

ESTAFAS EN VENTAS DE SEGUNDA MANO



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. En este artículo quiero hacer un apartado especial dedicado a la gente que **vende sus artículos en típicas páginas** de segunda mano. Sí, no estoy hablando de gente a la que estafan con una compra, sino **de gente a la que estafan cuando vende**. Esto es algo que cada vez es más frecuente porque *¿quién no quiere sacarse un dinero de aquellas cosas que ya no va a necesitar?*



🔍 *Las estafas como comprador y como vendedor son muy diferentes y, si hablo de ambas en el mismo documento quizás sea lioso, así que vamos a ceñirnos al caso del tú-vendedor 😊*

¿Así que si vendo también me pueden timar?

Las aplicaciones de venta de segunda mano son objetivo de muchos delincuentes, tanto si **compras como si vendes**. Como vendedores, hay muchas estafas a las que te puedes enfrentar, y estas son **las más frecuentes**:

- ⌚ **Sobrepagos:** Te compran lo que vendes **por más de lo que pides** (pero nunca ves el dinero)
 - Para que **te fíes más de ellos** y resulten más creíbles, o les des prioridad respecto a otras ofertas legítimas.
 - Para que te digan que fue un error y que **les devuelvas la diferencia** (tu nunca veras el dinero que supuestamente te han pagado, así que no les devuelves nada, te lo roban 😞).
- 💻 **Falsos servicios técnicos / administración de la plataforma:** Te contacta un falso servicio técnico de la plataforma para **pedirte los datos de tu cuenta** (que ya deberían tener 😞)
 - Para (supuestamente) **investigarte por fraude** o porque un usuario **te ha denunciado** (nunca te dicen quién ni cómo, ni ves notificación de denuncia alguna, solo su palabra).
 - Con esto, te roban la cuenta, tus datos personales y suplantran tu identidad.



- ⌚ **Falso pago con Bizum:** Te dicen que te han pagado el artículo por *Bizum*, en lugar de las formas que admite la plataforma
 - Pero en realidad no recibes un mensaje de que te han pagado X dinero, **sino de que te están solicitando X dinero.**
 - Si aceptas, **pagas al delincuente por nada** y, como ya habrás enviado el producto, también lo pierdes.
- 💀 **Comprobantes de pago falso:** Tu comprador te dice que ha pagado el producto, y **te envía un comprobante de pago falso.**
 - Si no lo compruebas, enviarás el producto y te quedarás sin ambas cosas.
 - Para evitar esto, tienes que confirmar en la app de venta o a través de tu banco **que de verdad has recibido un pago.**
 - Normalmente, el estafador **lo combina con imponerte una forma de pago, en lugar de usar una que admite la plataforma** (eso pasa también en la anterior). La siguiente forma detalla el motivo de esto.
- ฿ **Imposición de un medio de pago que no admite reclamaciones:** Los delincuentes quieren “sacarte” de la plataforma para que no uses su sistema de pagos.
 - Te piden usar otros que **no están pensados para hacer transacciones comerciales**, sino enviar dinero a familiares o amigos. Ejemplos son *MoneyGram*, *Western Union* o *PayPal* usando la opción de **pago amigo**.
 - Esto es más bien una **estafa típica de compradores**, pero si como vendedor el estafador te pide que le hagas algún pago (devolución o similar) por esta vía, habrás perdido tu dinero.

🔍 *¡Entiéndeme bien! Estos servicios **NO son fraudulentos**. Solo que no son para comprar cosas, sino para prestar dinero a conocidos, amigos o familiares*

- 캅 **Phishing:** Los estafadores mandan enlaces a **sitios falsos que son copias exactas** de otro que les interesa
 - La plataforma de ventas, un banco, etc. depende del tipo de timo y la fase de compra en la que se esté
 - Suelen usarlo para que el vendedor rellene sus datos con cualquier excusa, pero siempre con el pretexto de confirmar el pago.
 - Con ello, **robarán los datos del vendedor para suplantarle**, o los de la **tarjeta de crédito** para hacer compras fraudulentas o “vaciarle la cuenta”

-  **Devoluciones fraudulentas:** El vendedor envía el artículo en perfecto estado mediante el servicio autorizado de la plataforma.
 - El delincuente, tras recibirla, alega que **está roto, no funciona** o que **no cumple con el anuncio**, solicitando la devolución.
 - Al hacerlo, el delincuente **no entrega el artículo que el vendedor ha enviado**, sino otra cosa (o una unidad rota de la misma cosa que él ya tenía).
 - El vendedor se vuelve a quedar sin producto y sin dinero. El comprador ha obtenido una “reparación gratis” 😞



 **Se ha visto gente jactándose por redes de usar esta táctica para obtener una nueva unidad de un producto que ha roto sin pagarla. Se queda con la comprada y devuelve su unidad rota. En algunos medios se le llama el “timo de la rata”**

Estudio de estafas al vendedor reales

Todas estas estafas ocurren porque hay grupos organizados de criminales que se dedican a **“peinar” todos los anuncios que se publican** en este tipo de páginas para intentar estafar a los vendedores indiscriminadamente. ¿Quieres saber cómo se hace casi siempre? Veamos cuatro ejemplos para entrenar tu “sentido común” 😊

Ejemplo de timo 1: Pago directo fraudulento por empresa de envío de dinero

The screenshots show a listing for an iMac 21.5 (2017) priced at 600€. The seller is Trisha Takanawa, located in Pamplona (Navarra). The item is described as being sold as an offer by a particular vendor. The description states: "Se vende iMac de 21,5 con pantalla Retina, es el modelo de 2017 y fue comprado en verano de 2017. Funciona en perfecto estado y está impecable." The listing includes a map of Pamplona and a button to attract more buyers.

Imagen 1: Captura de pantalla de la página web que muestra la publicación de un iMac falso.

Imagen 2: Captura de pantalla de la página web que muestra la publicación de un iMac falso.

Imagen 3: Captura de pantalla de la página web que muestra la publicación de un iMac falso.

Imagen 4: Captura de pantalla de la página web que muestra la publicación de un iMac falso.

Figura 1. En Xataka quisieron probar hasta qué punto estaba de mal la situación de la venta de productos de segunda mano y crearon perfiles falsos con venta de productos ficticios para ver qué ocurría. Fuente: <https://www.xataka.com/servicios/todos-tipos-estafas-que-te-encuentras-wallapop-otros-sitios-compraventa-particulares>

- Tú pones algo a la venta (da igual lo que sea) en cualquier plataforma de venta. En la **Figura 1** puedes ver una prueba que hizo Xataka para ver cómo funcionan esta clase de timos, poniendo a la venta productos inexistentes.

 **Esto también te demuestra que poner a la venta algo que no existe es muy fácil. Ahora combínalo con IAs que generan imágenes más fotorrealistas que las que uso yo a la que pides que te cree una foto de cualquier cosa que quieras. ¿Te das cuenta de lo peligrosa que es esta combinación?**

- Tal y como Xataka experimentó, lo más típico es que, sin transcurrir mucho tiempo desde la puesta a la venta, **alguien te contacte** interesándose por lo que vendes. La secuencia de esta venta simulada por Xataka para estudiar el delito la puedes ver en la **Figura 2**.

Buenos días, Gracias por contestarme, estoy realmente encantado. OK, estoy a favor de la compra, sin embargo, tengo la intención de enviarle dinero en efectivo en un sobre por correo a través del servicio de entrega de DHL. Correo urgente de DHL a su dirección domiciliada. El servicio de mensajería de DHL recogerá el paquete por mí cuando le devuelva el efectivo. Si mi método de pago le conviene, déjeme esta información a continuación: PRIMER NOMBRE DIRECCIÓN POSTAL PRECIO FIJO NÚMERO TEL Le pido que lo haga lo antes posible para enviar su dinero a tiempo.	 Eva RdL Para: Micheline Marine > martes Re: anuncio iMac Wallapop Claro, Micheline. ¿Entonces cómo hacemos? ¿No quieres verlo antes o probarlo? Mi nombre es Eva RdL, Mi dirección es calle Xataka, 13, 1 derecha. 28010 Madrid Precio: 700 euros Teléfono: [REDACTED] Me vas contando cómo hacemos. Un saludo Enviado desde mi iPhone El 3 mar 2020, a las 11:03, Micheline Marine [REDACTED] escribió:	 Micheline Marine Para: Eva RdL > martes Re: anuncio iMac Wallapop Bien, iré a enviarle el sobre a través de DHL. Al recibir el sobre, por favor manténgame informado. Atentamente. Me gustaría informarle que he depositado el sobre que contiene el dinero para su envío rápido y seguro al servicio DHL EXPRESS y tuve que agregar 200 € porque debe pagar los costos del seguro antes de enviarlo. Hice un sobre que contenía € 900,00 para que recibiera el dinero según lo acordado una vez que haya hecho lo necesario si es posible hoy para recibir el sobre este día. ¿DHL me ha informado que le enviará una notificación para obtener instrucciones sobre qué hacer con él? Por favor, déjeme un mensaje una vez que haya acordado recibir el sobre. Atentamente !	 Micheline Marine Para: Eva RdL > martes Re: anuncio iMac Wallapop Me parece que la notificación seguramente te ha llegado. Para verlo, consulte su bandeja de entrada o correo no deseado para verlos y tome medidas lo antes posible. Os agradezco.
--	--	--	--

Figura 2. Secuencia de un intento de estafa de venta en una investigación de Xataka. Fuente: <https://www.xataka.com/servicios/todos-tipos-estafas-que-te-encuentras-wallapop-otros-sitios-compraventa-particulares>

Analícesmosla en detalle:

- **Mala redacción:** Esto es cada vez menos común por las IAs como ChatGPT o similares. No obstante, a veces te ponen la excusa de que son extranjeros y la usan como una herramienta más para convencerte
- **No regatean ni hacen ninguna pregunta.** Un comprador normal es típico que lo haga...
- **No piden más fotos ni datos del producto,** como haría un comprador normal
- **Te impone una forma de pago,** que es un indicio de los destacados en la sección anterior
 - El pago directo por DHL es uno de esos servicios de pago a amigos o familiares que no se debe usar para comprar
- **“Excusatio non petita”:** Te dicen que primero te entregan el dinero y tu envías el paquete para que te quedes tranquilo y no resulte sospechoso. Pronto comprobarás que no es así
- **Te mete prisa:** Todo lo que involucre meter prisa de alguna forma es fraude casi seguro...

Como veis, el mensaje tiene bastantes elementos coercitivos típicos de estafas, pero aun así hay otros típicos que no tiene esta estafa y que deberíais conocer (algunos aparecerán en ejemplos posteriores). Estos son:

- **Decirte que están fuera de España** como justificación para luego introducir algunos de los indicios de estafa que vimos en la sección anterior.
- **Pagarte más de lo que pides por el producto** (es decir, el sobre pago) como motivo para meterte prisa, que creas que estás ante un chollo e intentar que no pienses mucho en la situación para poder llevar a cabo el engaño.
- **Sacarte de la plataforma para que hagas la transacción fuera de ella** (por WhatsApp o similar): Así pierdes el derecho a reclamar, por lo que todo intento de pago que te diga eso puedes asumir que es un timo.

 **Lo de vivir en el extranjero o tener problemas para ir a España fue muy común hace tiempo como excusa para que les pagases de una forma que ellos pudieran robarte el dinero (es decir, fuera de la página de ventas en cuestión). Como esa excusa empezó a ser demasiado común y la gente ya tenía la mosca detrás de la oreja ahora recurren a otras técnicas. Pero seguramente volverá, cuando la gente se "olvide" de eso**

El caso es que el estudio de Xataka continuó con el intento de estafa y, efectivamente al vendedor le llegó una notificación de pago de DHL...pero desde una dirección completamente falsa (**de Gmail en lugar de DHL**), como se ve en la **Figura 3**.

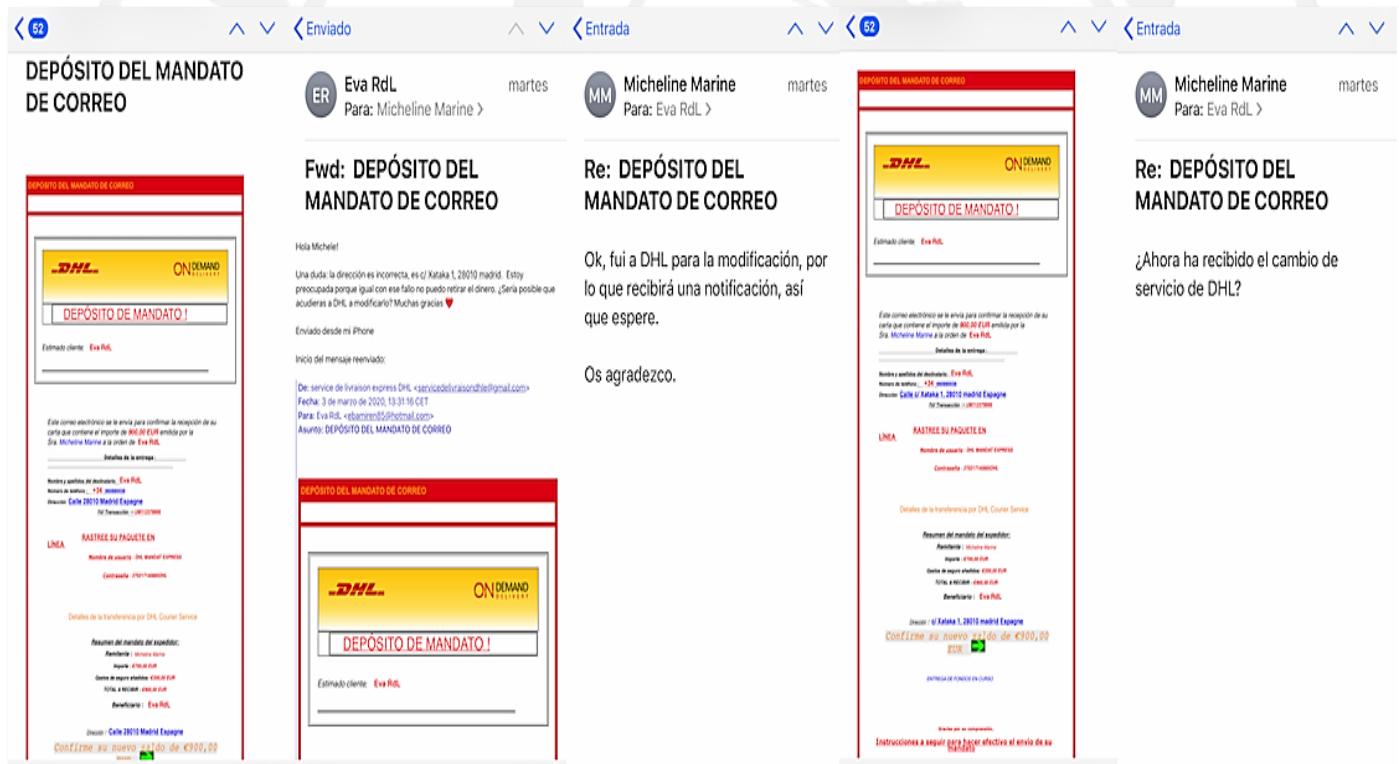


Figura 3. Secuencia de mensajes del estafador investigado por Xataka donde se mandó una falsa notificación de pago de DHL, suplantando estilos del mail y logos. Fuente: <https://www.xataka.com/servicios/todos-tipos-estafas-que-te-encuentras-wallapop-otros-sitios-compraventa-particulares>

 Que venga de DHL tampoco quiere decir nada. Es posible que se pueda suplantar el emisor también, y que aparezca uno creíble aunque el correo sea falso. Date cuenta de que hay cierto trabajo en la redacción de los correos para que no tenga un aspecto cutre

Si se accede al enlace que trae esta notificación vemos la trampa: Para que un supuesto empleado de DHL entregue el paquete es necesario introducir el número de tarjeta, el nombre del titular, la fecha de caducidad y el CV2, es decir, todo lo necesario para operar con ella. Como

se ve en la **Figura 4**, la excusa que alegan es que es para comprobar tu identidad y que no les estafes (irónicamente).

En resumidas cuentas, esta supuesta venta no es más que una **tapadera para robarte los datos de la tarjeta de crédito** y usarla para vaciar la cuenta todo lo que puedan, hasta que el banco detecte movimientos inusuales (si lo hace, porque el perfil de gasto que a veces usan está pensado para no levantar alarmas). Si tardas en darte cuenta podrás perder mucho dinero y tener problemas para recuperarlo

 **En esta situación solo te queda denunciar y cancelar la tarjeta lo antes posible, para iniciar el trámite con el banco y ver si puedes conseguir la devolución sin problemas.**

El 01/03/2020 , Sonia Dupont ha hecho una transferencia con DHL Express por **€100.00 EUR**. Le invitamos a que se tome unos minutos y lea nuestro comentario para comprender nuestro proceso de acreditación sistemática de su cuenta DHL.

Nota de DHL

Debe completar el llenado al recibir la notificación de DHL para estar seguro de su honestidad y para que el repartidor pueda mudarse a su hogar lo antes posible.

Para esto, le pedimos que confirme la información muy rápidamente al entregárnosla:

- Dirección postal:
- Número de tarjeta :
- Titular de la tarjeta :
- Fecha de caducidad
- Meses:
- Año:

código de seguridad ----- 3 dígitos en el reverso de la tarjeta o 4 dígitos en el frente de la tarjeta

- Número de teléfono :

por correo a la dirección dhserviceexpresse773@gmail.com para acreditar su cuenta lo antes posible porque permanece pendiente.

Figura 4. Formulario para robar los datos de la tarjeta y usarla para vaciar cuentas. La venta no era más que una mera excusa. Fuente: <https://www.xataka.com/servicios/todos-tipos-estafas-que-te-encuentras-wallapop-otros-sitios-compraventa-particulares>

Ejemplo de timo 2: Negociado fuera de la plataforma

Como comentaba antes, es bastante típico en estos timos usar una excusa para sacarte de la plataforma de ventas. Aquí podemos encontrar dos versiones del timo:

- **El comprador-estafador te dice que la plataforma de ventas se va a poner en contacto contigo** en el nº de teléfono que diste al registrar un usuario, haciéndote creer que esta es la forma que tiene esa plataforma de venta de completar las compras.

🔍 Esto es completamente falso, van buscando gente sin experiencia en ventas (para ello miran seguramente tu perfil, donde seguramente se ve el tiempo que llevas registrado, las ventas que has hecho, etc.) para estafar a vendedores nòveles que posiblemente no tengan claro còmo funciona del todo el sistema.

¿Y qué hace ese segundo estafador que se pone en contacto contigo por mensajería (o el mismo estafador haciéndose pasar por otra persona)? Crea una cuenta de WhatsApp o similar que se hace pasar por la plataforma de ventas. Y le mete trabajo: Poniéndose el **ícono de la plataforma real**, hablándote con **lenguaje legal** para que todo suene mucho más serio y formal, dándote un **número de transacción** imitando a los reales, diciéndote que está compra está siendo monitorizada por temas de calidad o seguridad... **cualquier cosa con tal de que te lo creas**.

- **El comprador-estafador te dice que se va a poner en contacto contigo él mismo** al número que has dado en la propia plataforma de ventas para pedirte los datos de pago. Ahora ya estás fuera de la plataforma de ventas, con el problema que comentábamos antes. En definitiva, Xataka también se encontró con esta variante y en la **Figura 5** puedes ver como el estafador empezó esta variante del timo en cuestión.

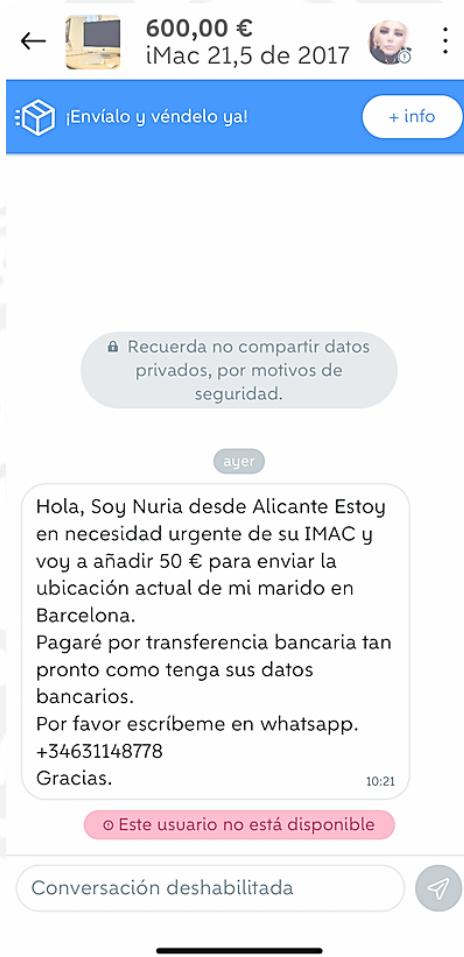


Figura 5. De entrada te hace un sobreprecio y te intenta sacar de la plataforma: ya cumple con dos de los indicios de estafa que vimos antes. Fuente: <https://www.xataka.com/servicios/todos-tipos-estafas-que-te-encuentras-wallapop-otros-sitios-compraventa-particulares>

🔍 Date cuenta de que eres tú quien le escribe al estafador. Esto lo hacen porque lanzan la estafa "en masa" y de esta forma solo aquellos que escriban pasan a la segunda fase. Es mucho más rápido que ir uno a uno esperando una respuesta...

La investigación de Xataka continuó con la estafa y estableció contacto con el estafador vía WhatsApp, como ves en la **Figura 6**. Aquí aparece de nuevo otro indicio de fraude, imponerte el medio de **pago por transferencia** ¿Por qué es peligroso este tipo de pago?

- **Como comprador**, porque te la juegas a que el vendedor no te envíe la mercancía.
- **Como vendedor**, existe un plazo de dos días para anular una transferencia, por lo que puedes enviar el paquete, el estafador anular la transferencia y quedarte sin dinero y sin lo que vendes. Aquí el factor prisa también va a jugar en tu contra, y el estafador lo va a usar para que envíes el paquete lo antes posible



Figura 6. Negociar una venta por WhatsApp siempre es mala idea. ¿Para qué has metido tu artículo en una plataforma de venta si al final vas a negociar una venta entre particulares? (es lo que estás haciendo si caes en esto). Fuente: <https://www.xataka.com/servicios/todos-tipos-estafas-que-te-encuentras-wallapop-otros-sitios-compraventa-particulares>

Por otro lado, no es raro que estos estafadores **también te pidan una foto de tu DNI** que se puede usar para otro tipo de estafas suplantando tu identidad.

Ejemplo de timo 3: Suplantando a la plataforma de ventas por el chat

Otra variante de timo de venta de segunda mano es cuando el vendedor recibe por chat interno de la aplicación un aviso dándole la **enorabuena por haber vendido un artículo** como el de la **Figura 7**. A través de ese aviso se acaba pidiendo el nº de teléfono o el email para completar el envío. No obstante, fíjate que el aviso tiene un botón para sacarte de la plataforma y un uso del lenguaje discutible, aunque el estilo copia perfectamente al de *Wallapop*

 **Espérate el mismo tipo de mensaje fraudulento en otras plataformas. Wallapop solo es un ejemplo, ¡esto pasa en todas!**

La clave para reconocer la estafa es que es similar a una variante de la anterior: te habla supuestamente alguien de la plataforma de ventas, pero desde el chat del supuesto comprador. Eso simplemente no es posible, **la plataforma no puede suplantar a ningún comprador** porque no tendría sentido (además de ser delito).

 **Por otro lado, la plataforma ya tiene la información que te pide porque la diste al registrarte, no tiene sentido que te la vuelva a pedir para confirmar nada**

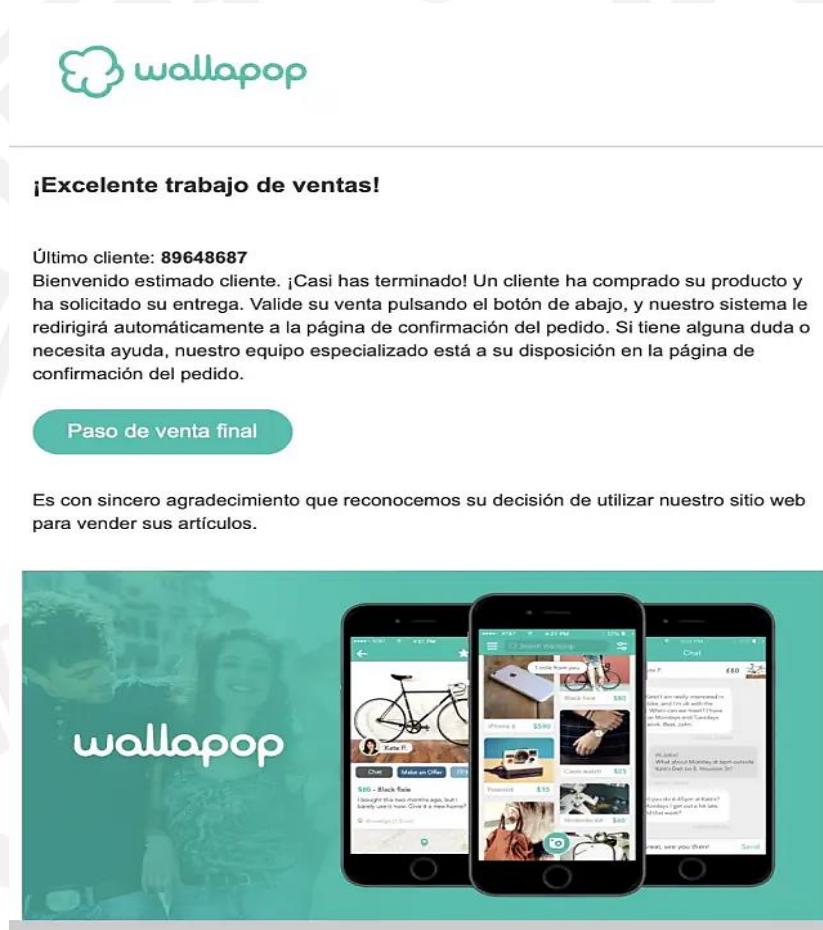


Figura 7. Falso aviso de compra de un producto en Wallapop . Tiene hasta un nº de cliente falso y un botón que te lleva a una página falsa, sacándose de la plataforma. Fuente: <https://www.20minutos.es/tecnologia/ciberseguridad/cuidado-vendes-wallapop-nueva-estafa-enganarte-facilmente-5240724/>

Si se continúa con el proceso dando teléfono o email, llegará un mensaje indicando que para finalizar la compra hay que seguir una serie de instrucciones, para al final **llegar a una página falsa que simula ser Wallapop** con un realismo bastante trabajado (**Figura 8**). En esta página falsa vuelven a pedirse los datos de la tarjeta como en un ejemplo anterior. **De nuevo la excusa de la compra es para robar datos de una tarjeta de crédito y vaciar cuentas.**

 **Las páginas que te llegan parecen auténticas y el proceso no es demasiado "estridente", lo que lo hace peligroso. Si se cuidase más el lenguaje (algo que ya es posible gracias a IAs como ChatGPT) la estafa sería aún más peligrosa 😞**



Figura 8. Todo este proceso de engaño para acabar pidiéndote nº de tarjeta, caducidad y CV2, es decir, los datos para operar con ella. Fuente: <https://www.20minutos.es/tecnologia/ciberseguridad/cuidado-vendes-wallapop-nueva-estafa-enganarte-facilmente-5240724/>

Como puedes comprobar en la **Figura 9**, dar un teléfono no cambia nada en este proceso: recibes un mensaje, vía WhatsApp normalmente, donde se te pasa una página falsa que se hace pasar por Wallapop o la plataforma que sea para hacer exactamente lo mismo que hemos visto.

🔍 ¿Te das cuenta de que en estas estafas en ningún momento hubo interés alguno en comprar lo que vendes? Lo que quieren son los datos de tu tarjeta

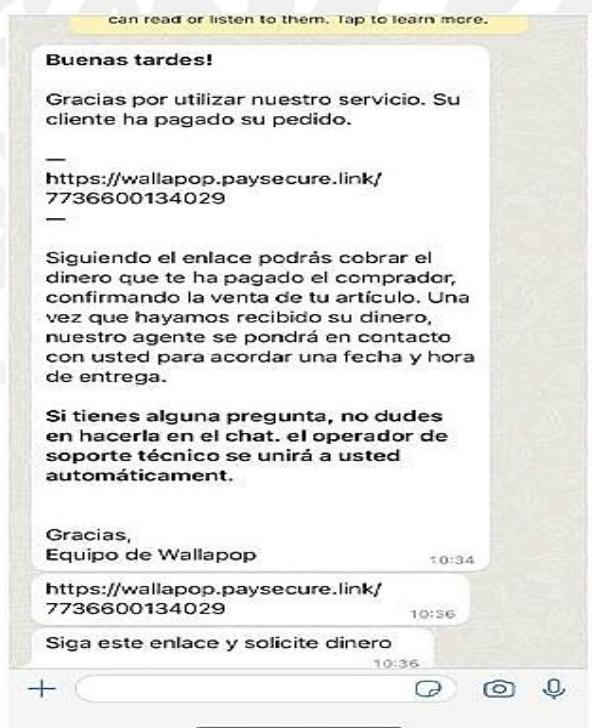


Figura 9. Mensaje para que des tus datos de tarjeta en una página falsa de Wallapop. Date cuenta de que acaba en .link (no en .es) y que el enlace está pensado para que sea muy creíble. Fuente: <https://www.adslzone.net/reportajes/seguridad/estafas-wallapop/>

Ejemplo de timo 4: Devoluciones fraudulentas

Este último ejemplo de timo es el que mencionábamos en la primera sección relativo a los **fraudes con las devoluciones**. Como veis en la **Figura 10**, el vendedor envía un producto en buen estado y el usuario que lo recibe declara que no lo está y **abre una disputa** en la plataforma.

💡 Si tienes en cuenta lo que comentábamos antes de la razón de estos timos, el estafador es capaz de adjuntar una foto del artículo con daños: pero es la unidad que él tenía y que está intentando cambiar por la tuya

Si el vendedor se traga el pretexto y acepta la devolución, el comprador **entregará el producto roto o dañado en una oficina** o punto de entrega. Una vez recibido, la plataforma procesará el reembolso al comprador-estafador.

💡 Y así se quedan con el dinero y el producto gratis 😊

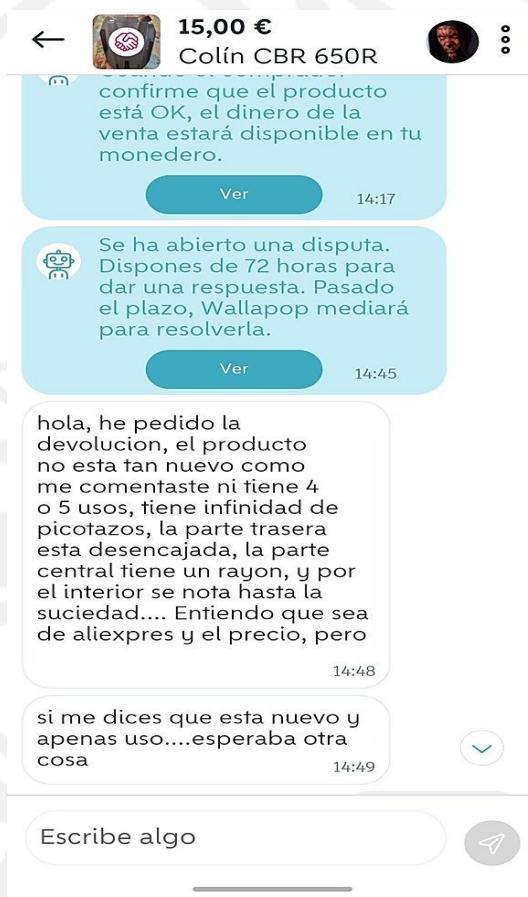


Figura 10. Echándole morro a la vida como comprador, a ver si obtiene una copia en mejor estado de la que ya tiene. Probablemente para venderla luego a otra persona. Fuente: https://www.larazon.es/economia/rata-wallapop-esta-nueva-estafa-online-plataforma-segunda-mano_202405156644654069f85800013cd210.html



Figura 11. Respuesta del vendedor, que ya ha jugado más veces este partido 😊. Fuente: https://www.larazon.es/economia/rata-wallapop-esta-nueva-estafa-online-plataforma-segunda-mano_202405156644654069f85800013cd210.html

¿Qué puedes hacer?

Como habéis podido ver, muchas de estas estafas se basan en que alguien te convence para **sacarte de la plataforma de ventas** y que le proporciones **toda tu información financiera** para de esta manera robarte hacerse pasar por ti o usarla de cualquier forma maliciosa. Así que el primer consejo que os puedo dar es que nunca salgáis en la plataforma de ventas y por supuesto nunca le deis a un particular ningún tipo de información financiera o personal como la que os estoy describiendo en este timo. **Solo el hecho de que te lo pidan ya indica que es un timo.**

Es además muy frecuente que estas plataformas de venta tengan tutoriales que te indican cómo se hace una venta real ilegal, para que sepas lo que puedes esperar el primer día que hagas una. Por ejemplo, *Wallapop* tiene un tutorial aquí: <https://ayuda.wallapop.com/hc/es-es/articles/12459232139793--C%C3%B3mo-puedo-identificar-una-estafa-de-phishing>.

 **Te recomiendo que busques algo equivalente en cualquier plataforma que uses, ayuda mucho**

Y también estoy obligado a advertiros de que no creáis que esto es algo que pasa muy raras veces sino que realmente **existen muchos grupos organizados que van a la caza de incautos** y no es ni la primera ni la última vez que veo a gente quejarse de la cantidad de intentos de estafa que sufren solo por tener un producto a la venta.

 **O dicho de otra manera si has puesto algo a la venta en cualquier estafa la probabilidad de que te contacte un delincuente de este tipo es muy alta. ¡Así que mucho ojo!**

Cómo detectar a un posible estafador y denunciar

Los estafadores que frecuentan estas plataformas son pillados con mucha frecuencia, por lo que **tienen que estar creando cuentas constantemente** para así poder seguir con las estafas (ya que las que son pilladas se suspenden). Esto hace que podamos hacer un perfil típico de usuario de plataforma de venta con gran probabilidad de ser estafador (además de los indicios mencionados anteriormente):

- Un perfil **nuevo** (pocos días desde que se creó).
- Vendedor o vendedora con perfil **sin validar** o **sin valoraciones**.
- No hay **ningún historial** de artículos comprados ni vendidos.

Si detectas que un usuario es un estafador o dudas sobre ello, puedes **denunciar** desde la aplicación de la propia plataforma para investigar los hechos. Normalmente las plataformas ofrecen estas opciones de denuncia o “reportar usuario” (**Figura 12**).

- **Fraude**: Si estás seguro de que lo es, con los indicios que te hemos dado en este artículo.
- **Sospecha de fraude**: Como el anterior, pero cuando no lo puedes asegurar. Mejor denunciar para que lo miren que dejarlo pasar por si acaso.
- **Mal comportamiento o abuso**: Insultos, amenazas, intentos de extorsión...puede ser por negarnos a negociar o a darle datos privados (precisamente porque es un indicio de estafa). Los insultos suelen ser una forma de coaccionar a la víctima. No te amedrantes, denuncia y bloquea.
- **No asistencia a la cita**: Si hemos quedado con alguien para la entrega en persona y no viene.
- **Artículo defectuoso o incorrecto**: En caso de que las fotos o descripción del artículo no mencionen cosas que si tiene lo que hemos recibido. Esta es la opción que desencadena el ejemplo de timo 4 que vimos antes.
- **Otras causas**: Por ejemplo, que el usuario no responda a ninguna de nuestras preguntas sobre el proceso de venta.



Figura 12. Herramienta de reporte de fraude de Wallapop. Todas las plataformas tienen una similar

 Normalmente también tienen un campo para dar contexto y explicaciones, como ves en la imagen.

¿Qué hacer si ya te han estafado?

Si has sido víctima de una estafa de este tipo, es importante que actúes con rapidez para minimizar el daño y recuperar tu dinero si es posible. Unos posibles pasos a seguir son:

- **Contacta con el vendedor:** Por si no es una estafa, sino un malentendido. Si se arregla así es mucho mejor, puedes estar dejándote llevar por la sospecha y que la situación real sea otra cosa.
- **Denuncia el fraude en la plataforma:** Si lo anterior no funciona, denuncia como vimos en la subsección anterior.
- **Denuncia el fraude a la policía:** Especialmente si te han robado mucho dinero o sospechas que es un fraude organizado. Puedes hacerlo **en comisaría o vía web**: https://www.policia.es/_es/denuncias.php.

 Debes denunciar a la policía y reclamar a tu entidad bancaria en caso de que hayan realizado cargos en tu tarjeta sin tu autorización, además de que debes cancelarla de inmediato para que no puedan seguir robándote dinero. Lo mismo si te han hecho un pago en físico con billetes falsificados.

- **Contacta con el banco:** Si has realizado un pago por adelantado y el producto no ha llegado o no se corresponde con lo que se anunciaba, es importante que contactes con tu banco para cancelar el pago.

 Si has realizado la transacción a través de un sistema de pago seguro, como PayPal (pero no pago amigo) o Bizum, también debes contactar con ellos para reclamar el dinero.

- **Conserva toda la información:** Relacionada con la transacción (mensajes intercambiados con el estafador, el anuncio del producto y los comprobantes de pago) para presentar pruebas.

Así que por favor si pones algo a la venta o conoces a alguien que lo va a hacer **avísale de que esto le puede ocurrir**, no sea que le pille un día despistado o el estafador sea extremadamente bueno y al final acabes con un disgusto y unos cuántos miles de euros menos en tu cuenta. **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, todo lo que se salga mínimamente de lo normal al vender algo tuyo, ¡apesta a estafa!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en mi canal de YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

¿Quieres leer alguna noticia/artículo relacionado?



- [Todos los tipos de estafas que te encuentras en Wallapop y otros sitios de compraventa entre particulares \(8/4/2022\)](#)
- [Así funciona el timo de Wallapop y el supuesto correo de DHL \(02/03/2020\)](#)
- [Cuidado con lo que vendes en Wallapop: esta nueva estafa puede engañarte fácilmente](#)
- [Cinco estafas que te puedes encontrar en Wallapop al comprar o vender con la aplicación \(03/11/2023\)](#)
- [Las 7 estafas de Wallapop que deberían ponerte en alerta \(09/04/2024\)](#)
- [Cómo evitar estafas en Wallapop: consejos para comprar y vender \(23/02/2024\)](#)
- [La "rata" de Wallapop: esta es la nueva estafa online en la plataforma de segunda mano \(15/05/2024\)](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 29/05/2023

² Algunas imágenes del texto del documento han sido generadas con la IA Bing Chat