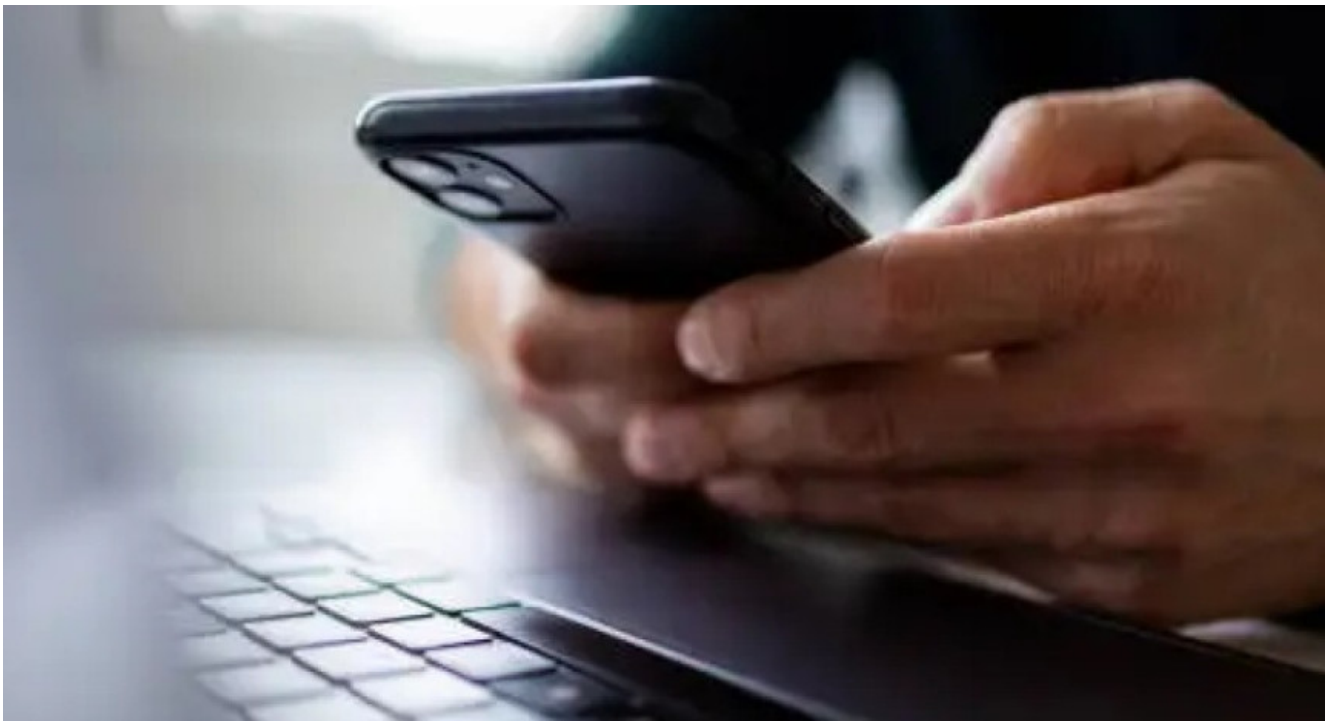
# Qué es y cómo evitar el smishing, el nuevo método de estafas por mensaje de texto

11/06/2025



En Argentina, varias personas se vieron afectadas por una nueva modalidad de estafa llamada **smishing**, **un ataque a través de SMS, que suelen ser falsas alertas sobre promociones o premios** que, supuestamente, el usuario se ha ganado de forma legítima a través de sorteos.

*Cuál es la nueva estafa vía SMS. Fuente: Pexels.*

Estos ciberataques están diseñados para generar una sensación de urgencia y llevar a las personas a actuar rápidamente, sin pensar en las consecuencias. Estos SMS les piden a las personas que **accedan a una plataforma, ingresen sus datos personales**, y de esta forma, les den acceso a los ladrones a **sus información financiera o personal**.

De hecho, son cada vez más comunes aquellos mensajes que **aparentan ser de bancos o empresas,** solicitando que

actualices tus datos o confirmes información mediante un enlace que, a primera vista, parece real. **Estas alertas urgentes suelen ser intentos de fraude conocidos como smishing,** y es fundamental estar alerta para no caer en la trampa.

 *Ciberseguridad. Foto: Unsplash*

# Smishing: 6 claves para protegerte de estafas por SMS

Para intentar evitar caer en este tipo de estafas cibernéticas, es importante tener en cuenta varias claves que podrían ser importante. La primera de ellas es **desconfiar de los mensajes urgentes de números desconocidos.** Sin embargo, hay otras banderas rojas a las que debés estar atento:

- **No abras enlaces de desconocidos:** si no reconocés al remitente o el mensaje genera dudas, lo mejor es borrarlo sin abrirlo.
- **Evitá apps no oficiales:** descargá solo aplicaciones desde tiendas oficiales. Mantené desactivada la opción de instalar apps de fuentes desconocidas.
- **Detectá errores de ortografía:** los mensajes oficiales no suelen tener errores ni redactarse de forma extraña. Si algo suena raro, desconfiá.
- **Verificá la seguridad del sitio:** antes de ingresar tus datos, asegurate de que la web comience con “https” y tenga el ícono del candado.
- **Contactá siempre por canales oficiales:** si recibís una alerta sobre tu cuenta, no uses los números del mensaje. Llamá directamente al número oficial del banco.
- **Denunciá cargos no autorizados:** si ya fuiste víctima, comunicate con tu banco y realizá una denuncia en la comisaría.

Fuente: Canal 26