

SMISHING: PHISHING EN FORMA DE SMS

Es un tipo de ataque de ingeniería social que se realiza mediante mensajes de texto, a través de los que los ciberdelincuentes intentan obtener información personal o financiera.



¿QUÉ QUIERE CONSEGUIR EL CIBERDELINCUENTE?



Obtener información personal o bancaria.



Vender productos o servicios falsos/inexistentes.



Infectar nuestro dispositivo móvil.



Suplantar nuestra identidad.



Extorsionar a la víctima.

NO MUERDAS EL ANZUELO SI...



... el remitente es desconocido o sospechoso.



... te solicitan información confidencial (número de cuenta, contraseñas u otra información sensible).



... los enlaces son sospechosos.



... te presionan para actuar rápidamente con amenazas o urgencias.



... las ofertas son demasiado buenas.

¡Recuerda! Desconfía de mensajes con información que no hayas solicitado previamente, no compartas datos personales y verifica siempre la fuente (con tu banco, tu comercio...).

Comunicanos estos incidentes en: incidencias@cyberzaintza.eus para combatir este tipo de amenazas en constante evolución.

