ESTAFAS BASADAS EN LA SUPLANTACIÓN

Hay diferentes estafas en internet relacionadas con la suplantación de identidad. Estas son las más habituales y las pautas para su detección.

PHISING - EMAIL

Emails que suplantan a contactos conocidos y empresas para estafarnos.

- Mirar siempre la dirección desde donde se ha mandado el email. Si está mal escrita es una estafa. Los emails de empresas suelen tener el nombre de la empresa después de la @: **"contacto@*amazon*.es"**

- Si es un email oficial de una entidad o empresa tiene que tener saludo personalizado, no "estimado usuario", "Hola"... sino **"Querido Juan García".**

SUPLANTACIÓN DE CUENTAS EN REDES SOCIALES

Para detectar cuentas falsas deberemos fijarnos en el nombre de usuario de la cuenta. No puede haber dos cuentas con el mismo nombre de usuario. Generalmente se crean cuantas con nombres de usuarios parecidos a los de las cuentas suplantadas.

En apps de mensajería también deberemos fijarnos en el número de teléfono.

SUPLANTACIÓN DE PÁGINAS WEB

Para saber si estamos en una página real miraremos la dirección de la página o ulr. Si está mal escrita será falsa siempre independientemente de cómo sea la página.

Ejemplo **www.macasonrisas.es mal**
www.macsonrisas.es bien

Una vez en la página correcta, para hacer compras o meter información debemos asegurarnos de que en la barra de direcciones haya un candado o la dirección comience por https..

SUPLANTACIÓN TELEFÓNICA

Para prevenir las estafas a través del teléfono, no se recomienda comprar nada, descargar nada o mandar dinero a nadie que nos haya mandado un mensaje o nos haya llamado por teléfono. Colgaremos, llamaremos al teléfono que tenemos de esa empresa o persona y le preguntaremos si nos hay llamado.