



Estafas bancarias online



Phishing
Smishing
Vishing
web spoofing



Los ciberdelincuentes no descansan

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

Entre los más habituales están los que **se hacen pasar por entidades bancarias y de servicios financieros**.





¿Cuándo no sospechamos?

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

Pero si somos clientes de esa entidad bancaria, es más fácil caer en la estafa.





¡Piensa y decide sin prisas!

**Los ciberdelincuentes nos atraen con mensajes
que aparentan una**

"falsa sensación de urgencia"

para que tomemos una decisión sin pensar.





Tipos de estafas



Correos
electrónicos
PHISHING



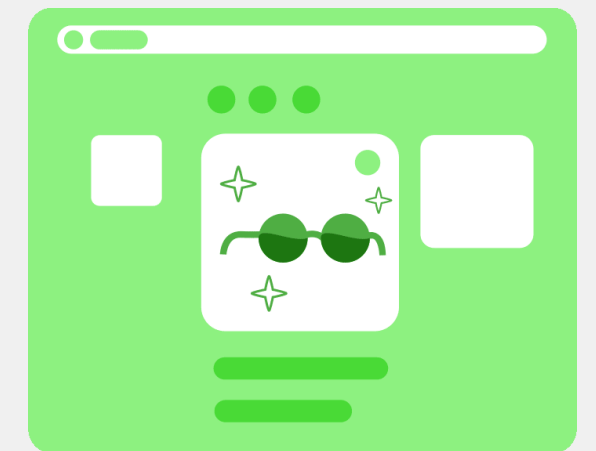
SMS
SMISHING



Llamadas
telefónicas
VISHING

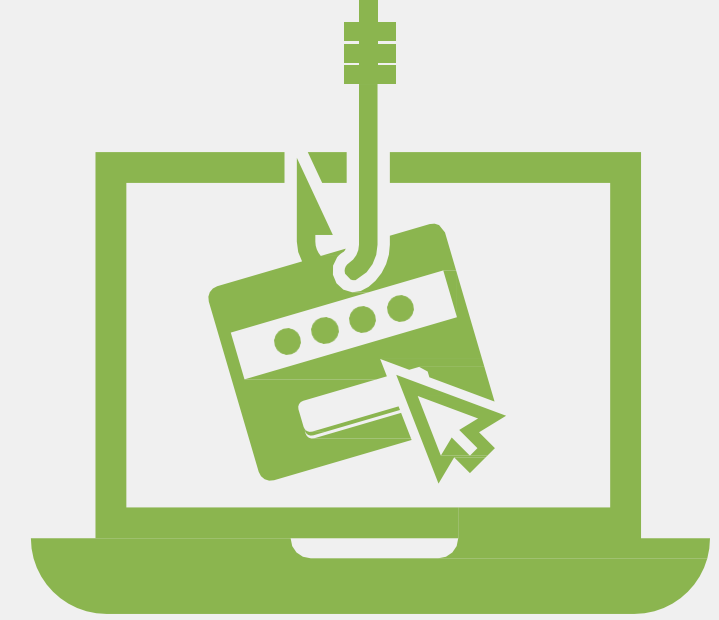


Páginas
web falsas
**WEB
SPOOFING**



consumes





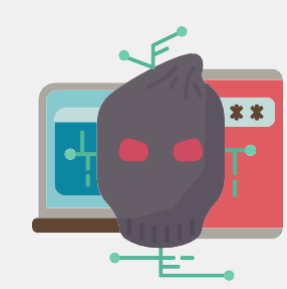
Phishing (1)

Suplantando la identidad de una entidad bancaria o de medios de pago online, con el objetivo de robar las contraseñas del usuario, información personal, datos bancarios de cuentas y tarjetas, con el único fin de robarnos dinero.



El método utilizado es el correo electrónico





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 **confirmes tu identidad** y/o contraseñas personales
- Te ofrecen un **premio** o participar en algún sorteo de la entidad





Smishing

En el teléfono móvil recibimos un **SMS** con un enlace.

El 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 **clik en un enlace**.

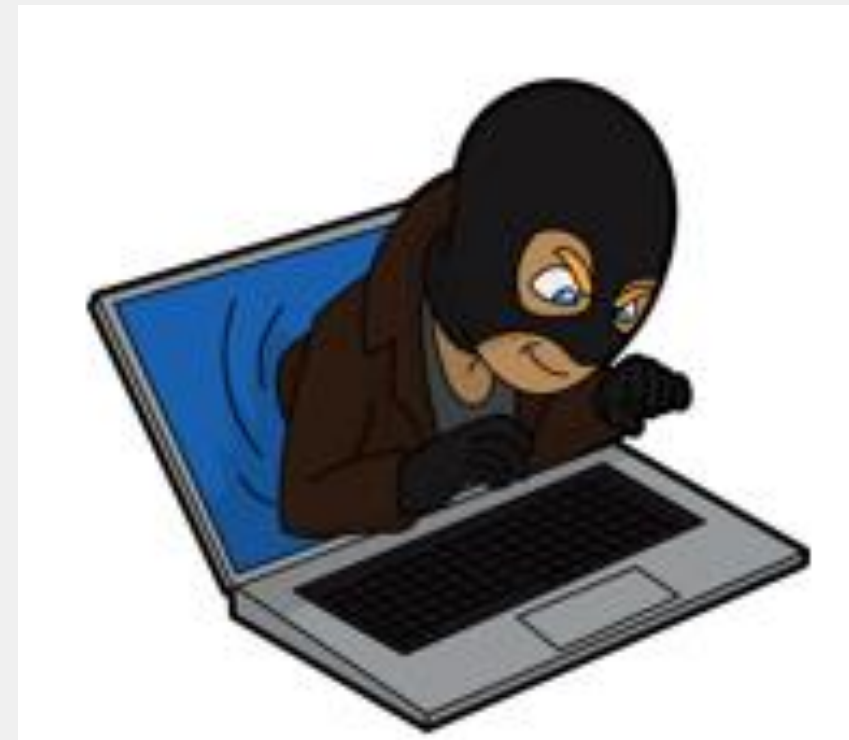


El método utilizado es el
SMS





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**





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





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.





Consejos para prevenir fraudes #1



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

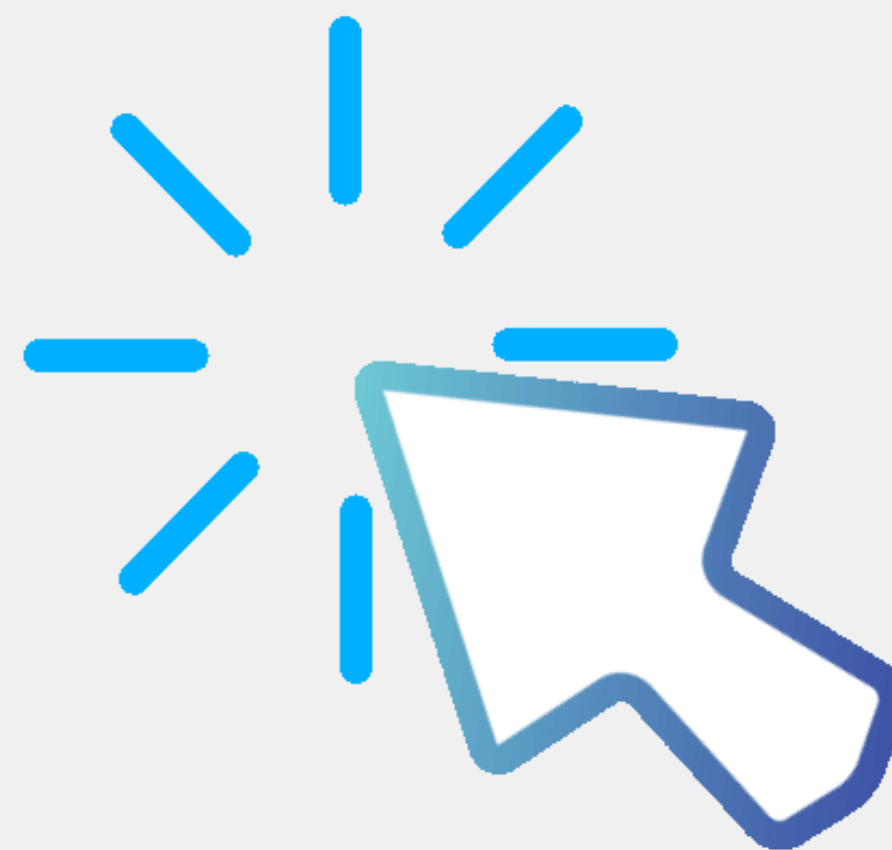




Consejos para prevenir fraudes #2



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.





Consejos para prevenir fraudes # 3



No descargues archivos adjuntos que puedas recibir en el mensaje.





Consejos para prevenir fraudes #4



Bloquea al remitente para evitar seguir recibiendo mensajes.





Consejos para prevenir fraudes #5



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

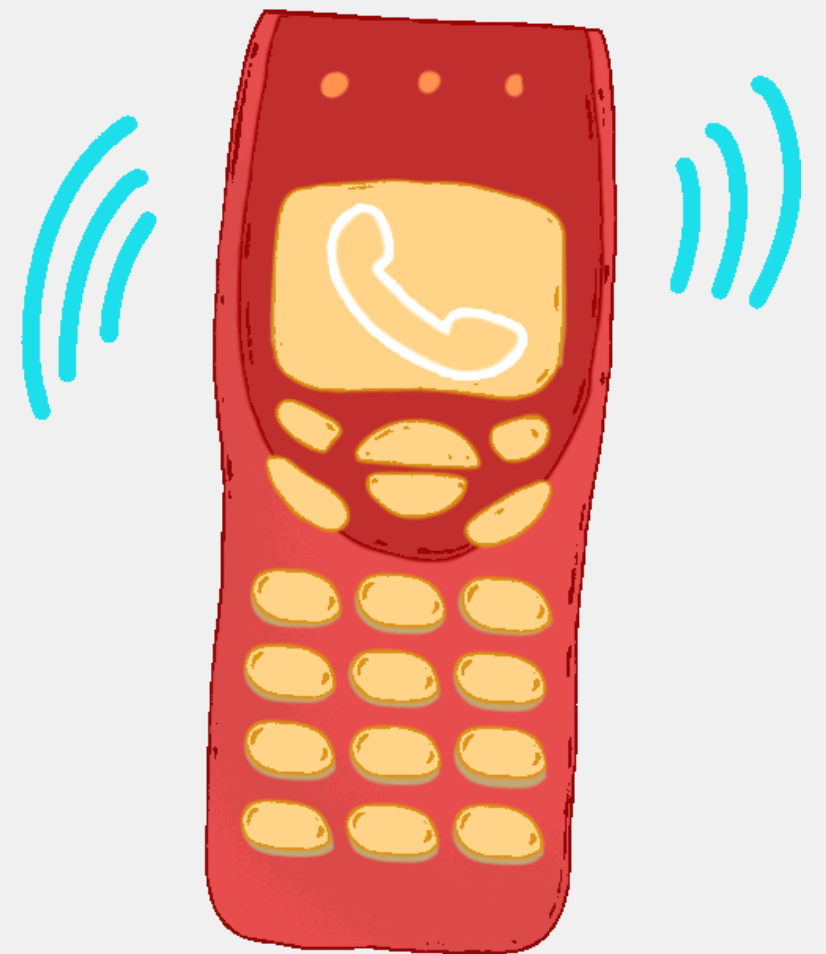




Consejos para prevenir fraudes #6

6

Si necesitas **contactar con tu banco,**
hazlo tú marcando el teléfono de
atención al cliente de tu entidad.





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.





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, para impedir el uso fraudulento de tus datos y contraseñas.





Consejos para prevenir fraudes # 9



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



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 976398630

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