

## INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 30 de junio 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 transformación 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.

### [INCIBE detecta una campaña de phishing que descarga malware Grandoreiro](#)

Esta semana INCIBE ha detectado una campaña de *phishing* que tiene como objetivo infectar los dispositivos, a través del enlace que acompaña al mensaje del email, con el *malware* conocido como Grandoreiro, troyano que se caracteriza por extraer información bancaria.

En caso de ser víctima de este engaño, se recomienda escanear el dispositivo con un antivirus actualizado para eliminar cualquier posible infección, borrar cualquier archivo que se haya descargado del correo y cambiar las contraseñas de las cuentas a las que se haya accedido, mientras se ha tenido instalado el *malware*.

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

### [Juice-Jacking: ¿en qué consiste este ataque y cómo puede protegerse de él una empresa?](#)

Puede darse el caso de que estando fuera de la oficina recibamos el aviso de que nuestro teléfono móvil corporativo se está quedando sin batería y veamos un puesto de carga gratuita. El problema de estas zonas de carga es que son públicas y, por lo tanto, vulnerables.

Al estar abiertas a todo el mundo, un ciberdelincuente podría ser capaz de modificarlas, de forma que al cargar los dispositivos, puedan instalar un *malware* en ellos. Esta técnica se conoce como *Juice-Jacking* y, a través de ella, también se pueden obtener datos personales, como, por ejemplo, contraseñas o información sensible.

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

Esta información puede ser usada en parte o en su integridad citando la fuente.

## Caso real del 017: un hijo tiene un accidente y le pide su madre pagar por Bizum la grúa

Una usuaria se pone en contacto con el servicio Tu Ayuda en Ciberseguridad tras ser víctima de un fraude. Había recibido en su teléfono un SMS de un número que no tenía registrado, donde supuestamente su hijo le decía que había tenido un accidente con el coche y necesitaba 350€ para pagar los costes de la grúa.

Además, le facilitaba un número de teléfono para que se pusiese en contacto con él a través de WhatsApp en el teléfono de la grúa, ya que no tenía disponible el suyo. Una vez realizada la transferencia, no volvió a recibir ningún mensaje y decidió escribirle a su número real. No obstante, este desconocía lo que había ocurrido. ¿Qué pautas le proporcionó INCIBE para solventar la situación?

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

## INCIBE identifica varias campañas de smishing suplantando a diversas entidades bancarias

INCIBE ha identificado varias campañas de suplantación a diversas entidades bancarias. En los SMS se indica al usuario que se ha realizado un cargo en su cuenta o que la cuenta o tarjeta ha sido bloqueada, incluyendo un enlace para resolver el problema, el cual redirecciona a una web fraudulenta para robar las credenciales de acceso a la banca *online* de la víctima.

Ante esta situación, es importante asegurarse de cambiar las credenciales de acceso al banco y utilizar contraseñas únicas y difíciles de descifrar para cada cuenta. Además, se aconseja verificar periódicamente los movimientos de la misma y guardar todas las pruebas disponibles del incidente por si hubiera que denunciar.

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

## Claves de las copias de seguridad para que se convierta en una práctica en el día a día digital

¿Por qué es importante hacer copias de seguridad? Para mejorar la capacidad de respuesta en caso de pérdida de datos, tener todos los archivos en un mismo lugar, mantener un mayor control de la información y liberar espacio en tus dispositivos.

A la hora de hacer la primera copia de seguridad, hay que saber elegir bien qué datos se quieren guardar, con qué frecuencia y dónde almacenarlos; verificar que la copia se haya realizado correctamente y que se pueda restaurar y, además, mantenerla en un lugar seguro.

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

## INCIBE localiza una campaña de suplantación a la Agencia Tributaria para propagar *malware*

INCIBE también ha localizado una campaña de *phishing* dirigida a la Agencia Tributaria, cuyo objetivo es distribuir varios tipos de *malware*. Uno de los mensajes alerta al usuario sobre un error debido a documentación inválida y otro pretende ser un reembolso de impuestos del pasado año fiscal. Ambos correos electrónicos contienen un enlace adjunto que descarga un archivo fraudulento.

En caso de ser víctima de este fraude, se debe desconectar la red del hogar para evitar que el *malware* se propague a otros dispositivos, así como ejecutar el antivirus y realizar un análisis completo del sistema, asegurándose de que esté actualizado.

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

incibe\_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

TU AYUDA EN CIBERSEGURIDAD

017  
Teléfono  
017

WhatsApp  
900 116 117

Telegram  
@INCIBE017

Formulario  
web

CONTACTANDOS

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA VICERREINIA PRIMEIRA DEL GOBIERNO MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL SECRETARÍA DE ESTADO DE ENERGÉTICA E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

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



Esta información puede ser usada en parte o en su integridad citando la fuente.