¿QUÉ ES EL SMISHING?

incibe.es/ciudadania

El remitente es un número de **teléfono desconocido**.

Solicitan **datos personales, credenciales o bancarios** bajo alguna excusa.

El mensaje es **importante, urgente o llamativo** que lleva a la acción.

A veces, invitan a **descargar** una supuesta aplicación oficial en el móvil.

Se facilita un **enlace**, generalmente acortado, para proceder con la gestión.

Fraude que consiste en **suplantar** a entidades y servicios a través del envío de **SMS** cuyo objetivo es **robar tus datos o infectar tus dispositivos**.

Si ya es tarde y han conseguido engañarte:

1. **Cambia tus contraseñas de inmediato**. También en aquellos sitios online en los que utilices esa misma clave. **¡Recuerda que esto no es una buena práctica!**
2. Contacta con tu **entidad bancaria** si tus datos bancarios pueden estar comprometidos. **¡Ellos te ayudarán!**
3. **Contrasta la información** con la empresa que supuestamente te está contactando a través de sus **canales oficiales**.
4. Reporta el **SMS** malicioso a **INCIBE (incidencias@incibe-cert.es)**
5. Interpón una **denuncia** en las Fuerzas y Cuerpos de Seguridad del Estado **aportando las evidencias**.
6. Y si aún tienes dudas, **contacta con 'Tu Ayuda en Ciberseguridad' de INCIBE**, llamando al 017, o a través de WhatsApp (900 116 117) o Telegram (@017INCIBE).

017

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
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta