

## INCIBE. INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 5 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 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.

### Cómo evitar que la huella digital afecte a nuestras empresas

Debido al gran auge de la digitalización, debemos ser conscientes de la información que compartimos en Internet de manera pública, ya que, incluso cuando creemos que es inofensiva, si no se trata correctamente, podría poner en riesgo la seguridad de la empresa, dando pie a que los ciberdelincuentes ataquen los sistemas, redes, ordenadores, etc.

Los datos pueden ser rastreados de dos formas, a través del *footprinting* y *fingerprinting*, pero, ¿en qué consisten estas técnicas y cómo podemos evitar que recopilen información sensible de nuestro negocio?

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

### Learn to Check: una plataforma para luchar contra la desinformación

La desinformación se localiza en gran medida a las redes sociales, mensajería instantánea y, en definitiva, Internet, por la capacidad de difusión que este medio ofrece. Además, cualquier usuario puede publicar una determinada información sin necesidad de que esta esté contrastada, sea veraz y rigurosa.

En este artículo de blog se presentan herramientas para combatir esta problemática social, ayudando a los usuarios a estar mejor protegidos, como el proyecto *Learn to Check*, una iniciativa que se basa en un conjunto de cursos de formación gratuitos. Su objetivo es fomentar el pensamiento crítico entre los jóvenes para desenvolverse con seguridad en la sociedad actual.

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

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

### Suplantando a la Agencia Tributaria para distribuir *malware* mediante correos electrónicos

Esta semana INCIBE ha detectado una campaña que suplanta a la Agencia Tributaria mediante la técnica *phishing* para distribuir *malware*. El mensaje usa como pretexto la necesidad de corregir unos datos, ya que ha identificado una diferencia en el IRPF. El correo va acompañado de un enlace, el cual descarga un archivo comprimido que contiene un ejecutable (archivo.exe) con un código fraudulento.

Es importante tomar las siguientes medidas en caso de ser víctima de este engaño: asegúrate de desconectar de la red de tu hogar el dispositivo para evitar que el *malware* pueda llegar a otros dispositivos y realiza un análisis exhaustivo con el antivirus.

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

### Smishing suplantando a la Seguridad Social que solicita actualizar los datos de tu tarjeta sanitaria

También se ha identificado una campaña de *smishing* suplantando a la Seguridad Social que solicita actualizar la tarjeta sanitaria por medio del enlace proporcionado para evitar perder los derechos que ofrece. A través del formulario al que se accede desde el enlace, se piden datos personales del usuario para robarlos y utilizarlos de forma fraudulenta.

Si has sido víctima de este fraude, recopila evidencias por si necesitas interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado y realiza *egosurfing*, es decir, busca los datos que se hayan podido publicar sobre ti en la Red.

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

### Phishing suplantando a FedEx que pide el abono de un importe para recibir un paquete

Recientemente, INCIBE ha detectado una campaña de *phishing* que suplanta a la empresa de paquetería FedEx. Mediante un correo fraudulento, con la excusa de necesitar abonar un pago para recibir un paquete, redirige al usuario por medio de un enlace a una encuesta y, posteriormente, a dos formularios, en los que se solicitan datos personales y bancarios.

¿Has caído en este engaño? No olvides contactar con tu entidad bancaria y avisar del incidente para evitar que se hagan cargos en tus cuentas o se cancelen las tarjetas. Asimismo, revisa regularmente los movimientos para controlar que no se realicen pagos no autorizados.

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

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

## Distribución de *malware* a través de un *phishing* que suplanta a Endesa

Detectada una campaña de distribución de *malware* a través de un correo electrónico fraudulento suplantando a Endesa. El mensaje indica que el usuario puede descargar su factura, adjuntada al correo como archivo comprimido .zip, pero en realidad es un archivo .msi, es decir, un archivo ejecutable que, en este caso, contiene un código malicioso.

Si te llega este *phishing* y ejecutas el archivo, aísla el dispositivo o equipo de la red para que el *malware* no pueda extenderse a otros dispositivos y realiza un análisis exhaustivo con el antivirus actualizado.

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

## III edición del MOOC 'Ciberseguridad para microempresas y autónomos'

El próximo 10 de mayo comienza una nueva edición del curso *online* y gratuito 'Ciberseguridad para microempresas y autónomos', que ya tiene abierta la inscripción para todas aquellas personas que deseen realizarlo. Con un enfoque divulgativo, a la vez que práctico, se presentan de forma extensa multitud de aspectos y conceptos de ciberseguridad cruciales para una digitalización segura de los negocios.

Este curso, en modalidad MOOC (*Massive Online Open Course*), cuenta con contenido actualizado sobre sus ediciones anteriores. A lo largo de 13 unidades, se abordan temas relacionados con el uso seguro de las nuevas tecnologías, la ingeniería social, la seguridad en la nube, las redes wifi, la relación con proveedores y clientes o cómo responder ante un incidente de seguridad, entre otros.

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



Suscríbete al [nuevo canal de Telegram de INCIBE](https://www.incibe.es/empresas/blog)

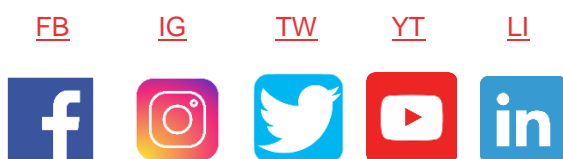
Esta información puede ser usada en parte o en su integridad citando la fuente.

# 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:



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