

PROTEGE LO TUYO:

GUÍA PRÁCTICA PARA PERSONAS MAYORES FRENTE A FRAUDES



Las personas mayores son las víctimas perfectas de los fraudes en las ventas a domicilio, en excursiones comerciales, en ventas por teléfono, así como a través de medios digitales.

Las personas mayores permanecen mucho tiempo en casa, disponen de tiempo libre para hablar, están dispuestos a escuchar y, la falta de familiaridad o destreza con las nuevas tecnologías, unida a su mayor vulnerabilidad, les convierte en el objetivo perfecto de los estafadores.

Por ello, resulta imprescindible saber prevenir y detectar determinadas situaciones y mantenerse informado para reducir el riesgo de ser víctima de un fraude.

En la Unión de Consumidores de Aragón llevamos muchos años ofreciendo consejos de seguridad a las personas mayores y a otros colectivos especialmente vulnerables, haciendo como norma general la siguiente recomendación

ATRÉVASE A DECIR:

“NO ME INTERESA”

Consejos de seguridad general en su vivienda

- Por su seguridad, jamás abra la puerta a personas desconocidas, ni siquiera a través del portero automático.
- Desconfíe si llaman en nombre del cartero en horarios que no son de reparto.
- Desconfíe de las personas que se presentan en su domicilio bien arregladas o tienen buena presencia, es para ganarse su confianza.
- No es recomendable permanecer al otro lado de la puerta y preguntar ¿quién llama? Con ello pone de manifiesto que se encuentra solo en la vivienda.
- No abra la puerta, aunque sea un poco, para ver quién es, ya que de un empujón pueden acceder al interior de la vivienda.
- Si vive solo, procure que figure alguna persona más en la placa del buzón. Se recomienda que figure la inicial en lugar del nombre completo, para no dar pistas de si es hombre o mujer.
- Si le llaman por teléfono, nunca diga si vive solo, ni facilite información sobre su nombre y apellidos, DNI, ingresos o datos bancarios.
- Si al otro lado de la puerta hay personas desconocidas que insisten en acceder a su domicilio, llame a la Policía Nacional (091), y si dispone del servicio de teleasistencia, pulse el botón de alarma, para manifestarles que se encuentra ante una situación de riesgo o peligro.

Fraudes más habituales

PRODUCTOS MILAGRO

Las personas mayores son especialmente vulnerables ante la publicidad engañosa de “productos milagro” que prometen curas milagrosas o beneficios extraordinarios para la salud. Desconfíe de frases como “cura todo”, “resultados inmediatos” o “científicamente probado” ya que no existe seguridad de que cumplan con la función terapéutica que publicitan. Su venta es un fraude para el consumidor y puede suponer un grave riesgo para la salud y también para su economía.

Productos milagro más habituales

- Aparatos de magnetoterapia con campos magnéticos que eliminan dolores, así como mantas y colchones.
- Cremas y otros productos para dolores, arrugas, adelgazar o dejar de fumar.
- Pulseras magnéticas y aparatos de masajes.
- Filtros de agua magnetizada o imantada.
- Productos que curan el cáncer.



Algunos de estos productos, como los aparatos de magnetoterapia, tienen un precio elevado, ofreciendo los comerciales la posibilidad de financiación inmediata a pagar en cómodos plazos, lo que incrementa su precio.

EXCURSIONES CON FINES COMERCIALES

Gran cantidad de productos, incluso los productos milagro, suelen venderse en excursiones con fines de promoción comercial.

En numerosas ocasiones, las empresas que se dedican a este tipo de ventas se ponen en contacto con asociaciones de personas mayores para ofrecerles una excursión a buen precio a cambio de recibir un obsequio. La finalidad de la excursión es intentar vender los diferentes productos con el gancho de recibir un regalo, creando en las personas mayores una necesidad de comprar estos productos para mejorar sus dolencias o enfermedades, por lo que resulta muy fácil caer en la tentación de comprar.

Atrévase a decir: No me interesa

CAMBIO DE COMERCIALIZADORA DE LUZ Y GAS

Las empresas comercializadoras de luz y gas tienen la prohibición de hacer publicidad “puerta a puerta”, y tampoco pueden realizar la contratación de sus productos a domicilio, salvo que el consumidor haya aceptado expresamente concertar una cita con esa finalidad.

Actualmente, la mayoría de cambios de comercializadoras de luz y gas se realizan a través de llamada telefónica.

Se trata de llamadas comerciales muy agresivas en las que el operador se identifica como de la compañía de luz o gas con la que Vd. tiene el contrato de suministro, o bien de otra comercializadora, con el fin de ofrecerle una mejor tarifa o con la excusa de haber detectado un error en su factura.

Lo que pretende el comercial es que le facilite los datos de su factura, y el CUPS que figura en la misma (código unificado de punto de suministro), así como los datos de su cuenta bancaria, con el único fin de cambiarle de comercializadora y/o de tarifa, sin que Vd. sepa realmente si le interesa la oferta. Además, suelen aprovechar para añadir en la contratación servicios adicionales (revisión de la caldera, seguros de impagos...) que Vd. no desea ni necesita.

Tenga en cuenta que si es beneficiario del bono social de la luz está en el mercado regulado (tarifa PVPC). Por tanto, si cambia su contrato a una comercializadora del mercado libre, pierde el descuento del bono social de la luz.

Las ofertas comerciales que recibimos son de comercializadoras del mercado libre, por lo que tenga especial atención con las mismas.

CAMBIO DE OPERADORA DE TELEFONÍA

Al igual que en los suministros de luz y gas, hay que prestar especial atención a las llamadas telefónicas ofreciendo una rebaja en sus servicios de internet y telefonía fija o móvil. Otra estrategia comercial es comunicarle que hay problemas de cobertura de la línea y, ante la imposibilidad de mantener el servicio, le han asignado otra operadora, o que ahora su operadora ha cambiado el nombre comercial.

No podemos saber realmente si nos llama nuestra operadora o es otra empresa que se hace pasar por ella. El único fin es conseguir un nuevo cliente. Tenga en cuenta que, si cambiamos de operadora y teníamos permanencia en el contrato, tendremos que pagar una penalización.

Tanto en luz, gas y telefonía debemos exigir que nos faciliten en un soporte duradero la propuesta con las condiciones del nuevo contrato, a fin de estudiarlo y si nos resulta de interés, poder formalizar el mismo.

En los procesos de contratación por vía telefónica, se procede a grabar la conversación, y el consumidor debe pronunciar la palabra “Sí” como respuesta a las preguntas para aceptar la contratación.

Cuando descuelgue el teléfono, no utilice la palabra “Sí” a fin de evitar que se manipule la grabación de una conversación y pueda considerarse que está conforme con la oferta realizada.

Por tanto, ante cualquier llamada comercial

Atrévase a decir: No me interesa

FALSAS REVISIONES DEL GAS

Los fraudes en las revisiones de las instalaciones del gas butano son un clásico que, cada cierto tiempo, reaparece en zonas determinadas donde los falsos revisores intuyen que pueden encontrar a personas mayores a las que engañar.

Es frecuente que los **“presuntos revisores del butano”** vayan al domicilio con la excusa de hacer la revisión y alertando del peligro de no hacerla.

Con esta excusa, es muy fácil que el consumidor acceda a que el revisor entre en su casa.

Una vez dentro, siempre encuentran fallos que reparar, o bien la goma del butano está rajada y/o el cabezal está defectuoso.



Son falsas reparaciones o sustituciones por las que cobran un precio excesivo (normalmente en efectivo), emitiendo facturas elevadas, si es que las emiten.

Tenga en cuenta que la goma del butano lleva la fecha de caducidad impresa en la misma, y su cambio puede hacerlo directamente el usuario.

Recuerde que antes de contratar el servicio, puede pedir presupuesto por el servicio.

Con respecto a la **revisión de la instalación de gas natural**, es obligatoria realizarla cada cinco años. Para ello, la empresa distribuidora de gas comunica al consumidor por carta y por carteles en el edificio la fecha en la que se va a realizar. Esa revisión nunca hay que abonarla al técnico que efectúa la revisión, ya que el importe de esta se carga en la factura del suministro de gas.

CONTROL DEL AGUA DEL GRIFO

Si recibe llamadas telefónicas o visitas con la excusa de ser personal del Ayuntamiento para hacer un control sobre la calidad del agua del grifo, tenga la certeza de que se trata de una empresa que vende filtros o aparatos depuradores de agua, que le convencerán de la necesidad de comprar su producto y de lo perjudicial que es para su salud el beber agua del grifo. Los ayuntamientos nunca actúan así.

Son aparatos con un precio elevado, y siempre le ofrecerán una financiación inmediata.

Atrévase a decir: No me interesa

FALSOS PREMIOS O SORTEOS

Si recibe una llamada telefónica, un mensaje en el teléfono móvil o un correo electrónico con la noticia de haber ganado un premio, y que para recibirlo debe facilitar datos personales y/o bancarios, o debe llamar a algún teléfono o acceder a algún enlace, no lo haga actuando de manera impulsiva, ya que lo más seguro es que se trate de un fraude.

LLAMADAS O MENSAJES PARA RECAUDAR FONDOS EN NOMBRE DE ONG

Desconfíe de llamadas telefónicas o mensajes realizadas en nombre de ONG con el fin de que se haga socio, realice aportaciones económicas o les facilite datos bancarios. Hay estafadores que recaudan fondos utilizando nombres de organizaciones sociales.

Si desea hacerse socio o realizar aportaciones puntuales a organizaciones sociales, póngase Vd. en contacto con ellas para realizar la aportación.

VISITAS, LLAMADAS O MENSAJES EN NOMBRE DE LA ADMINISTRACIÓN

Desconfíe de visitas, llamadas o mensajes en nombre de diferentes administraciones públicas (Ayuntamiento, Seguridad Social, Agencia Tributaria...)

La administración pública nunca se personará en su domicilio ni le llamará o mandará mensajes para comprobar datos personales relativos a su pensión, ni le solicitará que facilite sus datos bancarios.

Derecho de desistimiento en los contratos

En los contratos realizados a distancia y fuera de establecimiento mercantil **el consumidor tiene derecho a desistir del contrato sin alegar motivo alguno.**

En los contratos realizados a distancia (por teléfono o internet), el plazo para desistir del contrato es de 14 días naturales.



En los contratos celebrados fuera de establecimiento mercantil (visitas no solicitadas y efectuadas en el domicilio del consumidor, o excursiones organizadas con el objetivo de promocionar o vender productos o servicios), el plazo de desistimiento es de 30 días naturales.



Si el empresario no facilita al consumidor la información sobre el derecho de desistimiento, el plazo para desistir finalizará 12 meses después de la fecha de terminación del periodo inicial, es decir:

Contratos a distancia: 14 días naturales + 12 meses.

Contratos fuera de establecimiento mercantil: 30 días naturales + 12 meses.

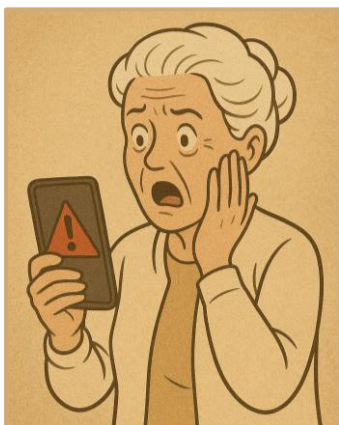
Fraudes que utilizan las nuevas tecnologías

Cada vez es más habitual que las personas mayores utilicen teléfonos móviles, ordenadores y tablet, así como el correo electrónico y redes sociales para mantenerse conectados con sus familiares y amigos, y para efectuar gestiones con las entidades bancarias, la administración y efectuar compras por internet. A medida que la tecnología evoluciona, las tácticas de los ciberdelincuentes (personas que utilizan internet para hacer fraudes y estafas) también van dirigidas a las personas mayores desprevenidas. El riesgo de ser víctimas de un fraude es mayor que nunca, ya que el colectivo de personas mayores está menos familiarizado con las nuevas tecnologías.

ESTAFA DEL HIJO O DEL NIETO

Es un medio de engaño que apela a los sentimientos.

Los estafadores se hacen pasar por hijos o nietos que están en apuros económicos o les han robado el móvil. A través de llamada telefónica o por envío de mensajes de WhatsApp solicitan que les envíe dinero rápidamente.



Debe verificar la identidad de la persona que le llama antes de mandar ningún dinero.

Por ello contacte con sus familiares antes de acceder a la petición de los estafadores enviando el dinero.

ESTAFAS DE SOPORTE TÉCNICO

Los estafadores se hacen pasar por técnicos informáticos o proveedores de programas informáticos, que afirman que su dispositivo tiene un virus o necesita una actualización urgente.

Le solicitarán acceso remoto a su ordenador y exigirán que realice un pago.

Nunca acceda a esta petición, ya que se hacen con el control del ordenador y acceden a datos, contraseñas y claves personales.



FRAUDES POR CORREO ELECTRÓNICO (PHISHING)



El phishing es un fraude donde el ciberdelincuente **remite correos electrónicos**. En inglés, este fraude se denomina **“Phishing”**.

A través del correo electrónico suplanta la identidad de un tercero como bancos, empresas o administración pública.

Su objetivo es robar información personal o bancaria (contraseñas, datos de cuentas bancarias y de tarjetas de crédito).

En dicho correo electrónico, 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 ofrece un premio o participar en algún sorteo.

Lea bien el mensaje, piense y no haga clic en el enlace. Si lo hace se instalará un virus o programa informático que dañará el dispositivo y accederán a datos personales, cuentas bancarias y contraseñas, con los que podrán estafarle.

FRAUDES POR SMS (SMISHING)



Se realizan a través de **mensajes SMS que llegan al teléfono móvil simulando la identidad de un tercero**. En inglés, este fraude se denomina **“Smishing”**.

A través del SMS alertan de un problema, por ejemplo, que han detectado que se está realizando una transferencia bancaria desde la cuenta y es urgente proceder para anular la misma.

El SMS le invita a hacer clic en un enlace con urgencia, o bien recibe a continuación una llamada telefónica para resolver la incidencia cuando, en realidad, se está realizando una operación fraudulenta.

FRAUDES POR PÁGINAS WEB FALSAS (WEB SPOOFING)



Es un fraude donde **el ciberdelincuente crea páginas web falsas que imitan a las páginas web reales** de terceros. En inglés, este fraude se denomina **“Web spoofing”**.

Los ciberdelincuentes envían un SMS o un correo electrónico con un enlace que nos lleva a la página web falsa, siempre con urgencia para que accedamos al enlace.

La página web falsa pide nuestra contraseña y los ciberdelincuentes roban nuestros datos.

FRAUDES POR LLAMADAS DE TELÉFONO (VISHING)



Es un fraude donde **el ciberdelincuente llama por teléfono suplantando la identidad** de un tercero. En inglés, este fraude se denomina **“Vishing”**.

El ciberdelincuente nos pide información personal o contraseñas con la excusa de que han detectado un problema y es urgente resolverlo. Si facilitamos esa información, realizan un fraude con nuestros datos.

Consejos para evitar fraudes por internet

- Desconfíe de mensajes o llamadas que requieran actuar urgente.
- No haga clic en enlaces de SMS o correos electrónicos, ni llame a los números de teléfono que aparezcan en el mensaje.
- No descargue archivos que pueda recibir en el mensaje.
- Bloquee a los remitentes de SMS, de correos electrónicos y de llamadas telefónicas, para no recibir más mensajes ni llamadas.
- Su banco nunca le pedirá datos personales ni números de cuenta o tarjeta y contraseñas por teléfono, SMS o correo electrónico.
- Si recibe una llamada en nombre de su banco solicitándole esos datos, no los facilite y cuelgue el teléfono.
- Si necesita contactar con su banco, hágalo a través del teléfono de atención al cliente de la entidad.
- Si ha sido víctima de un fraude o tiene dudas, llame a su banco lo antes posible para que bloquee la cuenta bancaria o la tarjeta de crédito, y así evitar que puedan seguir haciendo un uso fraudulento de sus datos y contraseñas.
- Para identificar una página web segura, verifique que dispone de un candado a la izquierda y que comience por “https” en lugar de por “http”. Sospeche de páginas web con errores gramaticales y faltas de ortografía.
- Acuda lo antes posible a la Policía Nacional, a la Guardia Civil o al Juzgado de guardia para interponer una denuncia.

Puedes recibir más información en la Unión de Consumidores de Aragón

Oficina en Zaragoza

Calle Alfonso I, 20. Entresuelo, centro.

Código postal: 50003, Zaragoza.

Teléfono: 976397602

Correo electrónico: info@ucaragon.com

Oficina en Huesca

Calle del Parque, 9

Código postal: 22003, Huesca

Teléfono: 976397602

Correo electrónico: info@ucaragon.com

Oficina en Teruel

Calle Yagüe de Salas, 16. 4º izquierda.

Código postal: 44001, Teruel.

Teléfono: 605026984

Correo electrónico: teruel@ucaragon.com