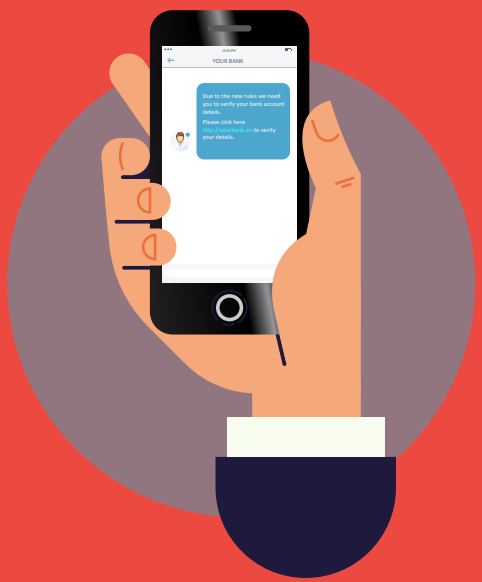
'SMISHING' BANCARIO POR SMS

El 'smishing' (combinación de las palabras SMS y 'phishing') es el intento de fraude para obtener información personal, financiera o de seguridad a través de un mensaje de texto.



¿CÓMO LO HACEN?

El mensaje de texto normalmente te pedirá que hagas clic en un enlace o que llames a un teléfono para "verificar", "actualizar" o "reactivar" tu cuenta. Pero... el enlace te lleva a una página web falsa, y el número de teléfono es el de un estafador que suplanta a una empresa.

¿QUÉ PUEDES HACER?

- **No hagas clic en enlaces, adjuntos o imágenes** que recibas en mensajes de texto no solicitados sin antes verificar el remitente.
- **No te apresures.** Tómate tu tiempo y haz las comprobaciones necesarias antes de responder.
- **Nunca respondas a un mensaje de texto** que te solicite tu PIN o la contraseña de tu banco, o cualquier otra credencial de seguridad.
- Si crees haber respondido a un 'smishing' y proporcionado tus datos bancarios, **contacta con tu banco de inmediato.**

EUROPOL EC3 European Cybercrime Centre · EBF · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN

#Ciberestafa