Guía sobre

fraudes online

y defensa ante la ciberdelincuencia

Colabora

UCARAGÓN

Zaragoza
AYUNTAMIENTO

Índice

OMIC · ZARAGOZA

La ciberdelincuencia está muy activa en 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.

Y es que 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.

Muchos de los ciberdelitos más habituales son aquellos en los que los ciberdelincuentes se hacen pasar por entidades bancarias o medios de pago online, con el objetivo de hacerse con el dinero de las personas afectadas.

Por ello es más importante que nunca estar alerta, estar documentado y conocer las formas en las que los delicuentes pueden hacerse con nuestros datos y contraseñas para estafarnos.

De esta forma, es conveniente estar familiarizados con términos como Phishing, vishing, smishing o web spoofing, para así estar prevenidos ante un eventual ataque. La información y la formación de la ciudadanía es fundamental para que el uso de las herramientas de la comunicación y la información, imprescindibles en la actualidad, sea una experencia positiva carente de riesgos y problemas.

¿Cuándo no sospechamos de un mensaje?

Los ciberdelincuentes buscan cada día nuevas maneras de ganarse la confianza de las personas para conseguir estafarlas, por lo que es importante estar alerta antes de hacer "click" en un enlace que recibamos. Por eso a veces no nos damos cuenta del engaño y caemos en la trampa.

Por ejemplo, en el caso de estafas bancarias es fácil sospechar del engaño cuando el mensaje que recibimos es de una entidad en la que no tenemos depositados nuestro dinero o productos bancarios. Sin embargo, cuando recibimos un mensaje que asegura ser de nuestra entidad bancaria es más fácil que caigamos en un fraude o estafa.

Pensar y decidir sin prisas, clave para evitar las estafas

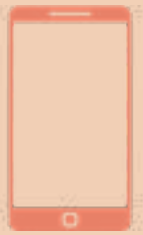
Los ciberdelincuentes nos atraen con una serie de mensajes que aparentan una **falsa sensación de urgencia** para conseguir que tomemos una decisión de forma rápida.

En la mayoría de las ocasiones, pensar antes de actuar es suficiente para darse cuenta de que el mensaje recibido es sospechoso. Por eso, antes de hacer "click" en un enlace recomendamos releerlo en busca de elementos que puedan resultar motivo de alarma.

TIPOS DE ESTAFAS

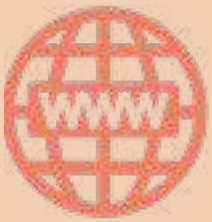
PHISHING
email

VISHING
llamada de teléfono



SMISHING
sms

WEB SPOOFING
página web



Phishing_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.

El método utilizado es el correo electrónico

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.
- Le piden que confirme su identidad y/o contraseñas personales.
- Le ofrecen un premio o participar en algún sorteo.

Smishing_sms

El smishing es un tipo de ataque de ingeniería social que se realiza a través de un teléfono móvil por SMS.

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

El método utilizado es el sms

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 solucionar este supuesto problema, el sms te invita a hacer clic en un enlace. El objetivo de estos mensajes es alarmar al usuario para que realice alguna acción sin pensarlo demasiado.

La comunicación puede inducir al usuario a que llame a un determinado número de teléfono para realizar la gestión, donde se solicitarán los datos que necesita el atacante; o a que pinche en un link que le redigirá a una página web maliciosa, donde se le pedirá al usuario que introduzca sus credenciales de la banca electrónica (usuario y contraseña) u otros datos sensibles.

Web spoofing_página web

Este ciberdelito está relacionado con el resto de ciberdelitos descritos en esta guía, ya que al hacer clic en el enlace recibido a través de SMS (smishing), o correo electrónico (phishing) 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.

El método utilizado es la página web

La web falsa adopta el diseño de la web que se pretende suplantar e incluso una URL similar.

Mediante esta táctica, los ciberdelincuentes consiguen ganarse la confianza de las personas a las que buscan estafar.

El objetivo es hacer creer a los usuarios que están ante un sitio legítimo. Pueden copiar la imagen, la estructura de la página, el contenido que tiene… de manera que la persona que recibe el mensaje cree estar en todo momento en una web de confianza.

Vishing_llamada de teléfono

Este ciberdelito está relacionado habitualmente con smishing. De esta manera, si se hace clic en el enlace recibido a través de SMS, a continuación se recibe una llamada telefónica "vishing" en la que el interlocutor se hace pasar por su entidad bancaria o otra empresa, y le pide un código SMS o sus claves personales para cancelar o resolver la incidencia.

El método utilizado es la llamada de teléfono

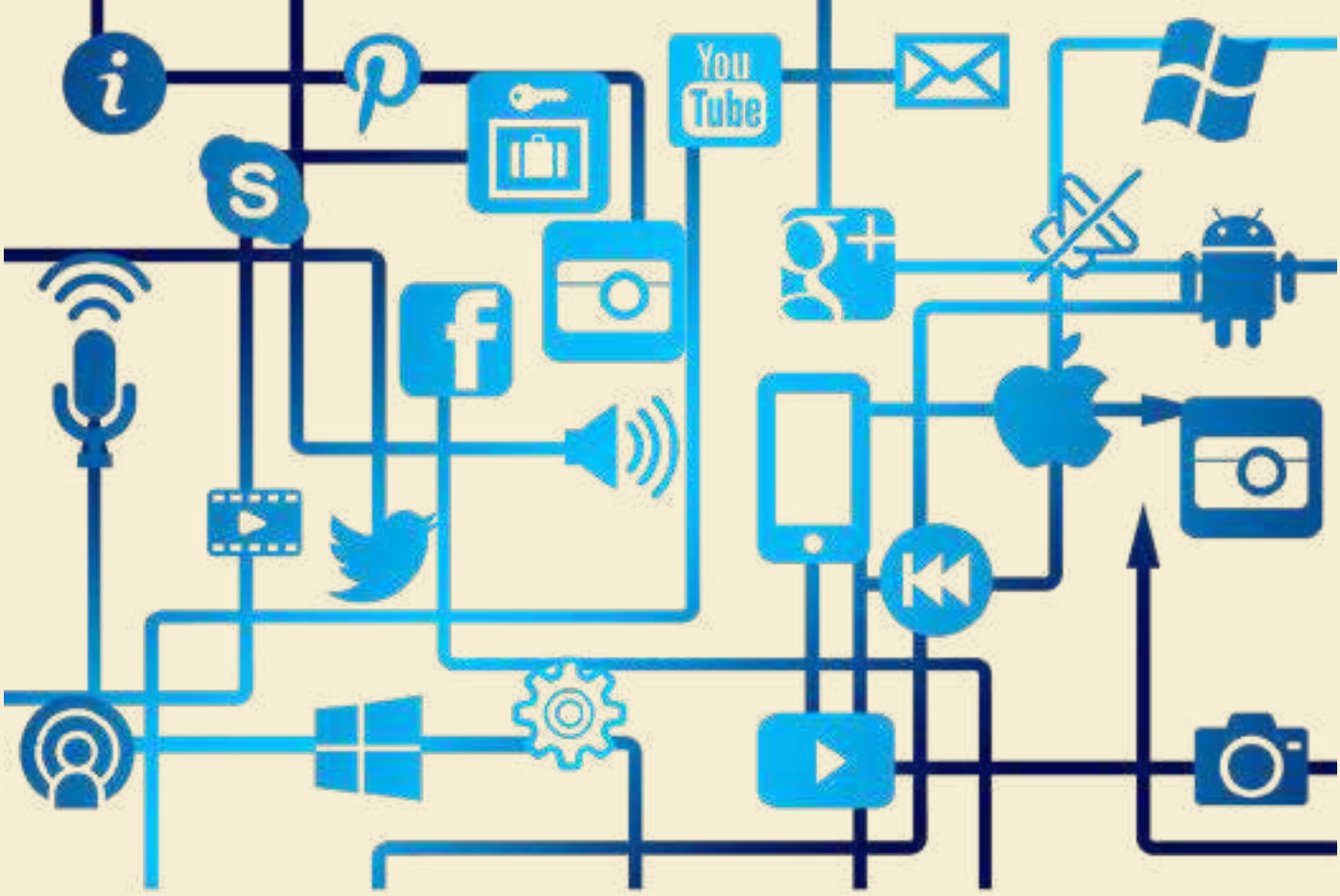
En realidad, lo que está sucediendo es que se está realizando una operación fraudulenta.

Otra de las opciones posibles es que solamente se reciba una llamada telefónica (vishing) haciéndose pasar por su entidad, solicitándole datos personales y contraseñas con el fin de bloquear una operación o compra fraudulenta.

Si en ese momento decide facilitar esta información, lo que está autorizando es una operación fraudulenta.

Consejos para evitar ser objeto de fraudes online

- Desconfíe 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 haga clic en enlaces que reciba en el correo electrónico y en SMS en su teléfono, ni llame a números de teléfono que puedan aparecer en el mensaje.
- No descargue archivos adjuntos que pueda recibir en el mensaje.
- Bloquee al remitente para evitar seguir recibiendo mensajes.
- Si recibe una llamada supuestamente de su entidad bancaria y le pide datos y contraseñas, corte la comunicación.
- Si necesita contactar con su banco, hágalo a través del teléfono de atención al cliente de tu entidad.
- Recuerde que su entidad bancaria nunca le va a solicitar por email, SMS o teléfono sus datos personales, ni datos de cuentas ni tarjetas, ni las claves y contraseñas personales.
- Si ha caído en la trampa o tiene dudas al respecto, póngase en contacto lo antes posible con su 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.
- Acuda a la Policía Nacional, Guardia Civil o Juzgado de guardia lo antes posible para interponer una denuncia.



Esta guía sobre fraudes online ha sido elaborada por la Unión de Consumidores de Aragón en colaboración con el Ayuntamiento de Zaragoza

Colabora

UCARAGÓN

Zaragoza
AYUNTAMIENTO