Fraudes y estafas comerciales

Fraudes a consumidores y recomendaciones para evitarlos

Ayuda y asesoramiento para los consumidores Europeos

ECC-Net

Centro Europeo del Consumidor España

Cofinanciado por la Unión Europea

GOBIERNO DE ESPAÑA MINISTERIO DE CONSUMO

SECRETARÍA GENERAL DE CONSUMO Y JUEGO

DIRECCIÓN GENERAL DE CONSUMO

Actualizado en noviembre de 2021

¿Dónde denunciar fraudes y estafas?

Fuezas y Cuerpos de Seguridad, Ministerio Fiscal y Tribunales

En caso de fraudes o estafas (conductas tipificadas como delitos), corresponde a las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía y Cuerpo de la Guardia Civil), el Ministerio Fiscal y los correspondientes Órganos Judiciales su investigación y persecución. Para los casos de ciberdelitos, se podrá dirigir la denuncia a la Brigada Central de Investigación Tecnológica de la Policía.

INCIBE y OSI

En los casos de ciberdelitos, además de denunciar ante la Brigada Central de Investigación Tecnológica de la Policía, se recomienda notificar el caso ante INCIBE-CERT (Centro de respuesta a incidentes de seguridad del Instituto Nacional de Ciberseguridad). Este Centro dispone de información en su página web www.incibe.es. Cuenta también con distintos canales para contactar, como la línea telefónica gratuita 017, el canal de WhatsApp 900 116 117 o de Telegram @INCIBE017. La Oficina de Seguridad del Internauta (OSI) también proporciona información y el soporte necesario para evitar y resolver los problemas de seguridad online.

Agencia Española de Protección de Datos

Si se hubieran facilitado datos personales como nombre, apellidos o el domicilio, también se recomienda notificar el fradue en la Agencia Española de Protección de Datos.

Deben guardarse siempre los justificantes de pagos, teléfonos de contacto, correos electrónicos o cualquier otro justificante que pueda contribuir a perseguir el delito

ECC-Net

Los Centros Europeos del Consumidor no tienen competencias para actuar en caso de fraudes o estafas

La Red de Centros Europeos del Consumidor (ECC-Net) es un organismo que trata de alcanzar acuerdos amistosos para resolver reclamaciones de consumo transfronterizo europeo entre consumidores y empresas. Los casos de fraude llevados a cabo por presuntos delincuentes o redes organizadas no son un asunto propiamente de consumo, sino presuntas estafas, tipificadas dentro de lo penal, por lo que corresponde a las Fuerzas y Cuerpos de Seguridad del Estado, así como a Jueces y Tribunales de Justicia investigar y resolver los hechos.

Compras online seguras, compras de confianza

El comercio online ofrece grandes ventajas como poder comparar distintos proveedores y ordenar la compra cómodamente. Sin embargo, hay que comprobar la seguridad de la tienda y la calidad de los productos para no caer en un fraude o comprar un producto falso. Recuerda, si un consumidor compra productos falsificados, no solo perderá sus derechos, adquirirá productos de menor calidad, perjudicará la innovación empresarial y formentará la competencia desleal. Tambien estará arriesgando su salud y seguridad.

Cómo evitar ciberestafas y fraudes online

Compra en canales oficiales

Utiliza páginas web y apps oficiales o de confianza. Verifica que el e-mail coincide con la empresa que supuestamente envía el correo. Generalmente, se utilizan dominios públicos o que se parecen al que sería el correo oficial. Sospecha de correos tipo @gmail, @outlook o similar. Los enlaces del correo deben ser comprobados antes de hacer clic en ellos. Comprueba la seguridad de la web colocando el cursor del ratón sobre el hipertexto de la URL (candado o llave). En caso de sospecha, contacta con el proveedor oficial.

Comprueba la identidad del comprador o vendedor

La identidad del comerciante como la dirección, CIF/NIF, la razón social, los datos de contacto, o registro mercantil deben aparecer de forma clara y accesible. Normalmente, en “Aviso legal”, Términos y condiciones” o “Política de privacidad”. En caso de duda, consulta la web oficial de la marca para conocer cuáles son los vendedores autorizados e identificar las tiendas fraudulentas.

- **Productos de segunda mano.** Infórmate de quién es el comprador o vendedor.
- **Productos reacondicionados.** Pueden tener una garantía distinta y que las expectativas del consumidor no se correspondan con las que ofrece el producto nuevo.

Exige buenas prácticas profesionales

Corrobora que la tienda está adherida a un código de conducta y código de buenas prácticas de comercio electrónico. Algunos de los sellos de confianza más conocidos son Confianza Online, Trusted Shops, AENOR, e-comercio, entre otros.

Protege tus datos personales

La empresa debe informar sobre los datos personales que se recogen, su uso y la finalidad. Esta información normalmente se encuentra en el área de “Privacidad” o en “Términos y condiciones”. Debe facilitar también información sobre el uso de cookies.

- **Consejo:**

- **No facilitar datos personales** (financieros, códigos, contraseñas, etc.) por internet o teléfono e informar a la entidad del que supuestamente procede el e-mail, el SMS o la llamada. Las entidades bancarias ni ningún otro proveedor legítimo pedirá al cliente datos personales o claves secretas de acceso.

Comprueba la información del producto

La información del precio total del producto debe ser clara y precisa, debe indicar si incluye o no los impuestos, los gastos de envío si los hubiera y la política de devoluciones. Esta información suele aparecer en los “Términos y condiciones” o el “Aviso legal”. Deberá sospecharse de las páginas web sin estos apartados.

Comprueba tus derechos como consumidor

La web deberá incluir información sobre los derechos del consumidor y las garantías. Por ejemplo, el derecho a desistir en un plazo de 14 días, así como los mecanismos para reclamar, como la plataforma ODR para litigios online.

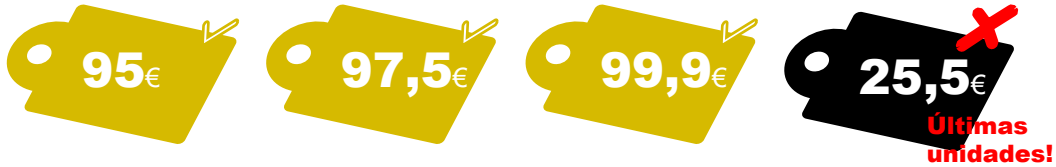
- **Consejo:**

- **Comprueba si existe un servicio de atención al cliente y llama** para verificar si funciona correctamente.

Sospecha de ofertas sorprendentes

Desconfía de aquellas webs que ofrecen precios excesivamente bajos en relación con los del mercado o las tiendas oficiales, así como si todos los artículos se venden al mismo precio. Sospecha si un producto aparece con un precio inicial muy inflado al que se le aplica un descuento muy alto u ofertas demasiado llamativas como para dejarlas pasar.

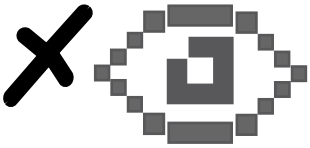
- **Consejo:**
  - **Cuidado con los mensajes que obligan a tomar una decisión rápida**. Comprobar si la urgencia es real. Para ello, consulta otras fuentes de información de confianza.



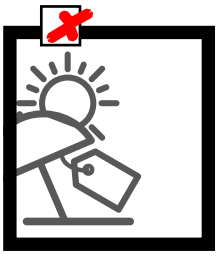
Duda de las webs con fallos en los contenidos

Desconfía de las páginas web que tienen fallos de diseño, imágenes y logotipos de baja calidad o poco profesionales, errores ortográficos o gramaticales. Las imágenes de los productos deben mostrar la totalidad del producto. En caso de duda, solicita más información al vendedor.

La mayoría de los sitios web que venden productos originales parecen profesionales.



La malloría de los si-
tios beb
que benden productos
originales
parrecen proffesionales



Busca opiniones y reseñas

Busca en Internet referencias y opiniones de otros consumidores y comprueba el tiempo que lleva el vendedor con presencia en el comercio online. En caso de duda, desconfiar.

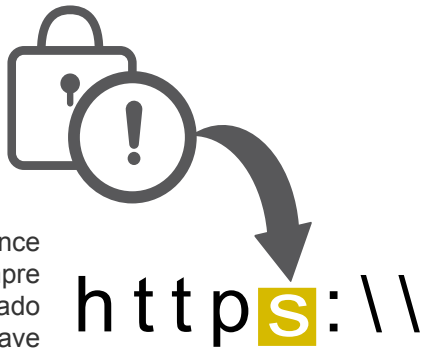
- **Consejo:**
  - Buscar en Internet: “Nombre de la empresa + estafa”

No descargues mensajes, archivos y enlaces sospechosos

No descargues archivos adjuntos o entres en enlaces en caso de que no se pueda confirmar que se trata de un e-mail o SMS legítimo. Es mejor acceder a la información que se ofrece a través de las apps o webs oficiales.

- **Consejo:**
  - **Sospechar de correos con mensajes no esperados, alarmistas o extraños.** Desconfiar si la comunicación es anónima del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”.

Recomendaciones de seguridad



Utiliza conexiones seguras

Comprueba que la web muestre un candado o llave y que su URL comience por http**s**. Evita conexiones wifi públicas gratuitas o abiertas y cierra siempre la sesión al finalizar la compra. Por lo general, para verificar que el certificado digital de la web es válido, basta con hacer clic sobre el icono con forma de llave o candado. Así se verifica quién ha emitido el certificado, para quién y el plazo de validez.

Usa claves y contraseñas seguras

Utiliza contraseñas alfanuméricas y caracteres especiales que no sean deducibles como cumpleaños, aniversarios… No compartas contraseñas y usa una diferente para cada servicio. Crea contraseñas para acceder al dispositivo y establece un bloque de tiempo. Si es posible, utiliza sistemas de autenticación biométrica.

Actualiza el antivirus y software

Comprueba que el sistema operativo y aplicaciones de seguridad del ordenador o dispositivo están actualizados. Las actualizaciones ayudan a proteger los dispositivos de múltiples amenazas y permiten un funcionamiento eficaz de los equipos, reduciendo las probabilidades de fallos.

Paga con sistemas seguros

¿La página web ofrece varias formas de pago pero a la hora de pagar solo acepta tarjeta de crédito? Este es un motivo para desconfiar.

- **Consejos:**
  - **Evitar pagar con transferencias directas** de dinero (como Western Union, Worldremit, Worldplay o Moneycorp).
  - **Pagar preferentemente con tarjeta de crédito**, sistemas de pago a contra-reembolso u otros sistemas de pago seguros como PayPal que aseguren que recibimos el dinero o el producto.
  - **Sospechar si se solicita continuar la gestión fuera de la plataforma de venta**.
  - **Desconfiar si se pide dinero por adelantado**, o pagar más por el producto sin motivo.
  - **Dudar si el vendedor está en el extranjero y exige pagar a un intermediario** para ver el producto.

Ingeniería social, manipular para defraudar

¿Sabías que los ciber-delincuentes utilizan la ingeniería social para defraudar?

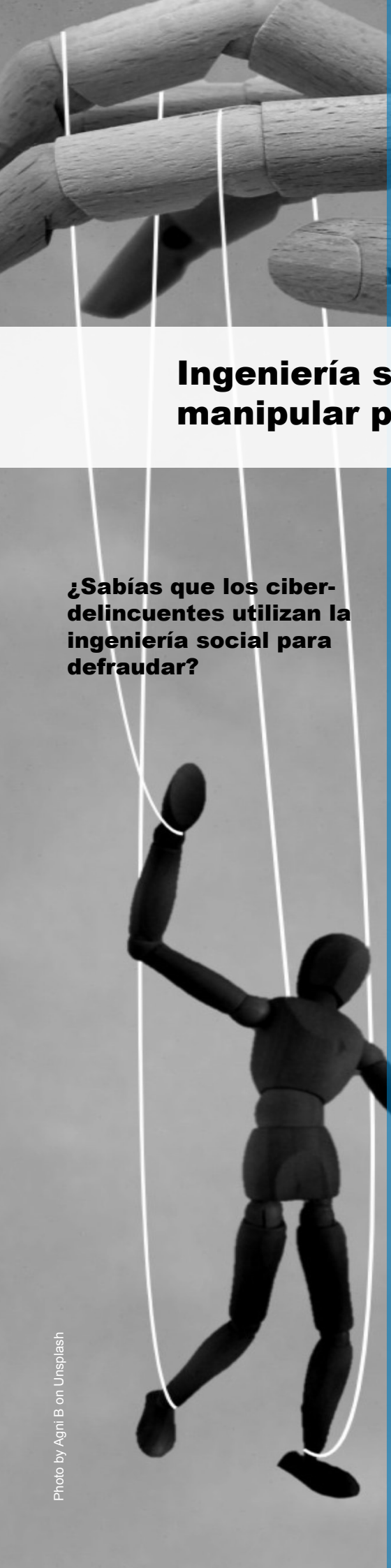


Photo by Agni B on Unsplash

Qué es la ingeniería social?

Cuando hablamos de ciberdelincuencia, generalmente se piensa en complejos códigos maliciosos creados para atacar. Pero ese tipo de ataques requieren una inversión de tiempo, recursos humanos y económicos muy elevados. En realidad, la mayoría de ciberataques se centran en atacar al mayor número de víctimas, con la menor inversión posible. Por eso, la técnica preferida de los ciberdelincuentes es la **ingeniería social**.

En términos de seguridad de la información, la ingeniería social es la manipulación a través de técnicas psicológicas y habilidades sociales que se utilizan para obtener información confidencial, como datos personales o financieros. Estos ataques, a menudo, aparecen como un mensaje de texto o de voz de una fuente aparentemente inofensiva o de confianza.

Canales utilizados

Principalmente el correo electrónico, pero también llamadas telefónicas, aplicaciones de mensajería, o las redes sociales.

Técnicas utilizadas

Falsa autoridad. Los ciberdelincuentes se hacen pasar por autoridades, personas de nuestra confianza o miembros de las Fuerzas y Cuerpos de Seguridad del Estado para conseguir sus fines.

Abuso de confianza. Se aprovechan de la disponibilidad de las personas por ayudar al prójimo, para obtener la información que necesitan. Es el caso, por ejemplo, de un ciberdelincuente que se hace pasar por un falso informático para acceder de forma remota a un ordenador.

Miedo. Amenazan a la víctima con cambios en los términos y condiciones de los servicios contratados, engañándoles con supuestos ataques a sus cuentas online, o cualquier otro engaño para infundir miedo en la víctima y conseguir que termine entrando en páginas web falsas y facilitando sus claves personales.

Extorsión. Coaccionan a la víctima utilizando el miedo de las personas a no ser socialmente aceptados o a perder su reputación. Por ejemplo, los casos de sextorsión.

Falsa gratuidad. Ofrecen un producto o servicio utilizando como señuelo una falsa gratuidad o un llamativo descuento, con el fin de obtener información confidencial.

Ciberestafas a consumidores y fraudes online más comunes

Phising

Técnica utilizada por ciberdelincuentes que suplantan la identidad de personas, entidades y servicios conocidos, engañando a los consumidores para que les faciliten información personal y bancaria. Para ello, envían correos electrónicos y mensajes (SMS) que utilizan como señuelo con el fin de que los consumidores accedan a una web fraudulenta o realicen una acción que ponga en peligro sus datos. En algunos casos, se piden los datos de la tarjeta de crédito que son utilizados para extraer dinero.

> **Spear phishing**
> Modalidad de phishing dirigida contra una persona, organización o empresa específica en la que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima.

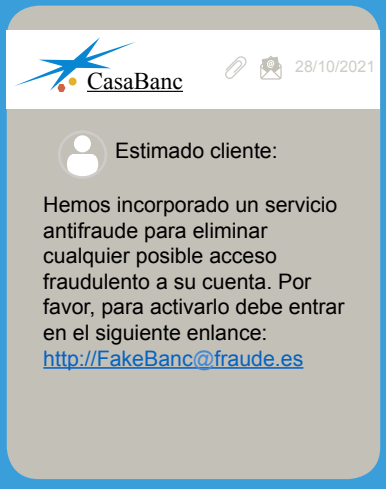
Smishing

Envío de un SMS a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc.- con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente, el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa.

Pueden combinarse distintas técnicas

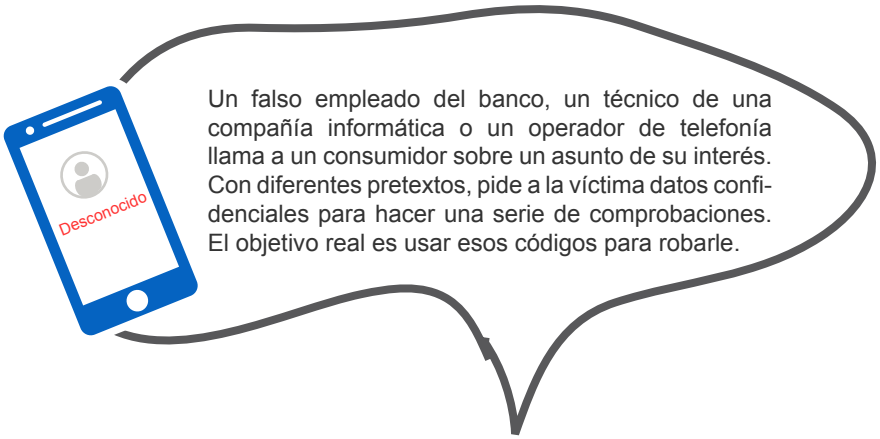
Ejemplo

Fernando recibió un mensaje de su banco donde se le comunicaba que habían incorporado a sus sistemas un servicio antifraude que eliminaría la posibilidad de accesos fraudulentos a su cuenta. Le pareció bien ya que aumentaría su seguridad. El mensaje incluía un enlace a una página web fraudulenta donde tenía que introducir datos personales como el DNI, claves de seguridad, número de tarjeta, fecha de vencimiento, o la firma electrónica. Afortunadamente, Fernando se dio cuenta de que la web no era la de su banco y denunció el hecho a la policía.



Vishing, llamadas telefónicas fraudulentas

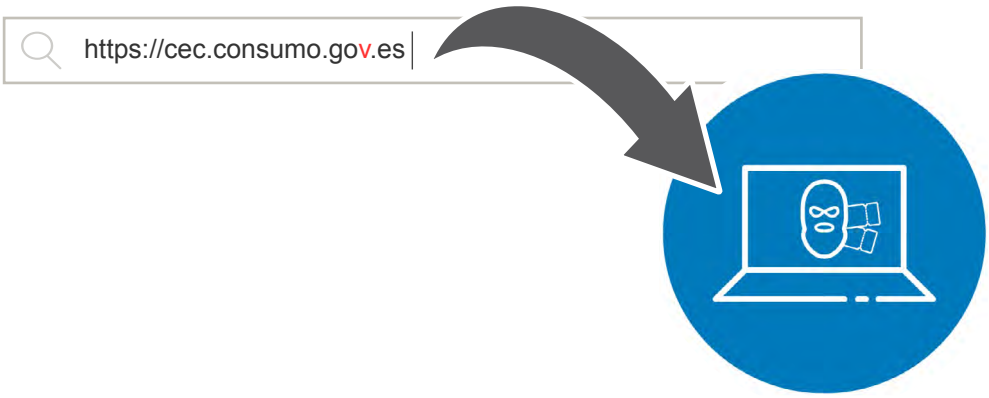
Tipo de estafa en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, para obtener información personal.



Pueden combinarse distintas técnicas

Typosquatting

Se trata de un fenómeno por el cual un usuario acaba en una página web que no es la que estaba buscando por el hecho de teclear erroneamente la URL en su navegador. Los ciber-criminales aprovechan esta situación para llevar al usuario a una página web maliciosa con un dominio (URL) similar al de la web legítima.



Falso comprador y falso vendedor

El falso comprador finge estar interesado en comprar un producto cuando, en realidad, su objetivo es recabar información personal que utilizará para cometer el fraude.

El falso vendedor normalmente pone a la venta productos muy apetecibles a un precio por debajo del de mercado utilizándolo como señuelo para solicitar al consumidor que adelante el dinero de un producto que no recibirá.

Ejemplo

Santiago puso a la venta su bicicleta en Wallapop y rápidamente recibe un mensaje de una persona interesada en comprarla. Llegan a un acuerdo sobre el precio: 235 euros. Antes de quedar para recoger la bicicleta, el comprador dice que pagaría por adelantado a través de Bizum pero en lugar de enviar el dinero, lo que hace es solicitarlo. Santiago, no se fija bien en el mensaje de solicitud y lo acepta, quedándose con la bicicleta, con 235 euros menos en su cuenta y sin volver a saber nada del falso comprador.

Estafas en Bizum

Falso comprador
Una persona interesada en un artículo de segundo mano vendido por un particular solicita el número de teléfono móvil del vendedor para hacerle un bizum en concepto de señal, pero en vez de enviar el dinero hace uso de la funcionalidad de "solicitud". Aunque en el mensaje se especifica claramente que es una solicitud, los estafadores saben que con las prisas es probable que no nos fijemos en ello y caigamos en el engaño.

Falso vendedor
Un supuesto vendedor pone a la venta productos muy llamativos a un precio por debajo del de mercado, y solicita al consumidor que adelante el dinero o una parte para hacer el envío. Una vez realizado el pago por Bizum, el producto nunca llega y el vendedor desparece.

Falsas prestaciones de la seguridad social o ERTEs
El estafador, a través de un SMS o de una llamada (vishing), simula ser un organismo público que se pone en contacto con una persona que tiene que recibir una prestación, informándole que se realizará el envío de dinero por Bizum. De nuevo, realmente se está solicitando el dinero en vez de recibirlo. Recuerda, los organismos oficiales no utilizan este cauce para estos trámites y nunca te solicitarán datos personales.

Falsas recompensas
El ciberdelincuente hace creer al usuario que recibirá una recompensa de una importante cifra de dinero a cambio de pagar una supuesta comisión de unos céntimos. Cuando hae clic en el botón de pagar, en realidad, está regalando al estafador el dinero prometido.

Recomendaciones para evitar estafas en Bizum

Comprueba la identidad del vendedor. En las compras entre particulares, se pierde la condición de consumidor y, por lo tanto, se pierden también muchos de los derechos que se tendrían si la compra se realizara a un profesional.

Utiliza los sistemas de pago internos de las plataformas o de las aplicaciones online. Desconfía si se solicita realizar el pago fuera de la plataforma o app.

Verifica si se está "recibiendo" o se está "solicitando" dinero antes de aprobar la operación.

Verifica que el número de teléfono es el correcto antes de confirmar el pago.

Denuncia ante los cuerpos y fuerzas de seguridad del Estado y comunícalo al banco, en caso de fraude.

Recuerda, en Bizum, el número de teléfono es el identificador único que permite el pago. Los pagos son inmediatos y se realizan de forma irrevocable.

Otros fraudes a consumidores

Estafas en alquiler de viviendas

Este tipo de estafas aparecen en anuncios -principalmente online- de alquileres que tratan de engañar al usuario con viviendas inexistentes o a un precio "súper-chollo". Así captan el interés del consumidor tratando de obtener su dinero lo antes posible. Estos mismos engaños se están dando también en páginas de ventas de vehículos de segunda mano a unos precios inusualmente bajos.

Algunas prácticas sospechosas

- Propietarios que residen en el extranjero y no pueden enseñar el piso en persona.
- Propietarios que sugieren hacer uso de intermediarios para la entregar las llaves o el contrato.
- Propietarios que facilitan poca información o ponen inconvenientes para comunicarse a través de la plataforma de venta.
- Propietarios que no ofrecen la posibilidad de enseñar el inmueble antes de alquilarlo.

- **Consejo**:
  - **Comprobar en Google Maps** si el inmueble es real y se corresponde con lo anunciado. Cuidado, en ocasiones, se citan a empresas como Airbnb o similares utilizando su marca de forma fraudulenta para aparentar mayor credibilidad.

Recomendaciones para evitarlas

Desconfía de ofertas sorprendentes
Mantén una actitud precavida ante alquileres con un precio muy bajo. Compara el precio con el resto de alquileres de la zona.

Sospecha de las webs con contenidos con fallos
Sospecha de las fotos de la vivienda que son copiadas de otra web con marcas de agua (logo o sello transparente superpuesto a una imagen) o si son las mismas que las publicadas en otros anuncios. Los errores ortográficos o frases inconexas son también un indicio de que el anuncio pueda ser falso.

Desconfía de ofertas agresivas
Sospecha de las prisas. Los ciberdelincuentes siempre quieren cerrar el trato rápidamente. Desconfía de los anuncios con ofertas vacacionales sin que el consumidor se haya registrado en ninguna web.

Utiliza sistemas de pago seguros
Sospecha si se solicitan pagos a través de servicios de envío anónimo de dinero como MoneyGram o Western Union. Desconfía si se requiere una transferencia a un banco que no sea de la misma nacionalidad que el "presunto propietario". No aceptes cualquier método de pago. Los servicios de envío de dinero en efectivo o transferencias a cuentas bancarias de países extranjeros dificultan la recuperación del dinero en caso de problemas o fraudes.

- **Consejo:**
  - Asegurarse de que la página de pago comience con "**https**".

Consulta opiniones y reseñas de otros consumidores
Analiza el perfil del vendedor. Lee las valoraciones de otros clientes, comprueba la antigüedad del perfil o los datos de contacto.

Préstamos fraudulentos

Falsos prestamistas ofrecen condiciones aparentemente muy ventajosas para conseguir dinero de forma rápida y sencilla. Para ello, solicitan al consumidor sus datos personales y que adelanten dinero para tramitar el supuesto préstamo, convirtiéndose en víctimas de una estafa.

Ejemplo

Hola Sr. y la Sra.
Por favor, amablemente me permiten esta publicación para compartir y ampliar nuestra ayuda de servicios.
Este mensaje se dirige a las personas, a los pobres, o aquellos que están en necesidad de un préstamo en particular para reconstruir sus vidas. que busca préstamo o elevar sus actividades, ya sea para una beca o para comprar un apartamento, pero no está banco o el archivo fue rechazado en el banco. Yo soy una persona que la concesión de préstamos que van desde 2000 a € 5.000.000 / a todas las personas capaces de cumplir con las condiciones. Yo no soy un banco y no necesito un montón de documentos para confiar en tí, pero tienes que ser una persona justa, honesta, confiable y Sage. Doy préstamos para vivir en toda Europa y la gente de todo el mundo. Estoy a su disposición para satisfacer a mis clientes un máximo de 5 días desde la recepción de tu solicitud. Si usted está interesado, por favor házmelo Póngase en contacto para obtener más información. Aquí está mi dirección de correo electrónico.

Recomendaciones para evitarlos

Utiliza canales oficiales
Solicita préstamos financieros a una entidad oficial, registrada en Banco de España (Registro Estatal de Intermediarios Financieros). Al formalizar un crédito o préstamo, éste debe registrarse en un fichero público de Banco de España que puede ser consultado gratuitamente. Comprobar que la documentación es oficial: contiene sellos oficiales, sin imágenes borrosas y con las rúbricas adecuadas.

Lee los términos y condiciones
Antes de firmar, lee los términos y condiciones. Comprueba que no haya gastos adicionales distintos a los acordados. En caso de no entender algún punto del contrato, consulta con un asesor o especialista, o acude a los organismos de consumo competentes o páginas web especializadas. Pregunta al prestamista qué incluye la cuota, qué sucede si no se paga una cuota, ante quién acudir en caso de discrepancias entre las partes, normativa aplicada, etc. Si la respuesta es ambigua o no responde a las preguntas, se recomienda descartarlo.

Comprueba la normativa aplicable
Si el prestamista es extranjero, debe comprobarse cómo funciona la normativa interbancaria europea.

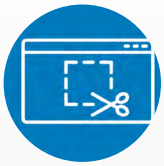
Consulta opiniones y reseñas de otros consumidores
Busca comentarios en la red de otros usuarios y comprueba si los datos del supuesto prestamista como el nombre, apellidos, e-mail o número de teléfono han sido utilizados en otras estafas. Comprueba que los e-mails utilizados no sean una dirección gratuita (@gmail.com, @hotmail.com, etc.)

Utiliza sistemas de pago seguros
Desconfía si se solicita realizar un pago a una tercera persona ajena a la operación. No realices pagos por adelantado. Las comisiones y gastos de gestión se abonan en las cuotas. El pago de las cuotas tampoco debe realizarse a través de empresas de transferencias de dinero rápido.

Desconfía de webs con contenidos con fallos
Desconfía de los anuncios o mensajes con fallos de diseño, errores ortográficos o gramaticales, así como de los anuncios recibidos por e-mail con supuestos chollos o gangas (intereses bajos o sin requisitos para la concesión del crédito).

Comprueba la identidad del comprador
Si el prestamista es extranjero, debe proporcionar datos verificables de registro en su país de origen, así como en España (Código de Identificación Fiscal, registro como sucursal en España, agente declarado por entidades foráneas, así como información del Registro Mercantil).

Presta atención a la publicidad
Los anuncios de posibles estafadores pueden aparecer junto con la publicidad de prestamistas profesionales.



Carding

Actividad que consiste en utilizar de forma fraudulenta numeraciones válidas de tarjetas de crédito/débito para realizar compras online. En estos casos, el titular de la tarjeta tendrá que efectuar la correspondiente denuncia y reclamar la devolución de los cargos efectuados.

Recomendaciones para evitarlo

Revisar periódicamente los movimientos de las cuentas bancarias para detectar cargos sospechosos y poder reclamarlos.

Anular las tarjetas lo antes posible en caso de pérdida o sustracción.

Falso soporte técnico

Los ciberdelincuentes se ponen en contacto con el consumidor haciéndose pasar por profesionales de servicio técnico para alertarle de un supuesto problema de seguridad en su equipo informático. El ciberdelincuente ofrece ayuda para desinfectar el ordenador del supuesto virus o malware (programa informático que se ejecuta sin conocimiento ni autorización del usuario para realizar funciones perjudiciales) solicitándo –por ejemplo- que entre en determinadas páginas web, descargue software, llame a un número de teléfono, que le autorice a acceder al ordenador por control remoto o incluso que le facilite su tarjeta o datos bancarios. Como consecuencia, el ciberdelincuente puede amenazar con mantener bloqueado el ordenador hasta que se abone una cantidad de dinero.

Ejemplo

Carlos recibe, por sorpresa, una llamada de un supuesto técnico que no habla bien ni español ni inglés y le comunica que su ordenador tiene un virus, además de otros problemas de seguridad, y que necesita acceder a su equipo para solucionarlos. Carlos le facilita el acceso por control remoto y acaba con el ordenador bloqueado. Para desbloqueárselo, le piden que haga una transferencia de dinero. Por suerte, Carlos no pagó el dinero y lo denunció a la policía.

Recomendaciones para evitarlo

No sigas las indicaciones del ciberdelincuente
No fiarse de las llamadas recibidas de un supuesto servicio técnico sin que se haya solicitado expresamente. Mantén la calma y no sigas las indicaciones de los ciberdelincuentes. En caso de duda, se recomienda cortar la comunicación y reportar el incidente al proveedor oficial. No permitas que alguien use tu equipo por control remoto sin haber comprobado su identidad. Si se ha concedido acceso a los estafadores, considerar restablecer el dispositivo.

Utiliza canales oficiales
Instala Apps originales desde las páginas web oficiales. Desinstala, lo antes posible, las aplicaciones que los estafadores hayan podido instalar. Comprueba si se ha detectado algún incidente de seguridad relacionado con botnets (ordenadores infectados por ciberdelincuentes para llevar a cabo acciones maliciosas) u otras amenazas a través del Servicio AntiBotnet de la Oficina de Seguridad del Internauta.

Usa dispositivos seguros
Cambia frecuentemente las claves de acceso de las aplicaciones y servicios.

Actualiza el antivirus y software
Analiza con las herramientas de análisis y desinfección que se dispongan si realmente el equipo se encuentra en riesgo. Descarga las actualizaciones de seguridad.

Cancela los cobros fraudulentos
Contacta con el banco para cancelar los pagos efectuados.

Falsas ofertas de empleo

Los ciberdelincuentes se aprovechan de candidatos que están en búsqueda de empleo publicando ofertas falsas y solicitándoles pagos por adelantado en concepto de gestión, seguro médico o formación inicial.

Ejemplo

Cristina envía su curriculum para participar en un proceso de selección. Pasados unos días la empresa le comunican que ha sido seleccionada. El correo proviene de otra empresa distinta, con faltas de ortografía y expresiones no habituales. Además, no se le convoca a ninguna entrevista por lo que el único criterio en el que se basan para contratarla es el curriculum. Tampoco le confirman ni el área en el que trabajará, ni el puesto. Unos días más tarde, recibe otro mensaje de la empresa que ofrecía el trabajo, proporcionando algún detalle más: fecha de inicio, duración y puesto concreto, pero que debe pagar 500 euros a través de MoneyGram por los gastos administrativos. Ese dinero se le devolvería en la primera nómina. Más tarde, se le informa de que se le está gestionando también su seguro de vida, pero que debe asumir un porcentaje del importe total. Por suerte, Cristina no pagó el dinero y lo denunció a la policía.

Recomendaciones para evitarlas

Desconfía de las webs con contenidos con fallos
Desconfía de las ofertas mal redactadas, faltas de ortografías o con una descripción vaga de la oferta.

Consulta opiniones y reseñas de otros candidatos
Busca información en internet de la empresa que oferta la vacante. Si no existe o no hay apenas referencias de la empresa, lo más probable es que sea un fraude.

Utiliza canales oficiales
Evita contestar los e-mails, especialmente si no se conoce la cuenta o el nombre del remitente o si es una cuenta gratuita tipo @gmail, o @ hotmail. Realiza las búsquedas de empleo en portales contrastados y de instituciones u organismos oficiales, comprobando siempre la política de protección de datos personales.

No descargues archivos y enlaces sospechosos
No descargues posibles ficheros adjuntos ni hagas clic en los enlaces.

Protege tus datos personales
No facilites datos bancarios ni realices ningún ingreso a cuentas bancarias.

Prácticas sospechosas
Sospecha de las ofertas que solicitan llamar a números de teléfono de tarificación especial (803, 806, 807, 905, 907…). Si se solicita dinero, seguramente es un fraude. Si se solicita al candidato que compre los materiales necesarios para desempeñar el trabajo, seguramente es un fraude. Sospecha de ofertas con salarios muy elevados.

Cartas nigerianas

Cartas en las que se prometen negocios muy rentables. El estafador se hace pasar por un abogado, familiar o amigo de un miembro del Gobierno o de un hombre de negocios que ha perdido la vida y dispone de una gran cantidad de dinero. Este asegura que tiene acceso legal al dinero y pretende transferirlo a una cuenta en el extranjero. Para ello, solicita a la víctima que abra una cuenta bancaria. Una vez abierta, comunica que han surgido unos problemas inesperados y que para solucionarlos, hay que pagar impuestos, honorarios o tasas especiales. Cuando la víctima deja de pagar, el estafador desaparece. En ocasiones, pasado un tiempo, vuelven a contactar con la víctima haciéndose pasar por investigadores que tienen conocimiento de la estafa y ofrecen su ayuda para recuperar el dinero perdido.

Recomendaciones para evitarlas

No contestes a este tipo de comunicaciones.

No facilites datos bancarios, ni personales.

En caso de haber contactado con los estafadores o haber abonado alguna cantidad, guarda todos los documentos recibidos, los mensajes enviados y resguardos de las transacciones.

Contacta con las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía y Cuerpo de la Guardia Civil), el Ministerio Fiscal y los correspondientes Órganos Judiciales.

Fraudes en loterias

En este tipo de estafas se utilizan nombres como El Gordo o El Niño. para hacer creer a la víctima que es la Lotería Nacional del Estado. Los estafadores le envían un e-mail informando de que ha ganado la lotería -a pesar de que no ha participado en ningún sorteo- y le piden que contacte con un agente. El agente solicita que rellene un formulario para verificar su identidad y que envíe una copia de su pasaporte o DNI. A continuación, normalmente a través de un e-mail, se ofrecen tres posibilidades de cobro: transferencia bancaria, abrir una cuenta en un banco determinado para ingresar el premio, o recoger el dinero personalmente (normalmente en un país alejado). Antes de abonar el premio, solicitan que se pague una suma de dinero. Una vez efectuado este pago, los estafadores desaparecen.

Recomendaciones para evitarlos

No respondas a ningún mensaje.

No envíes dinero.

No facilites datos bancarios o personales.

En caso de haber contactado con los estafadores o haber abonado alguna cantidad, guarda todos los documentos recibidos, los mensajes enviados y resguardos de las transacciones.

Contacta con las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía y Cuerpo de la Guardia Civil), el Ministerio Fiscal y los correspondientes Órganos Judiciales.

Slamming

Cambio de compañía de telecomunicaciones sin la autorización del cliente, utilizando técnicas fraudulentas. En estos casos, los usuarios se encuentran con que sus servicios de telecomunicaciones han sido “traspasados” a otro operador sin el consentimiento del titular.

Ejemplo

Jorge recibe una llamada de una compañía telefónica para ofrecerle un llamativo descuento. Cuando el comercial le pregunta si le parece interesante esa oferta, Jorge le dice que sí. Entonces, la compañía le pide sus datos personales con la escusa de que le mandarían más información. A partir de esa llamada, Jorge descubre, por sorpresa, que su proveedor de telefonía ha cambiado sin que él haya solicitado ese cambio.

Recomendaciones para evitarlo

Lee los términos y condiciones
Lee cuidadosamente toda la información sobre ofertas recibidas por correo antes de autorizar la aceptación de la oferta. Asegúrate de que se entienden, de forma clara, las tarifas y los términos y condiciones establecidos en la oferta de servicios.

Comprueba la identidad del vendedor
Ante cualquier cambio en el nombre de la compañía, llama al operador y solicita información.

Rechaza claramente las ofertas no deseadas
Si no se quiere contratar una oferta, hay que decir NO de forma clara. Una mera receptividad a la información puede ser interpretada por el operador como un consentimiento.

Si no se desea contratar un servicio, se recomienda no facilitar datos personales ni información bancara. El mero hecho de proporcionar estos datos podría interpretarse como una contratación del servicio o se podrían utilizar esos datos para solicitar, en nombre del consumidor, un cambio de titularidad en los servicios.

Antes de decir “SÍ” a un nuevo plan de ahorro, hay que asegurarse de que la oferta presentada es del operador contratado. Para ello, se recomienda contactar con la compañía y verificar si la promoción es legítima. Cualquier aceptación puede ser grabada y utilizada como prueba de solicitud de cambio de operador.

Recovery Room

Fraude realizado por empresas denominadas “recovery room” que contactan con personas que han sido víctimas de “chiringuitos financieros” (entidades financieras no autorizadas) y les proponen gestionar la recuperación de las pérdidas o recomprar las acciones o valores adquiridos.

Recomendaciones para evitarlos

Comprueba la identidad del vendedor
No respondas a ofertas de recompra de acciones o de recuperación de pérdidas sin antes cerciorarte de que se trata de empresas con referencias positivas o fiables.

Prácticas sospechosas
Desconfía si una empresa “Recovery Room” contacta contigo sin haberlo solicitado y te piden dinero por adelantado en concepto de pago de impuestos, honorarios o pólizas de seguro como requisito previo. Desconfía si recibes una supuesta llamada de la Comisión Nacional del Mercado de Valores (CNMV) con el fin de recuperar las pérdidas sufridas. La CNMV no contacta directamente con los afectados, ni autoriza el uso de su identidad, imagen corporativa o dominio cnmv.es con el fin de recuperar las pérdidas.

Cuentas de trading financiadas fraudulentas

Las cuentas de trading financiadas son servicios ofrecidos normalmente en páginas web que ofrecen la posibilidad de acceder a una cuenta de valores para realizar operaciones sin que el usuario arriesgue capital propio. La página web es la que aportaría el capital y ofrece al consumidor un porcentaje de las ganancias obtenidas. Sin embargo, para hacer usos de esas cuentas se obliga al usuario a realizar un curso cuyo coste, en ocasiones, asciende a varios miles de euros. La contratación de estos cursos podría suponer un riesgo de fraude o engaño en cuanto a la posibilidad de acceso a esas cuentas de trading.

Recomendaciones para evitarlas

Comprueba la identidad del vendedor
Averigua en Internet todo lo posible sobre la empresa y si no se obtienen resultados en la búsqueda, desconfía. Comprueba si los datos de la empresa como el nombre, apellidos, e-mail o número de teléfono han sido utilizados en otras estafas. Coteja que los e-mails utilizados no sean una dirección gratuita: @gmail, @hotmail, etc.

Consulta opiniones y reseñas de otros consumidores
Busca comentarios de otros usuarios.

Lee los términos y condiciones
Antes de firmar el contrato, lee los términos y condiciones. En caso de no entender algún punto del contrato, consulta con un asesor o especialista o acude a los organismos de consumo competentes o a páginas web especializadas.

Utiliza conexiones seguras
Comprueba que la página de pago es segura. Es decir, cuya dirección URL comience por https, y muestre un candado o llave.

Utiliza sistemas de pago seguros
Desconfía si una empresa obliga a realizar pagos o contratar servicios adicionales con costes a cambio de poder acceder a una cuenta de valores. Sospecha de los pagos que se soliciten hacer a una tercera persona ajena a la operación.

Desconfía de las webs con contenidos con fallos
Desconfía de los anuncios o mensajes con fallos de diseño, errores ortográficos o gramaticales, así como de los anuncios recibidos por e-mail con supuestos chollos o gangas (intereses bajos o sin requisitos para la concesión del crédito).