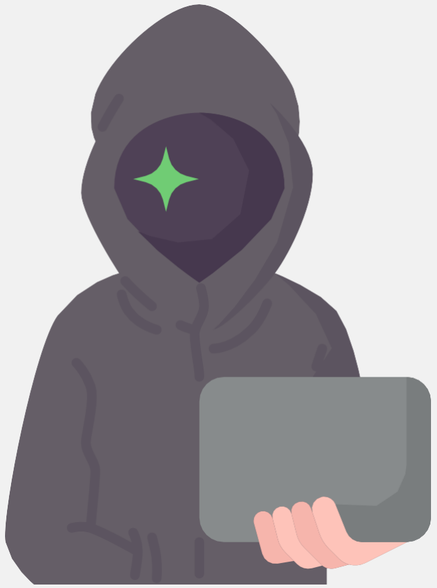
consumes

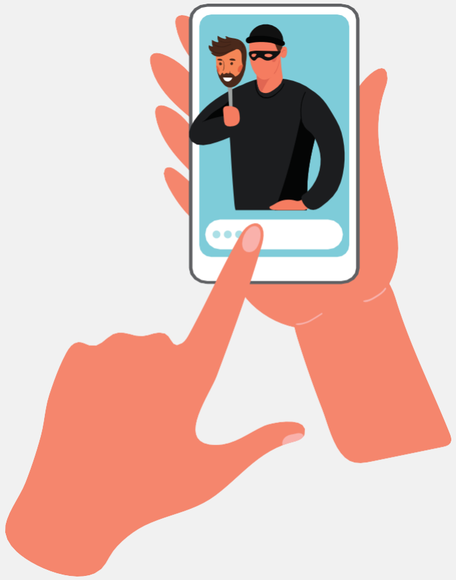
Estafas y fraudes bancarios online

Phishing, smishing, vishing y web spoofing

La ciberdelincuencia, muy activa



Los ciberdelincuentes están muy activos en lo que se refiere a estafas que suplantan la identidad de un tercero como organismos, administración pública o empresas.



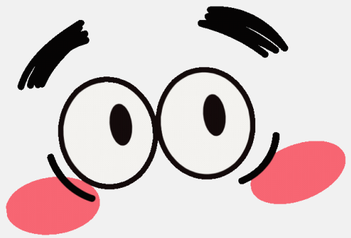
Entre los más habituales están los que se hacen pasar por entidades bancarias o medios de pago online

consumes

Cuando no sospechamos

Si no somos clientes de la entidad bancaria que supuestamente remite el email, SMS o llamada telefónica, pensaremos que se trata de un error o no hacemos caso.

Pero si somos clientes de esa entidad, es fácil que caigamos en un fraude o estafa.



consumes

Piensa y decide sin prisas

Los ciberdelincuentes nos atraen con mensajes que aparentan una

falsa sensación de urgencia

para que tomemos una decisión rápida y caigamos en la trampa.

consumes

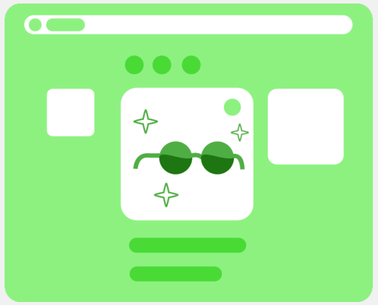
Tipos de estafas

Correos electrónicos
PHISHING

SMS
SMISHING

Llamadas telefónicas
VISHING

Páginas web falsas
WEB SPOOFING



consumes

Phishing (1)

Suplantan la identidad de una entidad bancaria o de medios de pago online (como PayPal), con el objetivo de robar las credenciales del usuario, información personal, datos bancarios de cuentas y tarjetas, con el único fin de robarnos dinero.

El método utilizado es el correo electrónico

consumes

Phishing (2)

En dicho email, nos informan que:

- **La cuenta bancaria ha sido bloqueada o se bloqueará en unos minutos**
- **Se van a realizar medidas de seguridad de la entidad**
- **Te piden que conffirmes tu identidad y/o contraseñas personales**
- **Te ofrecen un premio o participar en algún sorteo de la entidad**

Smishing

En nuestro móvil recibimos un SMS con un enlace.

Este mensaje SMS "simula" ser de nuestro banco.

El SMS alerta de una incidencia con tu tarjeta financiera o con tu banca online o que se está intentando hacer con tu tarjeta una compra fraudulenta, para lo que te invita a hacer clic en un enlace.

El método utilizado es el SMS

consumes

Web spoofing

Si haces clic en el enlace que recibes a través de SMS (smishing), accedes a una web fraudulenta (web spoofing) que suplanta la entidad bancaria, y captura los datos de tarjetas y/o credenciales.

El método utilizado es la página web fraudulenta

consumes

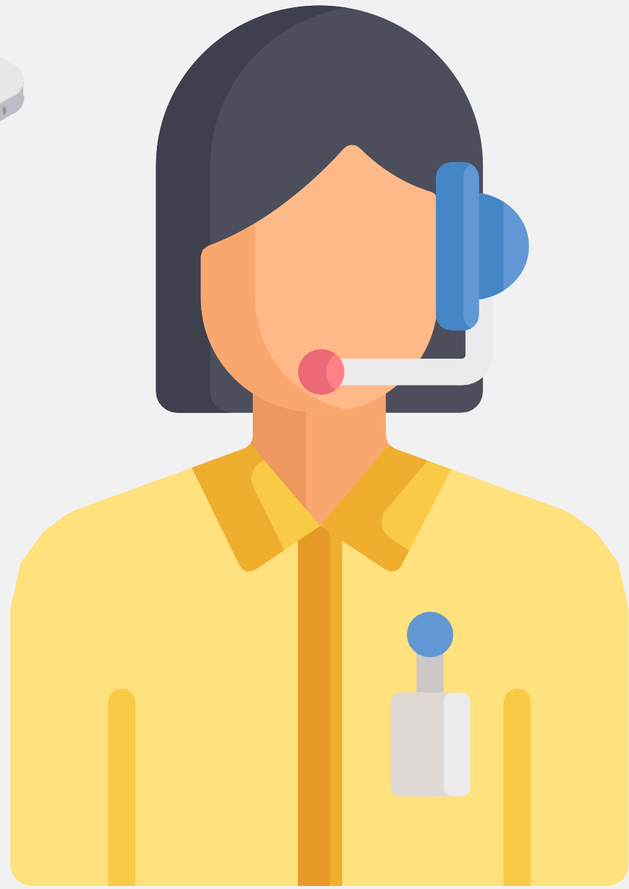
Vishing (1)

Si haces clic en el enlace que recibes a través de SMS (smishing), a continuación, recibes una llamada telefónica "vishing" en la que el interlocutor se hace pasar por tu entidad bancaria y te pide un código SMS o tus claves personales para cancelar o resolver la incidencia cuando, en realidad, se está realizando una operación fraudulenta.

El método utilizado es la llamada telefónica

consumes

Vishing (2)



También es posible que solamente recibas una llamada telefónica (vishing) haciéndose pasar por tu entidad, solicitándote datos personales y contraseñas con el fin de bloquear una operación o compra fraudulenta.

Si los facilitas, en realidad estás autorizando la operación fraudulenta.

consumes

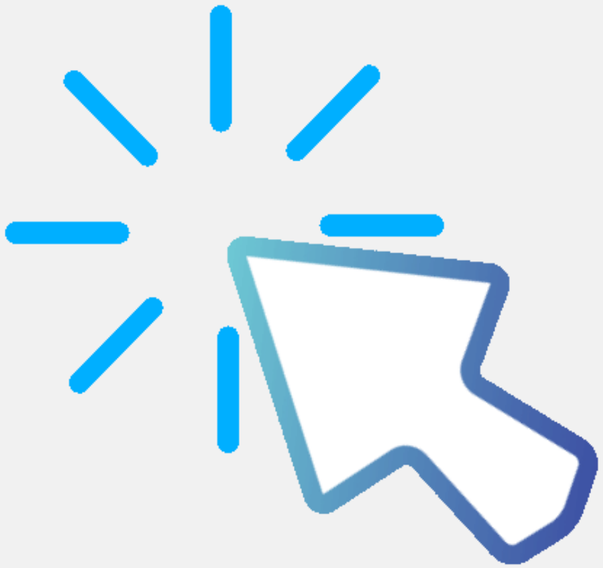
Consejos para prevenir fraudes #1

Desconfía de cualquier mensaje o llamada que requiera una actuación urgente o inmediata, aunque nos advierta de que nuestro dinero, cuenta o tarjeta están siendo objeto de un uso fraudulento.

consumes

Consejos para prevenir fraudes # 2

No hagas clic en enlaces que recibas en el correo electrónico y en SMS en tu teléfono, ni llames a números de teléfono que puedan aparecer en el mensaje.

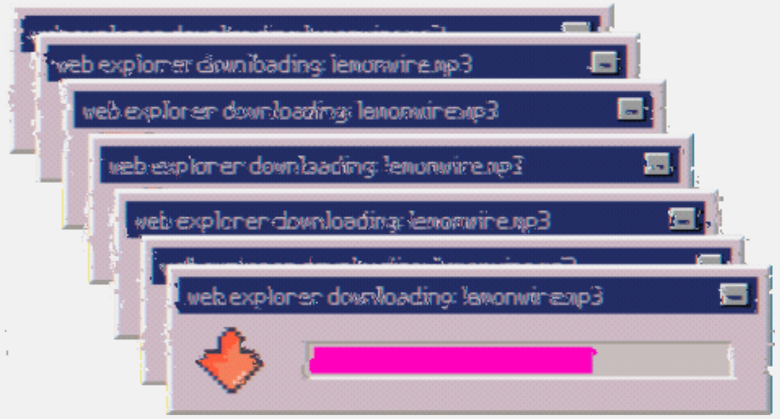


consumes

Consejos para prevenir fraudes # 3

3

No descargues archivos adjuntos que puedas recibir en el mensaje.



consumes

Consejos para prevenir fraudes # 4

Bloquea al remitente para evitar seguir recibiendo mensajes.

consumes

Consejos para prevenir fraudes # 5

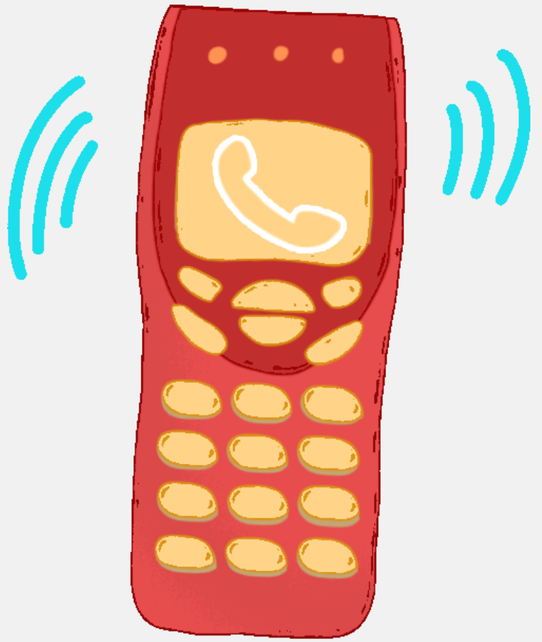
5

Si recibes una llamada supuestamente de tu entidad bancaria y te pide datos y contraseñas, corta la comunicación.

consumes

Consejos para prevenir fraudes # 6

Si necesitas contactar con tu banco, hazlo tú a través del teléfono de atención al cliente de tu entidad.



consumes

Consejos para prevenir fraudes # 7

Recuerda que tu entidad bancaria nunca te va a solicitar por email, SMS o teléfono tus datos personales, ni datos de cuentas ni tarjetas, ni las claves ni contraseñas personales.

consumes

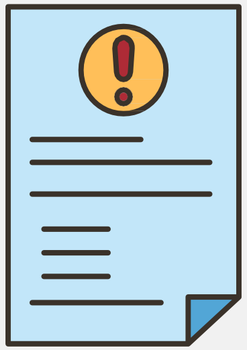
Consejos para prevenir fraudes # 8

Si has caído en la trampa o tienes dudas, ponte en contacto lo antes posible con tu entidad para bloquear la operación, la tarjeta o tu cuenta, y que no puedan seguir haciendo un uso fraudulento de tus datos y contraseñas.

consumes

Consejos para prevenir fraudes # 9

Acude a la Policía Nacional, Guardia Civil o Juzgado de guardia lo antes posible para interponer una denuncia



consumes

Unos consejos de la

Unión de Consumidores de Aragón

¿Necesitas ayuda?

Zaragoza:
C/ Alfonso I, nº 20, Entlo. Centro, 50003 Zaragoza
Tel. 976 397602 / Fax 976 398630
info@ucaragon.com

Teruel:
C/ Yagüe de Salas 16, 4º Izd. Edificio Social «Ciudad de Teruel» 44001 Teruel
605026984 / 628824443
teruel@ucaragon.com

Huesca:
C/ del Parque, 9 22003 Huesca
976 397602
Info@ucaragon.com

consumes