Conoce cómo protegerte del triple intento de suplantación

Actualmente los ciberdelicuentes están usando tres técnicas sencillas que, combinadas, consiguen robar nuestros datos o tener acceso a nuestras cuentas:

SMS

Esta técnica se conoce como **Smishing,**

Envían SMS haciéndose pasar por el banco, incluso **suplantando el número de teléfono oficial de la entidad.** Al recibirse, este mensaje fraudulento **se guarda en el grupo de SMS que normalmente recibimos del banco**, pareciendo un aviso real.

Este SMS contiene enlaces a páginas que son una copia del banco.

Web

Esta técnica se conoce como **Phishing,**

Esta copia, cada vez más realista tanto en móviles como en ordenadores, intenta r ecabar nuestros datos bancarios: usuario, contraseña y número de teléfono en muchos casos.

Llamada telefónica

Esta técnica se conoce como **Vishing,**

Una vez tienen nuestro teléfono personal, nos piden datos que nos pueden llegar via SMS, como la clave de firma, o incluso, pueden llamarnos directamente **suplantando el número d e teléfono de la entidad** para recabar más datos o confirmar las operaciones.

Ante cualquier duda, no facilites datos y contacta con nosotros mediante nuestro formulario o en el teléfono 91 423 0029, dentro de nuestra web Te Ayudamos