CONSEJOS PARA PROTEGERSE Y EVITAR SER OBJETO DE LOS FRAUDES ONLINE

- 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.
- 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.
- No descargues archivos adjuntos que puedas recibir en el mensaje.
- **Bloquea al remitente** para evitar seguir recibiendo mensajes.
- Si recibes una llamada supuestamente de tu entidad bancaria y te pide datos y contraseñas, corta la comunicación.
- Si necesitas **contactar con tu banco,** hazlo a través del teléfono de atención al cliente de tu entidad.
- 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 y contraseñas personales.
- Si has caído en la trampa o tienes dudas al respecto, ponte en contacto lo antes posible con tu entidad para que pueda bloquear la operación, la tarjeta o tu cuenta, y que puedan seguir haciendo un uso fraudulento de tus datos y contraseñas.
- Acude a la Policía Nacional, Guardia Civil o Juzgado de guardia lo antes posible para interponer una denuncia

OMIC · ZARAGOZA

OFICINA DE SEGURIDAD DEL INTERNAUTA (OSI)

La Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad (iNCIBE) informa a través de su página web, de forma periódica, sobre los nuevos ciberdelitos que surgen, para que la ciudadanía pueda defenderse de ellos.

UCARAGÓN

Colabora

Zaragoza AYUNTAMIENTO

FRAUDES ONLINE

Phishing, vishing, smishing y web spoofing

Unión de Consumidores de Aragón

Delegación Zaragoza: c/Alfonso I, 20, entrlo. centro, 50003, Zaragoza
976 39 76 02 / info@ucaragon.com
Delegación Teruel: C/ Yagüe de Salas 16, 4º izd Edificio Social «Ciudad de Teruel», 44.001 Teruel / 605 02 69 84 / teruel@ucaragon.com

OMIC Ayuntamiento de Zaragoza

Edificio Seminario, Vía de la Hispanidad, 20, planta 1, 50009 Zaragoza
976 72 47 38 / consultasomic@zaragoza.es

OMIC · ZARAGOZA

¿ES SEGURO INTERNET?

Internet pone a disposición de sus usuarios herramientas útiles que hacen nuestro día a día más sencillo. Sin embargo, hay que tener en cuenta que los delincuentes también operan en este medio, por lo que resulta esencial estar preparados para cualquier eventualidad. Phishing, vishing, smishing o web spoofing son parte de los términos con los que debemos familiarizarnos para así estar prevenidos ante un eventual ataque de la ciberdelincuencia.

UCARAGÓN

Colabora

Zaragoza AYUNTAMIENTO

CIBERDELITOS

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.

MÁS FRECUENTES

Entre los ciberdelitos más habituales están los que se hacen pasar por entidades bancarias o de medios de pago online para sustraer nuestro dinero, a través de formas de estafa como son el phishing, smishing, vishing y web spoofing.

PHISHING

Medio utilizado: EMAIL

A través de este medio se busca suplantar la identidad de una empresa, entidad bancaria o de medios de pago online (como PayPal), con el objetivo de robar las credenciales del usuario, información personal, o datos bancarios de cuentas y tarjetas, con el único fin de robarnos dinero.

En dicho email, nos informan de 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.

VISHING

Medio utilizado: LLAMADA TELEFÓNICA

Si se hace clic en el enlace recibido a través de SMS (smishing), a continuación se recibe una llamada telefónica "vishing" en la que el interlocutor se hace pasar por su entidad bancaria o otra empresa 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.

También es posible que solamente se reciba 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, estás autorizando una operación fraudulenta.

SMISHING

Medio utilizado: SMS

En nuestro móvil recibimos un SMS con un enlace. Este mensaje SMS "simula" ser de nuestro banco o cualquier otra empresa. 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.

WEB SPOOFING

Medio utilizado: PÁGINA WEB

Al hacer clic en el enlace que hemos recibido a través de SMS (smishing), se accede a una web fraudulenta (web spoofing) que suplanta la entidad del banco, y captura los datos de tarjetas y/o credenciales de la persona afectada.