Estafas y fraudes

Guía_

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

Índice

Estafas y fraudes

I. Introducción

Una estafa financiera es una acción realizada por una persona o empresa que causa un perjuicio económico a un tercero mediante engaño y con ánimo de lucro. Existen muchos tipos de estafas y fraudes financieros. En los últimos años, se han visto incrementados debido a las posibilidades que permiten las nuevas tecnologías y las redes sociales.

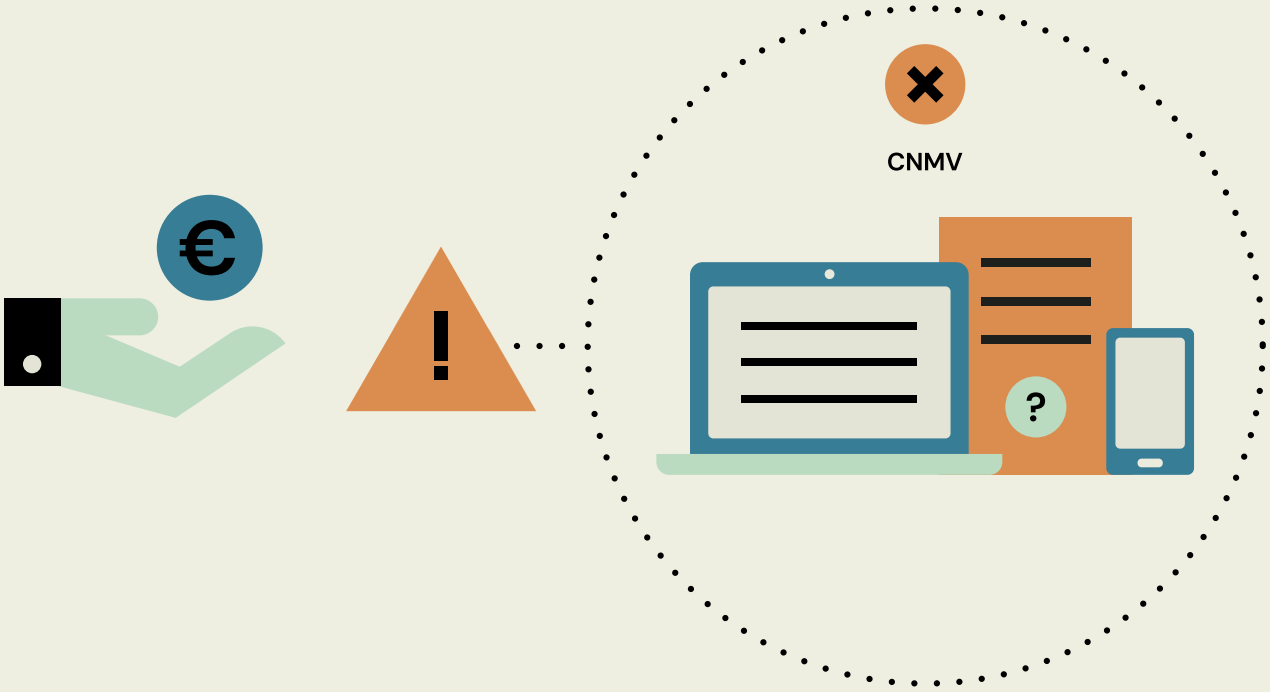
Caer víctima de una estafa financiera puede causarte grandes pérdidas económicas, así que más vale prevenir y aprender a identificarlas.

¿Cómo puedes identificar una estafa financiera?

Por ejemplo, si te prometen cuantiosas ganancias, utilizan métodos de inversión infalibles o facilitan soluciones imposibles a los problemas económicos. Las modalidades de engaño son infinitas y, en la mayoría de los casos, parten de una promesa de rentabilidad futura – lejos de las existentes en el contexto económico - a cambio de entregar un capital inicial al supuesto experto o entidad no autorizada para ofrecer este tipo de servicio.

Desconfía siempre de promesas de altos rendimientos futuros mediante inversiones infalibles.

Los términos **«chiringuito financiero»** o **«entidades pirata»**, definen de manera informal a aquellas entidades que ofrecen y prestan servicios de inversión **sin estar autorizadas** para hacerlo. Son peligrosos porque en la mayoría de los casos son, sencillamente, estafadores. La aparente prestación de tales servicios es solo una tapadera para apropiarse del capital de sus víctimas. Utilizan los mismos canales comerciales que puede emplear cualquier entidad legítima: teléfono, correo electrónico, páginas web, redes sociales, etc., aunque su modo de actuar es muy distinto.



Mientras las empresas autorizadas para prestar servicios de inversión están registradas y sometidas a las normas que regulan los mercados de valores y a estrictos controles por parte de los organismos supervisores (CNMV, Banco de España y Dirección General de Seguros y Fondos de Pensiones), los chiringuitos financieros actúan al margen de la legalidad.

Sus víctimas tampoco tienen las garantías de las que sí cumplen con las normas, como la cobertura de los Fondos de Garantía de Inversiones o de Depósitos y, por tanto, no pueden ser indemnizadas por el engaño sufrido.

¡Confiar en un chiringuito financiero es una forma segura de perder tu dinero!

La principal protección frente a un chiringuito financiero es identificarlo como tal. Lo más aconsejable es no confiar en ninguna entidad desconocida mientras no se haya podido verificar que está debidamente autorizada para prestar servicios de inversión.

Puedes verificarlo en el **registro de la CNMV,** del **Banco de España** o de la **Dirección General de Seguros y Fondos de Pensiones.** Otra opción rápida y sencilla es pedir información a la CNMV, llamando al teléfono **900 535 015.**

II. Tipos de estafas (y cómo evitarlas)

A continuación, se detallan una serie de prácticas que pueden ayudarte a identificar un chiringuito financiero como tal, así como recomendaciones para evitar ser víctima de sus estafas y fraudes.

2.1 Suplantación de identidad de entidades autorizadas

Empresas no autorizadas utilizan datos identificativos de empresas autorizadas e inscritas en la CNMV con el fin de confundir al inversor dando una apariencia de legalidad. Estas **«empresas clonadas»** son chiringuitos financieros. Utilizan ilegítimamente, incluso en sus páginas web, elementos identificativos idénticos o muy similares a los de empresas debidamente autorizadas e inscritas o sus mismas URLs, con cambios mínimos y casi imperceptibles.

Antes de contratar un producto financiero, comprueba los datos de la empresa oferente: denominación social, marca comercial, dominio y dirección web, sede y dirección postal, o número de registro en el organismo supervisor.

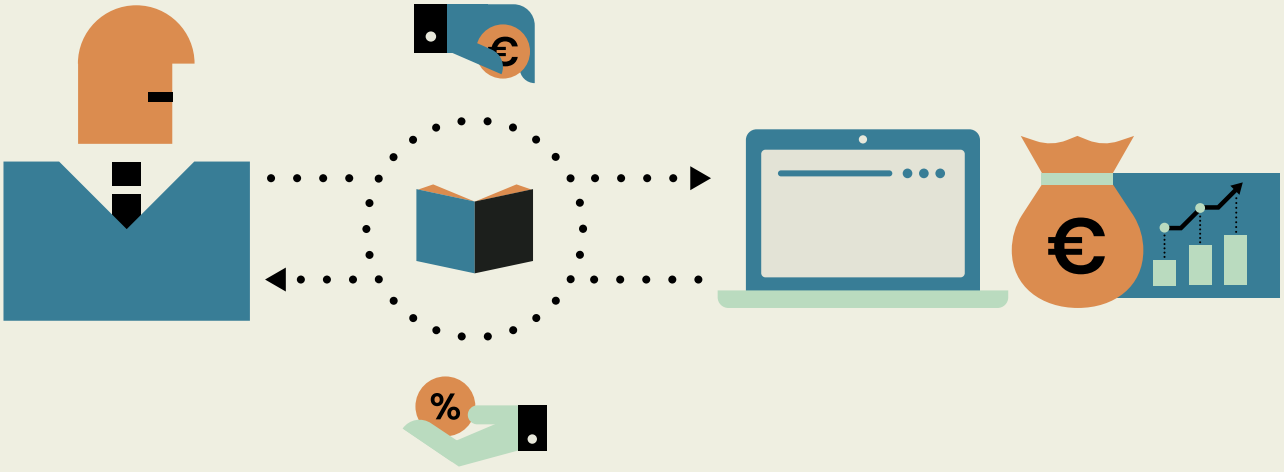
Asimismo, rechaza ofertas inesperadas o no solicitadas hasta comprobar que proceden de entidades debidamente inscritas en CNMV. Hay empresas y/o sitios web identificados en el registro de la CNMV con la palabra «clon», que no tienen vinculación alguna con las entidades autorizadas a las que suplantan la identidad. No confíes tu dinero a una de ellas porque están engañándote.

La comprobación de los datos de la entidad siempre se debe hacer desde la página web de la CNMV - **CNMV - Búsqueda por entidades.**

2.2 Servicio de cuentas de trading financiadas ligadas a cursos de formación.

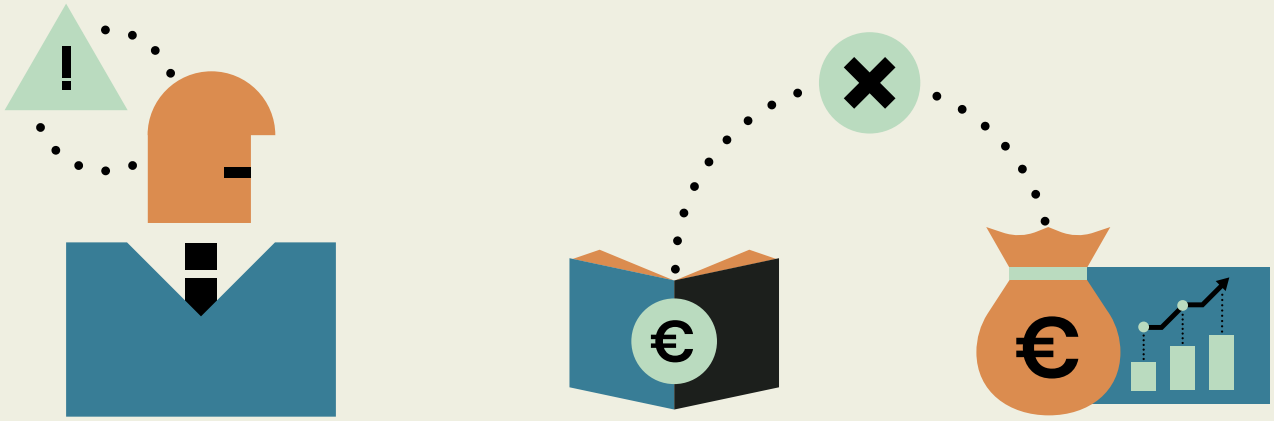
Existen determinadas páginas web que ofrecen un servicio que se denomina genéricamente **cuentas de trading financiadas.**

Dichos servicios ofrecen la posibilidad de acceder a una cuenta de valores para realizar operaciones como comprar y vender acciones, CFDs, Forex, etc. La particularidad es que el usuario no arriesgaría capital propio, operando aparentemente con el que le aportaría la propia página y a cambio, obtendría supuestamente un porcentaje de las ganancias obtenidas.



Para poder hacer uso de esas cuentas de trading financiadas, el usuario debe realizar un curso en el que, entre otras materias, se le explican las reglas de trading que ha de seguir y tiene que superar unas pruebas operativas en un entorno simulado y dentro de unos parámetros operativos (pérdida máxima diaria, nivel de riesgo, etc.). Dicho curso exige el abono de una cantidad previa, en ocasiones de varios miles de euros, para poder asistir.

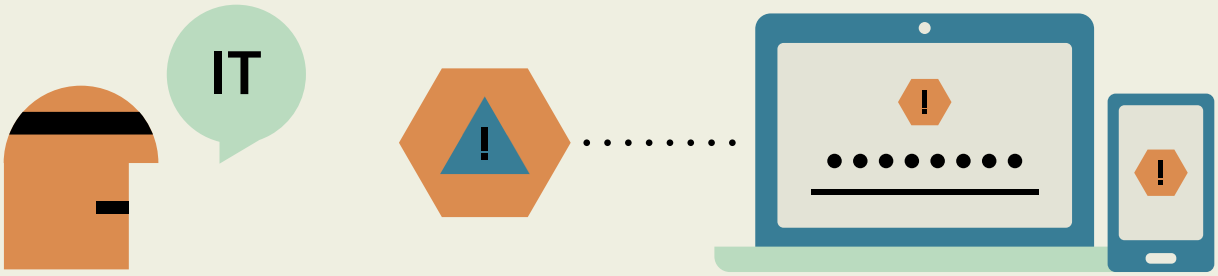
En muchas ocasiones, estos cursos son fraudes. Las víctimas pierden el dinero entregado para realizar el curso y nunca consiguen el acceso a la cuenta de trading financiada.



Sé consciente de los riesgos por la contratación de los cursos, entre ellos el de fraude o engaño en cuanto a la posibilidad de acceso a las cuentas de trading financiadas. Además, la impartición de estos cursos o la apertura de las citadas cuentas no entran dentro del ámbito de actuación y supervisión de la CNMV.

2.3 Nuevas estrategias informáticas (fraude del técnico informático)

Algunos chiringuitos utilizan herramientas informáticas para conectarse al dispositivo de un inversor y apropiarse de datos (como códigos de acceso o contraseñas) que les permiten operar sobre las cuentas de valores del inversor sin autorización.



Habitualmente, se hacen pasar por un técnico informático de la plataforma de inversión o de otra conocida empresa, que te alerta de algún problema en tu ordenador, móvil u otro dispositivo (por ejemplo, un cambio necesario de configuración). Para solucionar el supuesto problema, te piden que descargues un programa o app para conectarse a tu equipo en control remoto.

A veces, el propio chiringuito financiero te recomienda silenciar tu dispositivo y que te despreocupues del asunto. En realidad, lo que pretenden es acceder a tus cuentas bancarias o de valores, robar tus datos personales y/o hacer compras por Internet con tu tarjeta de crédito.

No compartas con terceros las claves de acceso a tus cuentas bancarias y de valores.

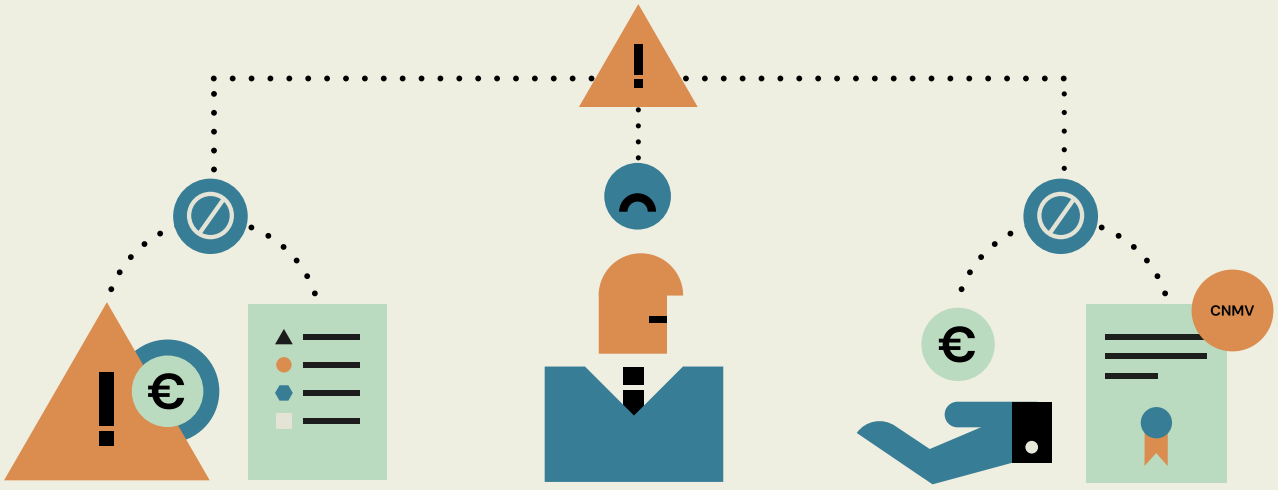
No permitas el acceso remoto a tus dispositivos informáticos.

No inicies una sesión para operar con tus cuentas bancarias y de valores con un tercero conectado.

2.4 Actividad de recovery room

Empresas denominadas ***«recovery room»*** contactan con personas que han sido víctimas de chiringuitos financieros, supuestamente para gestionarles la recuperación de las pérdidas o para recomprar acciones o valores adquiridos a través de empresas no autorizadas.

Estas estafas pueden provenir del chiringuito financiero que realizó el fraude inicial o de otras personas o empresas que hayan adquirido las listas de afectados. Pueden intentar que vuelvas a invertir dinero o, incluso, vender tus datos a otras empresas. Es decir, se trata de un fraude sobre otro engaño anterior, a menudo realizado por la misma entidad o personas.

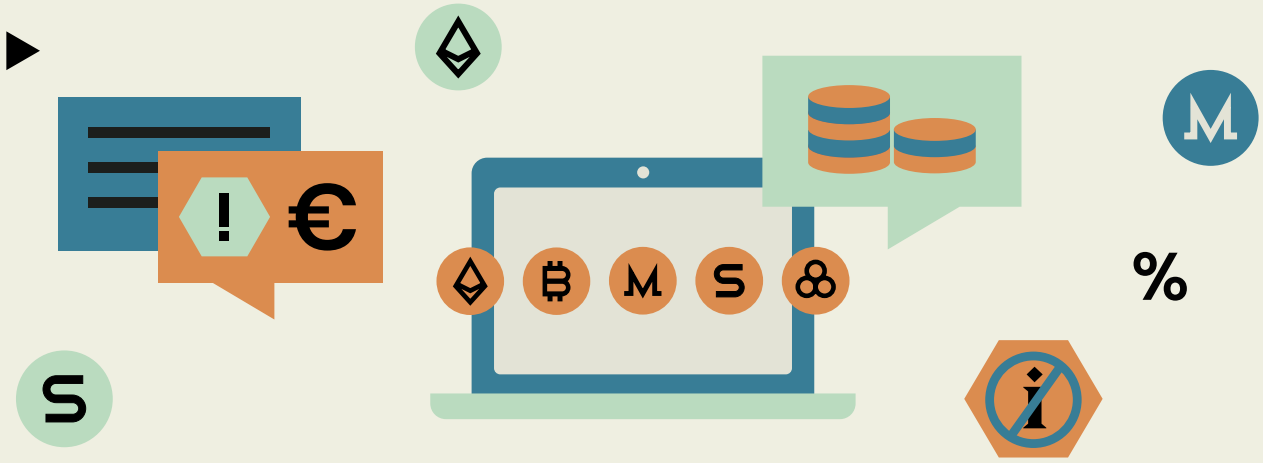


Si una empresa contacta contigo y te pide dinero por adelantado en concepto de pago por honorarios o impuestos, como requisito previo para prestar el servicio de recuperación de una inversión fallida o para la compra de acciones, es un indicio de que se trata de una *«recovery room»*. Nunca hagas un pago adelantado por este tipo de servicio.

Desconfía también si te contactan en nombre de la CNMV con el fin de recuperar las pérdidas sufridas. La CNMV nunca contactará directamente con posibles afectados ni autoriza el uso de su identidad o imagen corporativa con el fin de recuperar pérdidas.

2.5 *Fraudes relacionados con criptoactivos*

Los criptoactivos, incluyendo las criptomonedas o criptodivisas, pueden definirse como una representación digital de valor o derechos, es decir, son activos que no existen de forma física.



Existen numerosos criptoactivos falsos y estafas cuyo único objetivo es privarte de tu dinero. Se anuncian al público de manera agresiva en redes sociales, mensajes de texto, correo electrónico, por teléfono y mediante anuncios que aparecen en páginas web y redes sociales. Los estafadores utilizan diferentes técnicas, prometen increíbles ganancias y presionan a tomar decisiones rápidas con el objetivo de «no perder la oportunidad». La información suele ser poco clara y llena de tecnicismos sobre nuevas y complejas tecnologías para confundir al inversor.

No te fíes nunca de promesas de ganancias extraordinarias en poco tiempo y asegúrate de que las empresas están autorizadas y que no figuren en la «**lista negra**» de advertencias de las autoridades nacionales competentes. Desconfía siempre de propuestas de inversión que utilizan un lenguaje técnico difícil de entender.

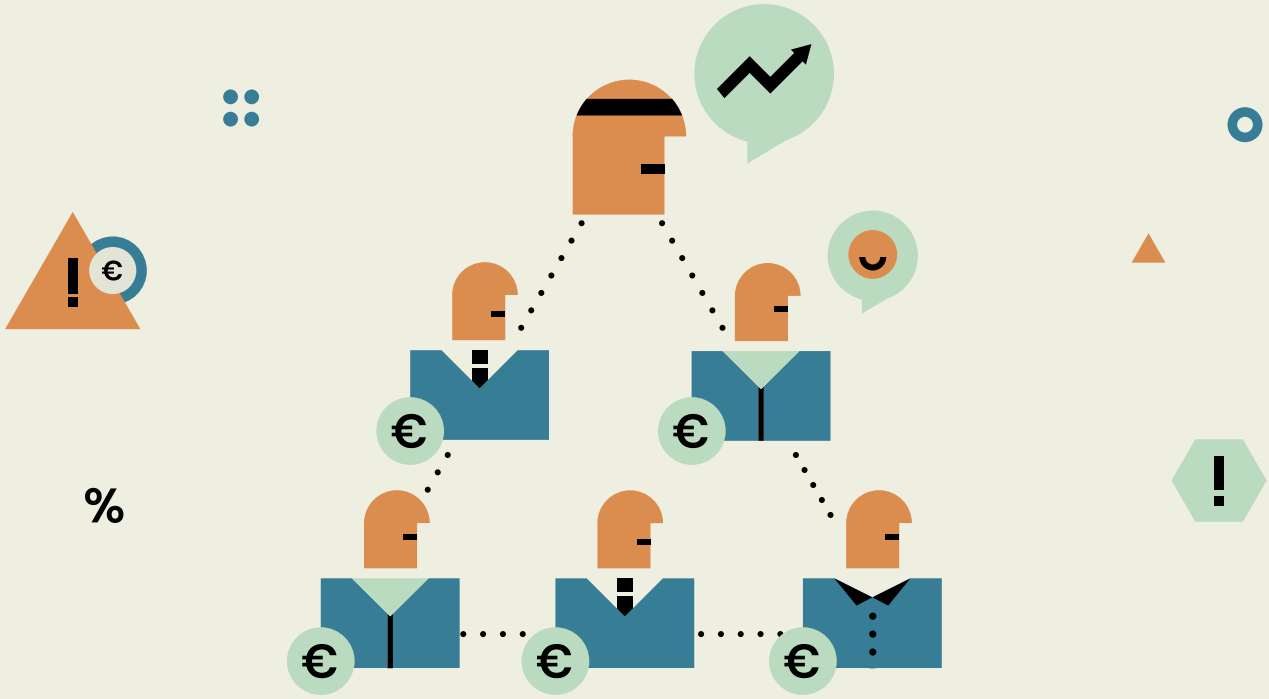
Nunca inviertas tu dinero en algo que no entiendes. Los intermediarios legítimos nunca te presionarán para tomar decisiones de inversión precipitadas.

¡Recuerda! Al no ser instrumentos financieros, depósitos o cualquier otro producto regulado, los criptoactivos quedan fuera de la protección que ofrecen las normas vigentes en España y la Unión Europea sobre servicios financieros.

2.6 *Esquemas Ponzi*

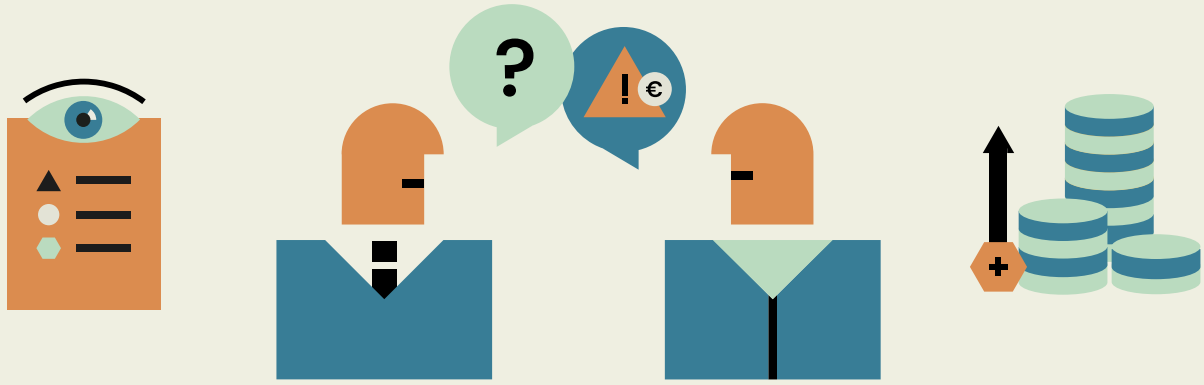
Un esquema Ponzi es una variante de la típica estafa piramidal, un modelo de negocio insostenible en el que unos pocos estafadores originales reclutan a nuevos participantes para formar parte de su negocio, creando una jerarquía en forma de pirámide.

En el caso de un esquema Ponzi de inversión, un estafador convence a nuevos inversores a aportar fondos para ser invertidos, ofreciéndoles altas rentabilidades. En realidad, el dinero no se invierte o se invierte solo en parte; los chiringuitos pagan «beneficios» (a veces muy grandes, aunque no siempre son los prometidos) a los primeros clientes, utilizando para ello el de los nuevos inversores.



Esos primeros clientes satisfechos (que suelen reinvertir sus beneficios) a veces actúan, sin saberlo, como cebo, y convencen a sus amigos y familiares a que también aporten dinero. Parte de las nuevas aportaciones puede servir para pagar a los clientes anteriores, pero la mayoría se lo queda el chiringuito.

Cuando deja de entrar dinero nuevo, o cuando lo decide el estafador, se colapsa el entramado y los clientes se quedan sin sus inversiones y sin su capital original.



La mejor forma de evitar ser víctima de un esquema Ponzi es desconfiar siempre de su reclamo principal: rentabilidades demasiado altas con respecto a las que ofrece el mercado. También es importante no basar las decisiones de inversión únicamente en la confianza o recomendaciones de amigos o familiares. Lo que es bueno para un inversor puede no serlo para otro, dependiendo de sus diferentes circunstancias personales y financieras. Utiliza las recomendaciones personalizadas de inversión de profesionales o entidades autorizadas para ello.

2.7 *Phising, smishing y vishing*

Todas estas técnicas, así como otras variantes de estas, tienen como objetivo conseguir nuestras claves personales de acceso a nuestras cuentas bancarias o de valores, con el fin de suplantar nuestra identidad, operar con nuestras cuentas y disponer de nuestros fondos.

El ***phising*** son correos electrónicos que parecen proceder de entidades financieras u otras entidades reconocidas y solventes (comercios electrónicos, correos, administraciones públicas...) que, por motivos «de seguridad», solicitan al destinatario hacer clic en algún enlace o hipervínculo que dirige a una página web falsa que simula ser la web legítima, e introducir sus claves de acceso u otros datos personales.

El ***smishing*** es una variante de la misma técnica, que utiliza SMS fraudulentos, en vez de correo electrónico.

El ***vishing,*** cuyo nombre deriva de la combinación de voz y phishing, es un fraude que persigue obtener datos personales y bancarios a través de una llamada telefónica, engañando a la víctima mediante la suplantación de la identidad de un tercero de confianza (por ejemplo, simulando ser empleado de una entidad financiera).

Evitar caer víctima del *phishing, smishing o vishing* no es difícil.

- Nunca respondas a correos electrónicos, mensajes de texto o llamadas telefónicas que solicitan información personal o confidencial.
- Elimínalos y no descargues ni ejecutes los ficheros adjuntos.
- No accedas a tu entidad a través de enlaces, sino tecleando la dirección URL auténtica en la barra de direcciones. Si la solicitud parece legítima, llama y pregunta en un número de teléfono establecido por la entidad verdadera (NO el que figura en el correo o mensaje) para verificarla.
- Crea contraseñas complejas (combinaciones de números y letras, mayúsculas y minúsculas, caracteres especiales…) únicas para cada sitio web y cámbialas con regularidad. Si crees que has sido víctima de una de estas técnicas, cambia tus claves de inmediato y avisa a tu entidad.

Es importante recordar que ninguna entidad financiera autorizada pedirá jamás a sus clientes información personal ni claves completas. Ellos ya disponen de esos datos y bajo ningún concepto necesitan pedírtelos y, menos aún, por medios tan poco confidenciales como el correo electrónico o el teléfono.

2.8 *Pharming*

El ***pharming*** es un cibercrimen parecido al *phishing*, pero más sofisticado. Los ladrones infectan tu equipo con *malware* que les permite redirigir el tráfico de sitios web legítimos a sitios web falsos, creadas para recabar datos confidenciales y que tienen el mismo aspecto que las auténticas. Así, pueden engañarte para que introduzcas tus datos confidenciales sin ningún temor, sin saber que los estás remitiendo a un delincuente.

Precauciones para evitar la estafa de *pharming*

- Instala programas reconocidos antivirus y *antimalware* y actualiza tus dispositivos.
- Utiliza un gestor de contraseñas. Una página web falsa te puede engañar a ti, pero no al gestor de contraseñas. Si no has visitado la página anteriormente, no la reconocerá y no rellenará automáticamente tus datos de acceso.
- Desconfía si el sitio web parece extraño, si la URL en la barra de direcciones se ve distinta o si la página comienza a pedir información que normalmente no se solicita.
- Verifica que tienes una conexión segura — que la dirección empieza por «https» (y no «http») y que hay un icono de candado en la barra de direcciones. Haz clic en el candado para asegurarte de que el sitio web tiene un certificado de confianza actualizado.

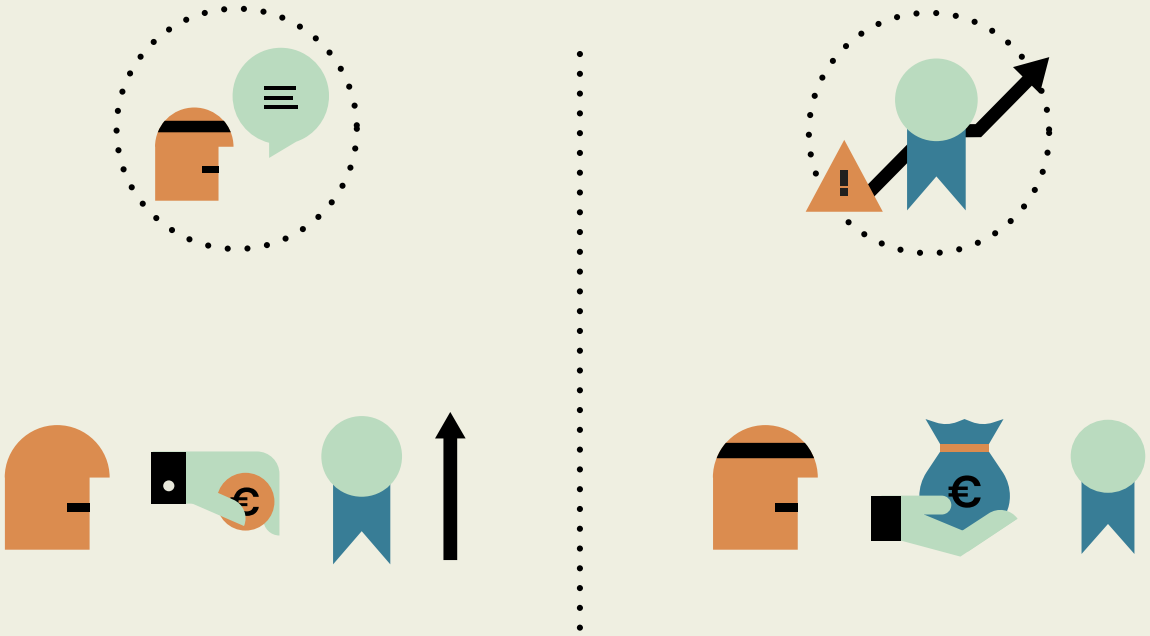
2.9 *Fraude financiero en redes sociales*

Actualmente, muchos inversores buscan información y consejos en las redes sociales. Los **«chiringuitos financieros»** o **«entidades pirata»** se aprovechan de esta tendencia para encontrar a sus víctimas. Aunque las redes sociales pueden aportar información válida y beneficiosa para inversores, también crean grandes oportunidades para estafas y fraudes.

Multitud de estafadores de todo tipo operan en redes sociales y suele ser difícil para las autoridades encontrarlos y poner fin a sus crímenes. Los estafadores pueden contactar con cientos de miles de personas de forma rápida y sin apenas esfuerzo económico. Es sumamente fácil y barato diseminar información engañosa en Telegram, TikTok, Instagram, Twitter, Facebook, etc., creando perfiles falsos, suplantando la identidad de entidades legítimas o publicando de forma anónima.

Las estafas propagadas por redes sociales incluyen todos los fraudes que ya hemos visto. Otro fraude común son los intentos de manipulación de mercado a corto plazo, diseminando rumores falsos o información engañosa sobre una empresa para afectar la cotización de sus acciones, positiva o negativamente.

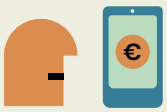
Por ejemplo, un rumor positivo sobre una empresa puede incitar a muchos inversores a comprar sus acciones, creando demanda desorbitada y haciendo subir mucho el precio de las acciones en poco tiempo, sobre todo si se propaga el rumor de forma «viral»



Cuando la cotización de las acciones alcance cierto nivel, los estafadores que empezaron el rumor venden sus acciones que han adquirido con anterioridad a menor precio, a un precio artificialmente alto, obteniendo ganancias. El mercado acabará corrigiéndose y la mayoría de inversores que compraron las acciones a precios altos sufrirán pérdidas. Lo mismo puede ocurrir a la inversa: rumores falsos negativos sobre una empresa pueden convencer a los inversores a vender sus acciones, lo que permite a los estafadores comprarlas a precios artificialmente bajos.

También hay que tener mucha precaución con los llamados «influencers financieros», es decir, personas que se dedican a hablar públicamente de sus estrategias de inversión, las ventajas de utilizar una determinada herramienta y la facilidad con la que obtienen beneficios de una forma rápida y sencilla.

Aunque existen personas honestas y entidades legítimas que publican recomendaciones de inversión en las redes sociales, muchos «influencers», son chiringuitos financieros que solo quieren atraer al público a plataformas digitales ilícitas o hacerles caer en algún otro tipo de estafa.



Aunque todo el mundo parezca estar a favor de determinados consejos de inversión a través de las redes sociales, no te dejes engañar. Aunque parezca que gran número de personas están invirtiendo en un producto determinado con aparente éxito, puede no ser verdad.

No te dejes llevar por el «efecto manada», un sesgo cognitivo que nos incita a actuar de una forma, simplemente porque lo que hacen los demás.

Desconfía siempre de ofertas de inversión no solicitadas que te llegan a través de redes sociales.

Asegúrate de verificar la fuente de cualquier información sobre inversiones que encuentras en Internet.

¡Cuidado con los «influencers financieros»,! Recuerda que los personajes famosos que dan recomendaciones de inversión en redes sociales normalmente reciben una compensación económica por hacerlo. Se les contrata porque tienen muchos seguidores. En ocasiones, ellos mismo son cómplices de estafadores, sin saberlo.

Aún en el mejor de los casos, las inversiones no son de talla única. Lo que puede ser recomendable para un inversor no siempre lo será para otro. Es más aconsejable acudir a un intermediario autorizado para recibir recomendaciones personales que encajen con tu perfil, objetivos y tolerancia al riesgo.

Nunca tomes decisiones de inversión basadas únicamente en recomendaciones de celebridades.

III. Resumen de recomendaciones para prevenir estafas y fraudes financieros

Confiar en una empresa no autorizada es una forma segura de perder tu dinero. Como no son verdaderos profesionales de los mercados financieros, no es posible recurrir a ninguno de los mecanismos de protección del inversor previstos en las disposiciones legales. Repasemos las principales recomendaciones para evitar estafas y fraudes financieros.

1

Lo más importante es no entregar nunca dinero a un intermediario sin haber verificado que figura en los registros de la CNMV, del Banco de España o de la Dirección General de Seguros y Fondos de Pensiones como entidad autorizada para prestar los servicios de inversión que quieres contratar. Lo más rápido y sencillo es pedir esta información a la CNMV. Comprueba también si la CNMV ha publicado una advertencia sobre la empresa.

> El teléfono de atención al inversor 900 535 015 de la CNMV está a tu disposición para informarte sobre la habilitación de las entidades para prestar o no servicios de inversión.

Desconfía de ofertas de entidades que dicen estar autorizadas pero cuya dirección está incompleta o no existe, el contacto es a través de números de móvil o cuyo prefijo no es español.

2. Desconfía siempre de cualquier propuesta de inversión que no hayas solicitado, sea a través del teléfono, correo electrónico, mensajes en redes sociales, o cualquier otro canal. Cuanto más tentadora es la oferta, más seguridad de que sea un fraude. Los intermediarios financieros autorizados no se dirijan a personas que no son clientes con ofertas de inversión.

3. Desconfía siempre de ofertas en productos de inversión que aseguran grandes rentabilidades sin riesgo. Estas promesas son falsas. A mayor rentabilidad potencial, mayor es el riesgo asumido. No hay inversión sin riesgo.

4. Desconfía de ofertas de financiación o de inversión en condiciones muy favorables de entidades situadas en países remotos, de las que no puedes obtener información. Casi siempre se trata de «entidades fantasmas» que te pedirán que envíes una cantidad de dinero que no recuperarás.

5. Protege tus datos personales. No compartas tus claves de acceso con terceros y desconfía siempre de los correos electrónicos, mensajes de texto o llamadas telefónicas que solicitan estos datos. No sigas ningún enlace de un correo electrónico sin haber verificado su procedencia.

6. Desconfía siempre de personas o empresas que intentan suplantar la identidad de la CNMV, utilizando su nombre o su logotipo para hacer recomendaciones o vender productos de inversión. Estas recomendaciones y ofertas siempre son estafas, ya qua la CNMV nunca recomienda inversiones.

7. Nunca tomes decisiones de inversión basadas únicamente en recomendaciones vistas en redes sociales y averigua la fuente de la información.

IV. ¿Qué hacer si has sido víctima de una estafa?

Si ya has entregado dinero a un chiringuito, no siempre será posible recuperarlo. Sin embargo, es importante estar atento a ciertas señales, para intentar reaccionar lo antes posible:

- La persona de contacto se vuelve inaccesible, no atienden a las solicitudes de reembolso, no se recibe ninguna información o la que se obtiene es insuficiente e incomprensible, etc. Estos son algunos de los comportamientos irregulares que delatan a un chiringuito financiero. En tales casos es aconsejable presionarles para que devuelvan el dinero, amenazándoles si es necesario con acudir a las autoridades. Este aviso no siempre es efectivo, ya que precisamente su situación de ilegalidad les permite desaparecer o cambiar de nombre con gran facilidad, lo que dificulta la actuación de los organismos supervisores.

- En ocasiones, su respuesta es que la inversión no ha resultado como se esperaba, que se han registrado pérdidas y que precisamente en ese momento no conviene deshacer posiciones sino aumentar la inversión, para aprovechar el inminente cambio de tendencia. Lo realmente peligroso en este caso es continuar realizando aportaciones, ya que con toda seguridad ese capital tampoco se va a recuperar.

- Tanto si consigues que te devuelvan todo o parte del capital como si no es así, es muy importante que pongas los hechos en conocimiento de la CNMV y denuncies lo ocurrido a la Policía o al Juzgado correspondiente. Puede ser la única oportunidad de recuperar tu inversión. Las denuncias presentadas permiten a los organismos responsables difundir las correspondientes advertencias, ayudando a que otros inversores no se vean estafados por el mismo chiringuito.

- Recuerda que, para garantizar la eficacia de una posible actuación judicial, deberás presentar toda la documentación que acredite los servicios recibidos y los importes implicados.

¿Necesitas más información?

Contáctanos por email

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

educacionfinanciera@cnmv.es