

EL “PAYPAL” O TIMOS CON MEDIOS DE PAGO QUE NO SON PARA COMPRAR



Proyecto P-45 “Audaz”



Buenas una vez más amantes de la nave del timo 😊. Os voy a hablar de un fraude **retorcido**. De esos que uno cae aunque tengas mucha experiencia técnica, porque requiere estar muy atento y tener un poco de conocimiento previo de medios de pago por Internet. Además, se aprovecha del descuido y de la confianza en la empresa que está por detrás que el público tiene. Y es que se trata de **un fraude que se hace con PayPal** (aunque luego veremos otros parecidos).



💡 *Y a lo mejor diréis: “No puede ser, pero si PayPal es seguro ¿Por qué no lo es ahora?”. Cuidado, yo no he dicho que no sea seguro, es más bien que se usa mal. Se trata de un fraude que se hace a través de PayPal, pero sigue siendo una de las plataformas de pago más seguras del mundo.... si se usa correctamente, claro 😊*

¿Cómo puede ser que haya un fraude usando PayPal?

Resulta que se han detectado casos de **tiendas de dudosa fiabilidad** que permiten comprar artículos a precios muy interesantes usando PayPal. Y a lo mejor diréis: *“Claro, te ponen el icono de PayPal, pero luego te redirigen a una página que imita PayPal pero es falsa, metes el usuario y clave y ya la tienes liada”*. Pues no, no es el que vamos a hablar hoy. **Este te dirige a la página de PayPal de verdad.**

💡 *Pero este fraude también existe, y si eso ha sido lo primero que te ha venido a la cabeza, te tengo que felicitar porque significa que estás en el buen camino para pelear contra los fraudes 😊*

Y el caso es que el pago se hace como de costumbre:

- Clicas en el botón de “**pagar con PayPal**”.
- Te redirige a la **página real** de PayPal, y entras en tu cuenta tras poner tus datos, como siempre.
- Confirmas el pago directamente y *PayPal* lo hace.
- Y esperas por tu producto...**que nunca llega**.

Entonces ahora pensarás: "Bueno, no pasa nada, reclamo la transacción y PayPal me devuelve el dinero". Pero... ¡Cuando te pones a reclamar PayPal te dice que **no tienes derecho a la devolución por la forma en la que has hecho el pago!** 🤦

¿Qué ha pasado exactamente?

Pues que **la tienda te ha engañado**. PayPal tiene **dos formas** de pagar a tiendas o a cualquier servicio que lo necesite (**Figura 1**).



Figura 1. Parecen lo mismo, pero no lo son. Mucho cuidado. Fuente: <https://www.xataka.com/basics/como-enviar-pedir-dinero-a-otros-usuarios-a-traves-paypal>

- Una es el **pago por un servicio** (el botón de abajo en la imagen), que sí que tiene derecho a reclamación y devolución, pero tiene una serie de **comisiones**, que es donde PayPal lleva la ganancia. Digamos que esas comisiones son como un seguro por si algo va mal.
- Pero también tiene lo que se llama el **pago a un amigo** (el botón de arriba de la imagen). Qué es sencilla y llanamente **una donación**. En ese tipo de pagos no hay comisión alguna, pero tampoco tienes derecho a reclamar nada, porque **se supone que le das dinero a alguien de tu confianza** y no tiene las protecciones del otro modo: <https://www.paypal.com/es/cshelp/article/%C2%BFcu%C3%A1l-es-la-diferencia-entre-el-env%C3%A3o-de-dinero-a-amigos-y-familiares-o-el-pago-por-productos-y-servicios-help277>.

💡 **Y ambas son formas legales de hacer pagos, lo que pasa que, como veis, tienen unas diferencias importantes...que los delincuentes conocen y aprovechan**

¿Qué ha hecho la tienda?

La tienda ha jugado con la prisa por comprar que puedes tener (muchas veces ponen avisos de "X personas tienen esto en el carrito", "Quedan solo X unidades en stock" o similar) y ha

configurado su sistema de pagos conectado por PayPal para que por defecto se haga **un pago a un amigo**, es decir una donación.

Así que la tienda usa *PayPal*, sí, pero por defecto cuando lo abre le dice que en lugar de ponerse por defecto en el modo de “pagos normales” lo haga en el modo de “pagos a amigos” o donaciones. Si vas con prisa y no lees la información que te da *PayPal* cuando vas a hacer el pago (donde efectivamente te informa de que lo que vas a hacer **no tiene reclamación**) pagas, y la tienda se queda con tu dinero y el producto.

 Que, por otro lado, probablemente jamás haya tenido a la venta y sea una tienda falsa creada sólo para hacer este tipo de estafa...

Tampoco es la única forma de ser víctima de este tipo de cosas, incluso la propia *PayPal* y otros sitios de pagos similares listan las estafas más comunes que se hacen por estos medios, fíjate:

- <https://www.paypal.com/es/cshelp/article/%C2%BFcu%C3%A1les-son-las-estafas-comunes-y-c%C3%B3mo-puedo-detectarlas-help201>
- <https://www.moneygram.cc/proteccion.aspx>

Y ten en cuenta que esto te puede pasar en cualquier plataforma de ventas o red social onde haya un servicio de esta clase. Las excusas para que lo hagas, como ves en la **Figura 2**, son variopintas.

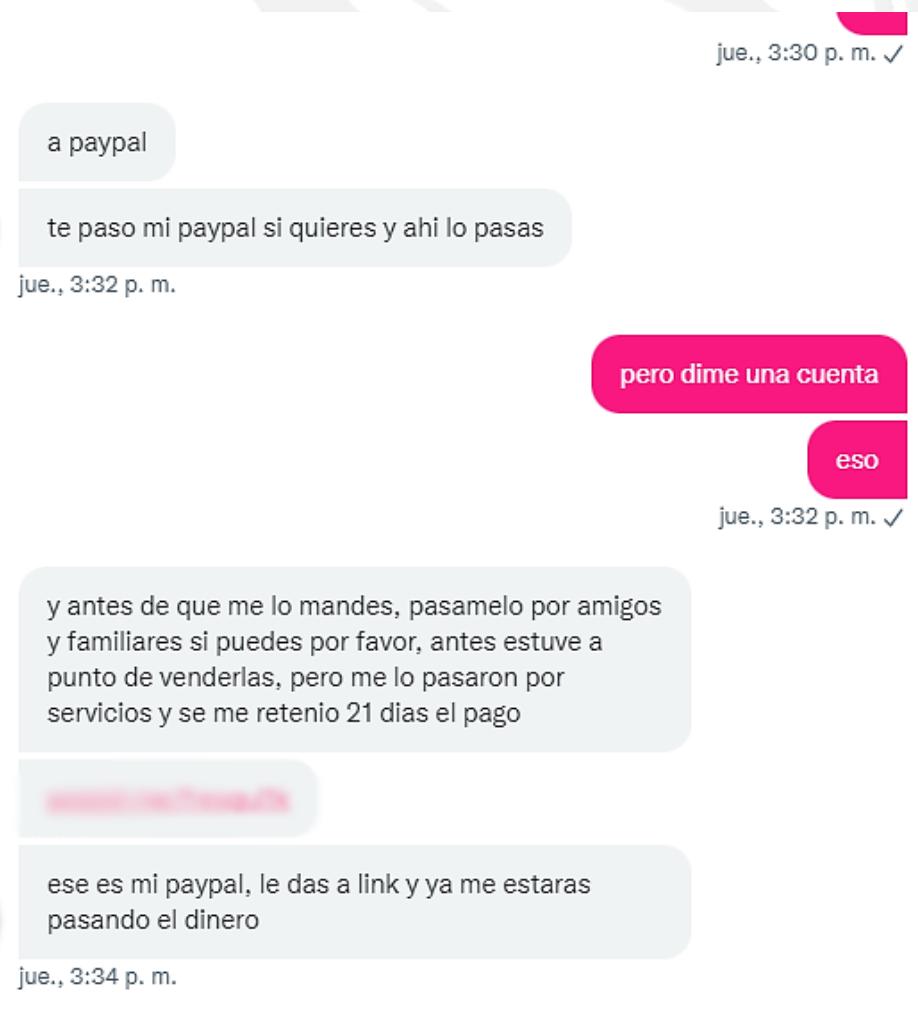


Figura 2. Es muy típico también que en una compra te pidan usar PayPal en lugar del sistema de pagos de la plataforma en cuestión, y aprovechen para colártela así. Fuente: <https://maldita.es/timo/20231204/paypal-pago-amigos-familiares-donacion/>

¿Y sólo se hace con PayPal?

¡Por supuesto que no! Lo que pasa es que *PayPal* quizás sea el servicio más conocido donde hay víctimas de este tipo de cosas. En realidad, estas estafas también se hacen frecuentemente con servicios cuya función principal es **enviar dinero a otras personas directamente**, es decir no son servicios de pago, **sino servicios de transferencia de dinero**.

🔍 *Ejemplos populares de este tipo de servicios son Western Union y MoneyGram pero hay muchos más (más abajo te pongo una tabla)*

Estos servicios tienen una función **legal y clara**: enviar transferencias de dinero a personas conocidas de manera segura y con unas tarifas conocidas de antemano. **NO SON EN ABSOLUTO UNA ESTAFA**. Pero es importante tener clara una cosa: **no son servicios para hacer compras de nada a una tienda o particular**, porque no tienen ninguna clase de cobertura al comprador.

Si entramos a las páginas web de estos servicios vemos que directamente ofrecen los servicios de transferencia, que es para lo que sirven y lo que fueron creados.



Figura 3. Página principal de la empresa de transferencia de dinero Western Union. Fuente: <https://www.westernunion.com/us/es/home.html>

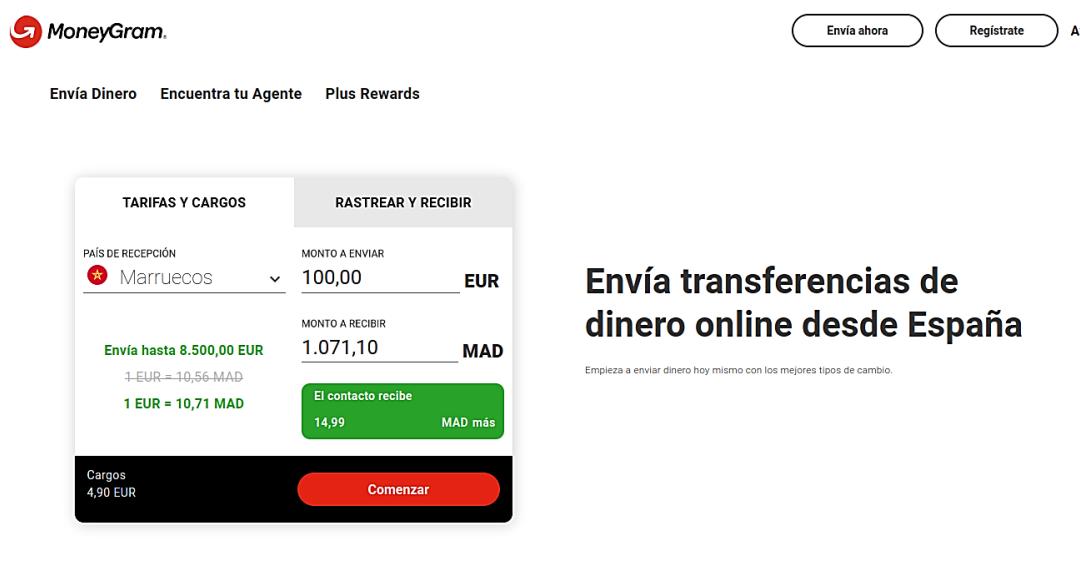


Figura 4. Página principal de la empresa de transferencia de dinero MoneyGram. Fuente: <https://www.moneygram.com/mgo/es/es/>

Pero si consultamos sus **condiciones de servicio**, vemos que nos dicen **claramente** que no debemos usarlas para hacer pagos por compras, debido a la carencia de cobertura para esta función. No son servicios de pago, y **no debemos usarlos como tales**, aunque el estafador se ponga extremadamente pesado y te dé 1000 razones para que lo hagas apelando, a cualquier cosa que te puedas imaginar (les vale cualquier cosa para convencerte).

Como usuario del servicio de envío de dineroSM de Western Union, valoramos tu negocio y nos enorgullece entregar tus fondos al destinatario de una manera rápida, cómoda y fiable. Sin embargo, hay personas de todo el mundo que intentarán utilizar cualquier sistema para recibir pagos en relación con ventas o solicitudes fraudulentas.

Asegúrate de saber a quién le estás enviando el dinero. Si estás comprando bienes o servicios y pagando a través de la red de Western Union, es tu responsabilidad verificar la reputación y la legitimidad del vendedor. Western Union no será responsable por la no recepción o la calidad de las mercancías o los servicios.

Cuelga la llamada si el interlocutor te indica que respondas a preguntas formuladas por Western Union.

La seguridad es responsabilidad de todos. Mantente informado. Mantente al tanto de las tendencias de fraude al consumidor.

Recuerda, si es demasiado bueno para ser cierto, probablemente lo es.

Figura 5. Aviso acerca de no usar Western Union para hacer compras, en la propia página de la empresa. Fuente:
<https://www.westernunion.com/es/es/frequently-asked-questions/faq-consumer-protection.html#01>

Proteger a los clientes es una prioridad

MoneyGram es una manera rápida cómoda y segura de enviar dinero por todo el mundo. Nuestros servicios ayudan a miles de clientes a satisfacer sus compromisos financieros así como a dar apoyo a familiares.

Desafortunadamente, algunas personas han utilizado nuestros servicios para la realización de fraudes, engañar o estafar a consumidores con una variedad de estafas. MoneyGram se dedica a proteger a nuestros clientes y nuestra marca y, es por ello, que detener las estafas y el fraude es una prioridad para nosotros. A continuación, encontrará una descripción de algunas de las estafas habituales y las formas de protegerse ellas.

Empiece con los aspectos básicos de Protección del consumidor

Asegúrese de que la persona o empresa a la que envía dinero (o en nombre de la cual envía dinero) es alguien en quien confía y conoce. Es importante mantener la confidencialidad de la información relacionada con su envío. Nota: Una vez que se haya enviado el dinero, la cancelación o el reembolso no son posibles. Si necesita cancelar o modificar una transacción, llame a MoneyGram o póngase inmediatamente en contacto con el agente MoneyGram en el que realizó el envío.

Figura 6. Aviso acerca de no usar MoneyGram para hacer compras, en la propia página de la empresa. Fuente:
<https://www.moneygram.cc/proteccion.aspx>

No te quepa duda, lo que quieren es "coger la pasta y marchar corriendo"

Dado que esto empieza a ser ya más conocido por el público en general, una treta común es **recurrir a otras empresas similares** a estas, que sirven para lo mismo, son perfectamente legales, pero menos conocidas (y de esto se aprovechan) o que no se asocian tradicionalmente al negocio de la transferencia de dinero. Otras que debes conocer son las de la siguiente tabla.

Empresa	Sitio web oficial
Wise (antes TransferWise)	https://wise.com/es/
Remitly	https://www.remitly.com/es/en
Xoom (propiedad de PayPal)	https://www.xoom.com/es
WorldRemit	https://www.worldremit.com/es/
Ria Money Transfer	https://www.riamoneytransfer.com/es/
Correos	https://www.correos.es/es/es/particulares/dinero-y-compras/envio-de-dinero

¿Y hay otras formas de pagar peligrosas para hacer compras?

Pues sí, sí que las hay. Los delincuentes van a tratar siempre de que **no hagas el pago por el sistema que tengan la plataforma de compra** que estés usando, para que así pierdas toda capacidad de reclamar el dinero que te han estafado y, por tanto, que se lo quiten a ellos o les suspendan la cuenta inmediatamente, perdiendo esa fuente de ingresos.

Pago con transferencias bancarias directas

Una primera forma que tienen de engañarte es tratando de que les **hagas una transferencia bancaria directamente** desde tu cuenta a una que te den ellos. Las transferencias bancarias solo se pueden anular **poco tiempo después** de que se hagan, en función de lo que los bancos llaman "**hora de corte**" y, si detectas que ha habido un problema o una estafa en alguna que has hecho, por ejemplo porque en unos días no te llega el producto que has pagado, vas a tener **muy difícil o imposible recuperar el dinero**. Puedes ver más información aquí:

- <https://www.ing.es/seguridad-internet/que-es-el-fraude-de-la-transferencia-bancaria>
- <https://www.genesis.es/blog/hogar/como-anular-transferencia-bancaria>
- <https://www.bbva.com/es/salud-financiera/como-anular-una-transferencia-bancaria/>

Los bancos contemplan una devolución de transferencias de **hasta 10 días** en caso de error, pero para eso **el receptor tiene que aceptar la devolución**, y evidentemente un delincuente no lo va a hacer 😬. También puedes pensar que cómo es posible que los delincuentes abran cuentas corrientes y se arriesgan a eso, teniendo en cuenta que les pueden identificar y denunciar desde el propio banco. Y tienes razón, pero pasan dos cosas:

1. **Pueden abrir una cuenta bancaria con la identidad de otro**, si el banco no comprueba adecuadamente la identidad de quién la abre (especialmente si se hace online, y todo agravado por el tema de los deepfakes)

 Ahora ya sabes para qué se roban DNI o se piden fotos de esos documentos en muchas estafas...

2. **Pueden estar compinchados con algún empleado/a corrupto** que las abre "de tapadillo", sin hacer casi ninguna comprobación (ovejas podridas hay en todas partes...)

En cualquier caso, los delincuentes, en cuanto reciben el dinero, lo transfieren a otros sistemas que hacen que seguir la ruta de tu dinero sea muy difícil, por ejemplo algunos servicios de criptomonedas...

Pago con tarjeta regalo

Una tarjeta regalo de cualquier empresa no es más que **dinero “virtual” para una tienda** específica que se compra con dinero real. Muchas empresas tienen tarjetas regalo: *Amazon, El Corte Inglés, Sony, Microsoft, Apple, Nintendo...* Y son pues un instrumento de **donación de dinero** parecido al de *Western Union y MoneyGram* que vimos antes, pero con la intención de comprar algo en esas tiendas.

💡 *Puedes regalársela a quien quieras o cargar tu propia cuenta de usuario con ellas: las ventajas son no meter una tarjeta de crédito real (más seguridad) y limitar tus gastos para no pasarte*

Cuando compras una tarjeta regalo y se activa, el código que lleva dentro, que normalmente tienes que rascar, pasa a ser válido. Cuando alguien canjea ese código, se carga el dinero en su cuenta de la tienda, y ya puede gastar el equivalente a lo que has pagado por la tarjeta regalo.

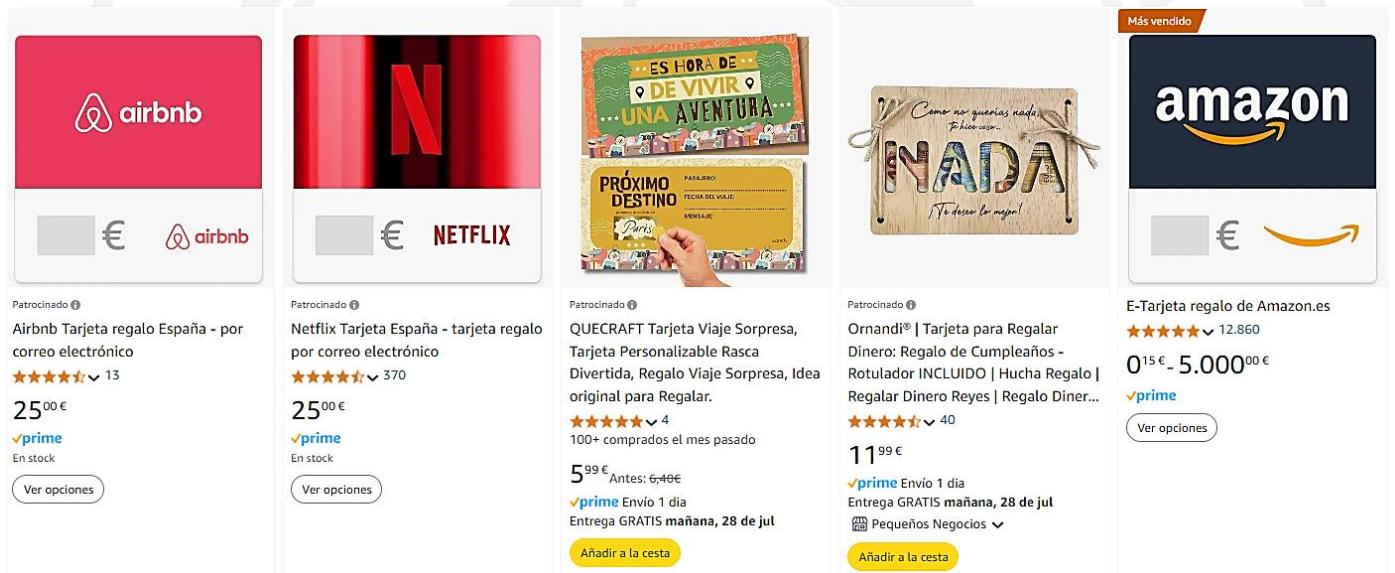


Figura 7. Varios ejemplos de tarjetas regalo. Llama mucho la atención la de Amazon, en la que puedes cargar una cantidad muy alta de dinero

Este método se usa porque es como un “**cheque al portador**” y, una vez que alguien lo canjea, el comprador original no tiene forma de recuperar el dinero. Además, descubrir quién lo ha canjeado realmente es o extremadamente difícil o imposible. En otras palabras, tampoco es un medio adecuado para pagar por ningún artículo.

💡 *Es más, me atrevo a decirte que cualquier petición que te hagan de pagar con tarjetas regalos es un fraude seguro, así que nunca lo hagas...*

¿Y qué nos queda si ya somos víctimas?

Aquí ya depende de la velocidad de actuación y la suerte que tengas.

- **Puedes hablar con PayPal** (o el servicio que hayas usado para pagar), por si tienes suerte y todavía se puede deshacer la transacción.

- **Debes denunciar** a ver si con un poco de suerte detienen a los responsables y podemos con el tiempo recuperar el dinero que hemos perdido.
- **Llamar al 017 del INCIBE** para pedir consejo sobre tu situación particular

Pero realmente poco más podemos hacer...Por eso, el mejor consejo que os puedo dar es que antes de darle a OK a la compra **leáis con lupa la información que os aparece en pantalla**, aunque estéis pagando con *PayPal*. Y mucho cuidado con los otros medios de pago que os he dicho también

Y con esto acabo. Sed muy cuidadosos y que no os peguen un "Paypal" 😊. Y como siempre digo al final, por si acaso tienes una amigo/a emocionado con estas cosas: **¡Que corra la voz!**

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

Y recuerda amigo/a, ¡los servicios para transferir dinero a familiares o amigos no se pueden usar para comprar nada!



¿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?



- [Estafan a una persona tras realizar una compra online pagando con PayPal donaciones \(06/06/2023\)](#)
- [Cómo te la pueden colar si pagas a través de PayPal: cuidado si realizas un pago a "amigos y familiares" o como donación \(4/12/2023\)](#)
- [¿Cuáles son las estafas comunes y cómo puedo detectarlas?](#)
- [Precaución al usar este método de pago en PayPal, podrías caer en una estafa \(10/12/2023\)](#)

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 19/06/2023

² Algunas imágenes del texto del documento han sido generadas con la IA Microsoft Copilot