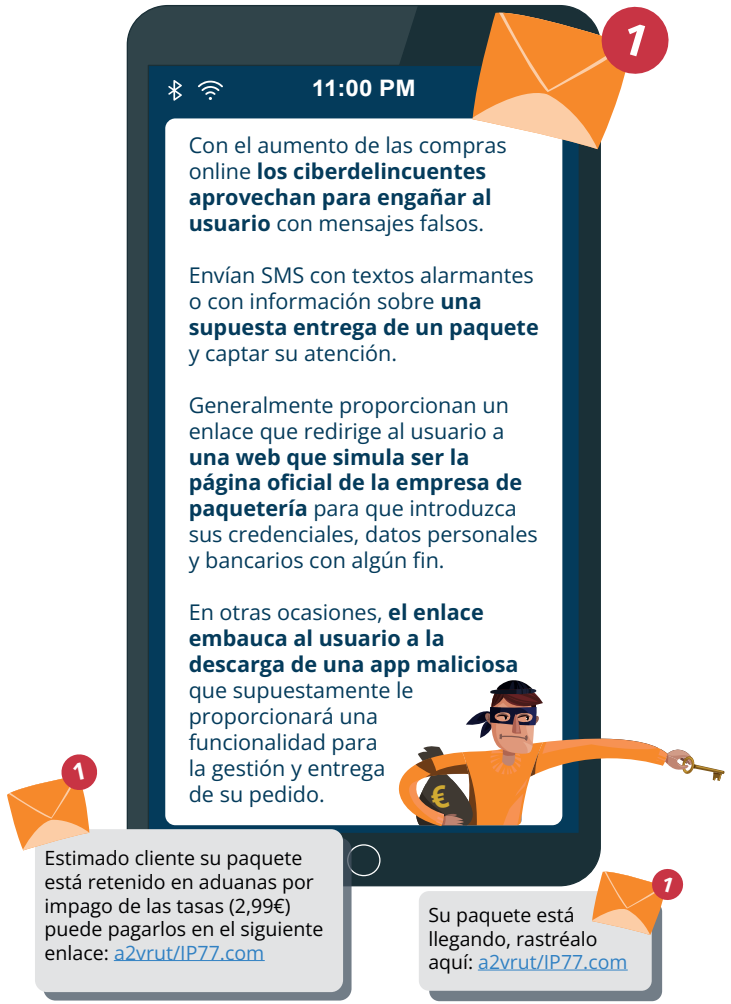
¿QUÉ ES EL SMISHING?

Es una técnica de ingeniería social en la cual un ciberdelincuente envía un SMS simulando ser una entidad legítima a un usuario, con el objeto de adquirir su información personal, bancaria, credenciales o realizarle un cargo económico.

¿Por qué suplantan los ciberdelincuentes a través de SMS a servicios de mensajería y reparto de paquetes?



incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

TU AYUDA EN CIBERSEGURIDAD

017

WhatsApp
900 116 117

Telegram
@INCIBE017

Formulario web

PROTÉGETE DEL SMISHING

Que no te engañen con SMS fraudulentos que suplantan a empresas de mensajería y paquetería.

Te explicamos cómo detectar, evitar y denunciar los SMS fraudulentos.

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
TR 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
En colaboración de:
OSI Oficina de Seguridad del Internauta
aem Asociación española de empresas de mensajería

¿CÓMO DETECTAR ESTE FRAUDE?

Analiza el SMS. Si te pide algo con **urgencia**, sospecha.

Revisa si el enlace facilitado coincide con el dominio de la **página oficial de la empresa**. Si algún carácter es distinto, mal síntoma.

Atento a la redacción. Los **errores ortográficos** no son buena señal.

Comprueba el **horario de recepción del mensaje**. La noche, fines de semana, madrugada o festivos no suelen ser momentos habituales para el envío de notificaciones utilizadas por entidades oficiales.

Vigila el estado de tus pedidos **solo desde la aplicación oficial de la empresa** de paquetería o desde la página web donde realizaste la compra. Descarta otras opciones.

CONSEJOS PARA MANTENERTE SEGURO FRENTE AL SMISHING

01

Extrema la precaución ante cualquier SMS que no estés esperando.

02

Activa los detectores de spam si tu móvil dispone de ellos para que no recibas SMS potencialmente maliciosos.

03

Recuerda que ninguna entidad te pedirá por SMS que le facilites contraseñas o datos privados y financieros a través de un enlace en un mensaje.

04

En caso de duda, pregunta a la entidad que supuestamente te está escribiendo, a través de sus canales oficiales disponibles para los usuarios, sobre la veracidad de la información recibida.

¿QUÉ PUEDE PASARTE
SI RESULTAS VÍCTIMA DEL ENGAÑO?

Estás proporcionando a los ciberdelincuentes tus datos bancarios y personales y credenciales de acceso a tus cuentas, con las consecuencias que ello te pueda ocasionar:

- **Realización de cargos en tus cuentas bancarias.**
- **Creación de perfiles falsos en tu nombre.**
- **Robo de cuentas de usuario.**
- **Instalación de aplicaciones maliciosas para fines maliciosos.**
- **Recepción de fraudes dirigidos en base a tus gustos, preferencias, hábitos, ubicación, etc.**

¿CÓMO PUEDES DENUNCIAR?

1

Recopila todas las pruebas del fraude que puedas, como capturas de pantalla del SMS, URL de la página web fraudulenta, extracto bancario con los cargos indebidos, perfil falso, aplicación maliciosa, etc.

2

Una vez tengas estas evidencias en tu poder, **contacta con las Fuerzas y Cuerpos de Seguridad del Estado** para presentar una denuncia. También puedes acudir presencialmente a una comisaría y solicitar asesoramiento para formalizar la denuncia.

Para más información, **INCIBE** pone a tu disposición la Línea de **Tu Ayuda en Ciberseguridad, 017**, un teléfono gratuito y confidencial disponible todos los días del año. Servicio disponible también en **WhatsApp (900 116 117)** y **Telegram (@INCIBE017).**

Policía Nacional
https://www.policia.es/_es/denuncias.php

Guardia Civil
https://www.guardiacivil.es/es/servicios/denuncias/index.html