

176 - SEGURIDAD

Evita las estafas por SMS y llamadas

Reconoce los mensajes y llamadas falsas que suplantan a bancos, empresas de paquetería o familiares.



NIVEL
Fácil

TIEMPO
15 min

CATEGORÍA
Seguridad

WEB
soporteinformatico360.com

Los estafadores envían SMS y hacen llamadas haciéndose pasar por empresas conocidas. Su objetivo es que pulses un enlace o des tus datos. Aprende a reconocerlos y a cortar a tiempo.

■ Qué necesitas

- ✓ Tu móvil
- ✓ El teléfono oficial de tu banco a mano
- ✓ Ganas de desconfiar un poco

■ Paso a paso

01

Desconfía de los enlaces en SMS

Un SMS de «paquete retenido» o «cargo no reconocido» con enlace casi siempre es falso. No lo pulses.

Mensajes

Tu paquete está retenido.
Paga 1,99 € aquí: bit.ly/...

02

No des códigos ni claves

Nadie de tu banco te pedirá por teléfono códigos SMS, el PIN o que confirmes una operación.

03

Cuelga y llama tú

Si te llaman con prisas, cuelga y llama tú al número oficial que aparece en tu tarjeta o en la web.



04

Cuidado con el «Hola mamá»

Si un supuesto hijo escribe desde un número nuevo pidiendo dinero, llámale a su número de siempre antes de nada.

05

Bloquea y denuncia

Bloquea el número y marca el mensaje como spam desde el propio móvil.



06

Avisa si has caído

Si diste datos bancarios, llama a tu banco para bloquear la tarjeta y presenta denuncia.

■ Consejos**CONSEJO 1**

El número que aparece en pantalla se puede falsificar: no te fíes solo de él.

CONSEJO 2

Instala apps solo desde la tienda oficial, nunca desde un enlace de SMS.

CONSEJO 3

Puedes consultar dudas gratis en el 017 de INCIBE.



Importante: Si has instalado una app desde un enlace de SMS, pon el móvil en modo avión y pide ayuda a un técnico.

¿Prefieres que lo hagamos por ti?

Diagnóstico sin compromiso y presupuesto cerrado antes de empezar.
En taller, a domicilio en Madrid o por asistencia remota.

910 117 112

soporte@soporteinformatico360.com
soporteinformatico360.com