



28/junio/2024

## ¡CUÍDATE DEL SMISHING!

### TIPOS DE ATAQUES DE SMISHING

**Verificación de cuenta:** La víctima recibe un mensaje de texto de una supuesta empresa o proveedor de servicios.

**Premios o loterías:** Se informa a las víctimas que han ganado un premio, o la lotería.

**De soporte técnico:** Los usuarios reciben un mensaje sobre un problema con su dispositivo o cuenta.

**Alertas de fraude bancario:** Los mensajes parecen proceder del banco de la víctima, advirtiendo transacciones no autorizadas o actividades sospechosas.

**Estafas fiscales:** La persona recibe mensajes que dicen ser del SAT.

**Cancelación de servicios:** La víctima recibe un mensaje de que una suscripción o servicio está a punto de cancelarse por un problema de pago.

### ¡PROTÉGETE!

- No hagas clic en enlaces sospechosos o en mensajes de texto.
- No reveles datos personales a través de SMS.
- Revisa tus cuentas bancarias regularmente.
- Instala un antivirus en tus dispositivos.
- No abras vínculos sospechosos.
- Descarga aplicaciones solo de tiendas y desarrolladores oficiales.

