BOLETÍN INFORMATIVO

INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 11 de agosto 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.

De empresas más pequeñas hasta el objetivo final. Así funciona el *Island Hopping*

La base de una empresa segura está en el conocimiento y la concienciación y, por eso, es importante que las organizaciones se mantengan informadas de todo lo relacionado con el mundo de la ciberseguridad, desde las últimas técnicas utilizadas por los ciberdelincuentes hasta las mejores formas de combatirlas.

Es por ello que resulta vital conocer el *Island Hopping*, puesto que podría representar una amenaza para los negocios. Los ciberdelincuentes empiezan primero por proveedores u otras empresas pequeñas, ya que no tienen tantas medidas de seguridad y son más fáciles de dominar. De este modo, reúnen información para llegar a su objetivo final.

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

Caso real del 017: intento de fraude amoroso utilizando técnicas de *deedfake* para suplantar a un personaje público

Un usuario se siente intranquilo y se pone en contacto con Tu Ayuda en Ciberseguridad de INCIBE, a través de WhatsApp, tras instalarse una aplicación de búsqueda de pareja y encontrar un perfil de un chico que le resultó atractivo, aunque en ninguna de las fotos mostraba su rostro.

Después de varios días mandándose mensajes decidieron intercambiar sus números. Su nuevo amigo le confesó que su nombre no era verdadero, ya que se trataba de un personaje público. Después de unos días, hicieron una videollamada, y así el usuario corroboró su identidad. Tras varios días de mensajes y llamadas, decidieron conocerse en persona, pero el supuesto amigo le dijo que su padre no le iba a permitir viajar a España si antes no le hacía un regalo. Ante esta situación,

empezó a dudar, por lo que decidió contactar con el 017 antes de realizar alguna compra o transferencia económica.

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

INCIBE detecta una campaña de *phishing* que utiliza códigos QR

Esta semana INCIBE ha detectado una nueva campaña de correos electrónicos fraudulentos, de tipo *phishing*, que destaca por el uso de códigos QR. El método detectado podría vulnerar las herramientas de seguridad, además de ser efectivo incluso utilizando un doble factor de autenticación.

En caso de ser víctima de este engaño, se recomienda eliminarlo inmediatamente y ponerlo en conocimiento del resto de empleados para evitar posibles nuevas víctimas. En algunos de los casos detectados los destinatarios eran personal directivo o con grandes responsabilidades en la organización.

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

¿Cuáles son los principales tipos de *hackers*?

En numerosas ocasiones, el término *hacker* se asocia a un pirata informático que intenta obtener información personal, todo ello con fines delictivos. Sin embargo, esta descripción es parcialmente inexacta, ya que, en realidad, abarca a un grupo de expertos en tecnologías informáticas con diferentes motivaciones.

Entre ellos destacan los de sombrero blanco o *hackers* éticos, quienes detectan brechas de seguridad en los sistemas informáticos con permiso de la organización y dentro de los límites de la legalidad. Por otro lado, los de sombrero negro hacen referencia a los ciberdelincuentes, también llamados *crackers*, que se dedican a explorar los sistemas de información sin autorización del usuario o la organización, explotando vulnerabilidades con fines ilícitos. Finalmente, los de sombrero gris comparten características de los dos casos anteriores y tratan de encontrar las brechas de seguridad de las empresas sin su conocimiento.

Más información: https://www.incibe.es/ed2026/talento-hacker/blog

Estafas que prometen ganar dinero por caminar, escuchar música o ver vídeos

En redes sociales se ha convertido en algo común encontrarse con anuncios y vídeos de otros usuarios, en algunos casos incluso *influencers*, que prometen formas fáciles y rápidas de ganar dinero. Suelen solicitar realizar una serie de tareas simples, como rellenar encuestas o ver anuncios y, a cambio, recibir el dinero acordado.

Estas actividades no tienen por qué ser fraudulentas. Sin embargo, los ciberdelincuentes se aprovechan de este modelo de 'negocio' para engañar a los usuarios, poniendo en circulación fraudes con *modus operandi* igual o muy similar

a los que ofrecen las empresas legítimas. Es por ello que desde INCIBE recomendamos consultar las reseñas, investigar sobre la plataforma, utilizar fuentes confiables y, en caso de duda, no utilizarla, ya que podría ser una estafa.

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

INCIBE detecta una campaña de *phishing* suplantando a Correos

INCIBE también ha identificado una campaña de correos electrónicos falsos que suplantan a la empresa de mensajería y paquetería Correos, utilizando la técnica de *phishing*. En el mensaje se indica al usuario que se ha intentado entregar un paquete y no se ha podido realizar la entrega, por lo que solicitan una nueva fecha para su envío.

En caso de ser víctima de este fraude, se recomienda practicar *egosurfing* para saber si los datos personales han podido quedar expuestos en Internet, así como recopilar toda la información para poder tomar acciones legales y presentarla ante las Fuerzas y Cuerpos de Seguridad del Estado.

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

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