

SMISHING

Entra en este enlace y realiza el pago de la tasa de aduanas para recibir tu paquete.
www.webfraudenta.es

¿Un enlace para que pague tasas de aduanas?
¡Qué raro! Si no he comprado nada...

El SMS del paquete

No pulses en un enlace si no estás seguro de a qué sitio web te redirige. Tampoco respondas al SMS con tus datos.

Recuerda, aunque un SMS aparentemente proceda de una empresa o servicio conocido, podría tratarse de un fraude. Contrasta la información con terceras fuentes de confianza.

 Si quieres saber más, consulta nuestra web.

incibe.es/ciudadania

 **Financiado por la Unión Europea**
NextGenerationEU

 GOBIERNO DE ESPAÑA

VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

 R 2026

 incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

 017

 OSI Oficina de Seguridad del Internauta

En colaboración de:
 aem Asociación española de empresas de mensajería

PHISHING

¿Has accedido hoy a las 10:00h a tu banco?



Si recibes un correo, recuerda dedicarle un tiempo antes de acceder a sus peticiones.

Si no estás seguro de su veracidad, con estas pautas saldrás de dudas.

Detectados accesos no autorizados en tu cuenta

Tienes un nuevo correo

MiBanco.es para mi <info@mi BANCO.es>

Estimado/a cliente,

Le escribimos desde MiBanco.es para informarle que su cuenta de ahorros ha sufrido una **h**aqueo y puede haber perdido cierta cantidad económica.

Por favor, **a**cceda **i**mediatamente al siguiente enlace para facilitar a nuestro soporte técnico sus datos bancarios y poder solucionarlo.

www.mybanko.es/%20/soporte2

Verifica el remitente, revisa la ortografía del correo, comprueba los enlaces o archivos adjuntos antes de pulsar sobre ellos y, si te exige, extorsiona o incita a hacer algo de manera rápida o urgente, **SOSPECHA**.

Ante la menor duda, marca el correo como **SPAM** y elimínalo.

 Si quieres saber más, consulta nuestra web.



incibe.es/ciudadania

VISHING



Buenos días, soy Marcos, llamo de tu compañía de teléfono. Hemos encontrado un problema con tu última factura y quisiéramos confirmar los datos de tu cuenta para ver si ha habido un error.

¿De dónde dices que me llamas?

Ninguna compañía me pediría datos sensibles por teléfono, no me fío, creo que lo mejor será colgar y bloquear el número de teléfono.


Si recibes una llamada de una supuesta entidad del tipo que sea, ¡nunca des tus datos! ¡Evita el vishing! Si dudas de su veracidad, busca el contacto oficial y llama directamente para esclarecer el asunto.

Perfil verificado
600 000 000

Llamar



incibe.es/ciudadania

 Si quieres saber más, consulta nuestra web.

SPOOFING

Tienes un nuevo correo

Para: micorreo@gmail.com

De: micorreo@gmail.com

Asunto: ¡Tengo información sobre tí!

Te he hackeado y tengo mucha información sobre ti. ¡Págame en bitcoins o publicaré tus fotos y documentos privados!

El ciberdelincuente explica en el correo que ha estado monitorizando el ordenador de la víctima.

¡Espera! Tengo mi sistema actualizado, mi antivirus no detecta ninguna amenaza y no tengo fotos comprometidas.

Esto debe ser un fraude de tipo *mail spoofing* que consiste en falsear la dirección del remitente.

Si no pagas, publico tus fotos

El ciberdelincuente ha suplantado mi email para engañarme, pero sé que no debo ceder al chantaje.

Y tú, ¿sabes ahora cómo actuar si te pasa lo mismo? Marca como **SPAM**, borra el correo y contacta con el 017 si tienes dudas.

SPAM

PAPELERA



incibe.es/ciudadania

Si quieres saber más, consulta nuestra web.