INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 12 de mayo 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.

Apúntate a nuestro taller *online* y celebra con nosotros el Día de Internet 2023

El 17 de mayo se celebra en todo el mundo el Día de Internet, bajo el lema 'Ciudadanía digital. Derechos y oportunidades'. Un año más, INCIBE se suma a esta iniciativa para promover el uso seguro de las tecnologías por parte de la ciudadanía, impartiendo un taller *online* de 11:00 a 12:00 para ayudar a los usuarios a proteger sus conexiones inalámbricas y dispositivos.

A lo largo de la sesión se abordarán aspectos como los tipos de ataques a conexiones inalámbricas, la protección de la red wifi, el uso de wifis públicas, medidas de seguridad en *Bluetooth* y NFC, y riesgos y buenas prácticas de dispositivos *wearables*.

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

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

Múltiples campañas de *phishing* que intentan obtener las credenciales de tu gestor de correo electrónico

Esta semana INCIBE ha detectado múltiples campañas de correos maliciosos de tipo *phishing* que tienen como objetivo robar las credenciales de acceso del gestor de correo. En ellas la víctima recibe un email indicándole que la contraseña de usuario caducará pronto o que hay una nueva actualización de mantenimiento del servicio y que no podrá seguir utilizándolo a partir de una determinada fecha. Además, se le solicita acceder a un enlace malicioso para cambiar la contraseña, actualizar el servicio o confirmar que desea borrar el email.

En caso de haber facilitado las credenciales de acceso, es recomendable modificarlas lo antes posible, y siempre que se pueda, habilitar un doble factor de autenticación.

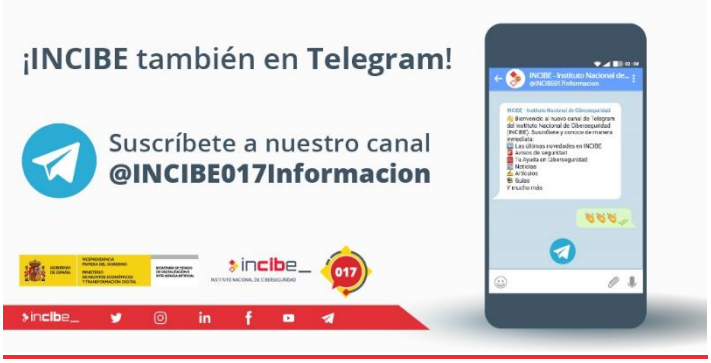
Más información: https://www.incibe.es/empresas/avisos

Principales formas de estafa a través del email: *phishing* más comunes

La suplantación de identidad está a la orden del día en el mundo digital. Según un informe publicado en 2023 por Trend Micro, el 91% de las empresas es susceptible de sufrir un ataque de *phishing*. Esta práctica tiene múltiples formas y variantes. Algunos ejemplos son la suplantación a la Agencia Estatal de Administración Tributaria (AEAT), empresas de mensajería o entidades bancarias, además del fraude *Bussines Email Compromise* (BEC) o del CEO.

En función de las necesidades de los usuarios, es decir, de la época del año, los ciberdelincuentes se decantarán por unas modalidades de *phishing* u otras. Ante esta situación, como empleados, ¿qué podemos hacer para evitar caer en sus engaños y poner en riesgo la seguridad del negocio?

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



Suscríbete al nuevo canal de Telegram de INCIBE

BOLETÍN INFORMATIVO

Para más información:

https://www.incibe.es/
https://www.incibe.es/empresas
https://www.incibe.es/ciudadania
https://www.incibe.es/menores
https://www.incibe.es/incibe-cert

Redes sociales:

FB IG TW YT LI