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 26 de marzo de 2021.- 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, ciudadanos y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

INCIBE gestionó más de 130.000 incidentes de ciberseguridad durante el año 2020

INCIBE, a través de INCIBE-CERT, el Centro de Respuesta a Incidentes de Seguridad, ha gestionado 133.155 incidentes de ciberseguridad durante el año 2020, de los cuales 106.466 hacen referencia a ciudadanos y empresas. De esos incidentes, el 35,22% correspondía a *malware* y el 32,02% a cualquier tipo de fraude, seguido de sistemas vulnerables, con un 17,39%.

Con el objetivo de incrementar la confianza digital de los ciudadanos y las empresas de España, INCIBE ofrece entre sus servicios la creación de contenidos de concienciación. Entre ellos destacan los avisos de seguridad, con la publicación en 2020 de 495, en los que facilitaba información de actualidad y utilidad para sus públicos objetivo. Cabe destacar que en los últimos años ha aumentado el nivel de prevención y anticipación de la sociedad a los problemas en temas de ciberseguridad.

Más información en: https://www.incibe.es/sala-prensa/notas-prensa.

Suplantado el Ministerio de Asuntos Económicos y Transformación Digital con una supuesta factura electrónica

Además, esta semana, INCIBE ha detectado una campaña de envío de correos electrónicos fraudulentos que tratan de suplantar al Ministerio de Asuntos Económicos y Transformación Digital, utilizando como pretexto el envío de una supuesta factura electrónica, con el fin de difundir *malware*.

Más información en: https://www.incibe.es/protege-tu-empresa/avisos-seguridad.

Preparados para luchar contra los fraudes online

Dado que los menores utilizan a menudo Internet, pueden verse afectados por estafas o engaños en la Red, llamados fraudes online. Generalmente, su propósito es suplantar al usuario y robar sus datos o dinero. Niños y adolescentes pueden experimentar estos problemas, ya sea porque utilizan los mismos entornos digitales que los adultos o porque algunos fraudes van dirigidos concretamente a los usuarios más jóvenes.

Además, los fraudes online pueden valerse de diferentes métodos de distribución para llegar a sus posibles víctimas, pero en el contexto del menor algunos tipos de fraudes son más comunes, como aquellos que les llegan a través de un mensaje privado en las redes sociales, un chat en los juegos online o un correo electrónico. ¿Cómo pueden aprender a reconocerlos?

Más información en: https://www.is4k.es/blog.

Cómo mejorar el rendimiento de los dispositivos con herramientas de mantenimiento y limpieza

Los usuarios suelen recurrir a diversas herramientas de protección, como los antivirus para analizar y detectar *malware*, virus o cualquier tipo de archivo que pueda ser potencialmente peligroso.

Sin embargo, más allá de estas herramientas de protección, es recomendable utilizar otras destinadas a la limpieza y mantenimiento del dispositivo que ayudarán a terminar con los problemas de rendimiento ocasionados por la acumulación de archivos residuales y temporales.

¿Cuánta información temporal y archivos innecesarios se van acumulando en los sistemas con el paso del tiempo?

Más información en: https://www.osi.es/es/actualidad/blog.

Modus operandi en el día a día de un ciberdelincuente

Actualmente, hablar de conceptos como fraude, extorsión, chantaje o engaño implica hablar de ciberdelincuencia. Estos conceptos son cada vez menos presenciales y más digitales. Los ciberdelincuentes se adaptan a la temporalidad de diversas situaciones, por ejemplo en 2020 sus esfuerzos se centraron en la pandemia mundial, atacando a farmacéuticas, laboratorios y proveedores, lo que les permitió ocultarse entre la marea de información para pasar desapercibidos.

¿Cómo actúan? ¿Cuáles son sus objetivos principales y cómo los consiguen? ¿Cómo pueden las empresas protegerse de ellos?

Más información en: https://www.incibe.es/protege-tu-empresa/blog.

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