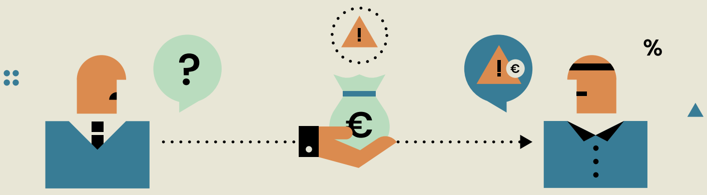
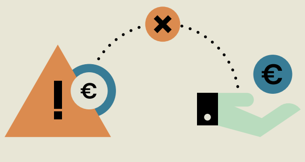
Tipos de estafas y fraudes financieros (y cómo evitarlos)

¿Qué es una estafa financiera?

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.

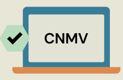




Los términos **«chiringuito financiero»** o **«entidades pirata»**, definen de manera informal a aquellas entidades que ofrecen y prestan servicios de inversión sin estar autorizadas para hacerlo.

Los chiringuitos financieros no están registrados ni sometidos a las normas y controles por parte de los organismos supervisores.

La principal protección frente a un chiringuito financiero es identificarlo como tal. Puedes verificarlo en el registro de la CNMV o llamando 900 535 015.



Nueve tipos de estafas y fraudes financieros (y cómo evitarlos)

1. Suplantación de identidad de entidades autorizadas

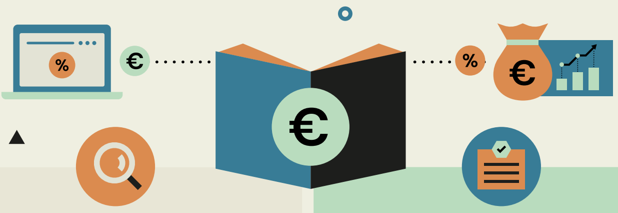
¿En qué consiste?

Empresas no autorizadas (chiringuitos financieros o entidades pirata) utilizan datos identificativos de empresas autorizadas e inscritas en la CNMV con el fin de confundir al inversor bajo una apariencia de legalidad.

¿Qué hacer?

- Rechaza ofertas no solicitadas hasta comprobar que proceden de entidades inscritas en CNMV.
- Antes de contratar un producto financiero, comprueba los datos de la empresa: denominación social, marca comercial, dominio y dirección web, sede y dirección postal, o número de registro en el organismo supervisor.

2. Cuentas de trading financiadas ligadas a cursos de formación



¿En qué consiste?

Páginas web que ofrecen servicios para operar con una cuenta de valores con la condición de realizar previamente un curso de formación. El pago del curso es, en muchas ocasiones, un fraude.

¿Qué hacer?

- Sé consciente de los riesgos de engaño o fraude por la contratación de los cursos. Su impartición o la posibilidad de acceso a las cuentas de trading financiadas no entran dentro del ámbito de actuación y supervisión de la CNMV.

3. Fraude del técnico informático

¿En qué consiste?

Estafadores se hacen pasar por técnicos informáticos que instalan herramientas para conectarse al dispositivo de un inversor, apropiarse de sus datos y operar sobre sus cuentas de valores sin autorización.

¿Qué hacer?

- 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.

4. Phising, smishing y vishing

¿En qué consiste?

Técnicas que tienen como objetivo conseguir las claves personales para acceder a cuentas bancarias o de valores, suplantar identidades, operar con ellas y disponer de los fondos.

¿Qué hacer?

- 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.
- Crea contraseñas seguras (combinaciones de números y letras, mayúsculas y minúsculas, caracteres especiales…).
- Ninguna entidad financiera autorizada pedirá jamás a sus clientes información personal ni claves completas.

5. Pharming

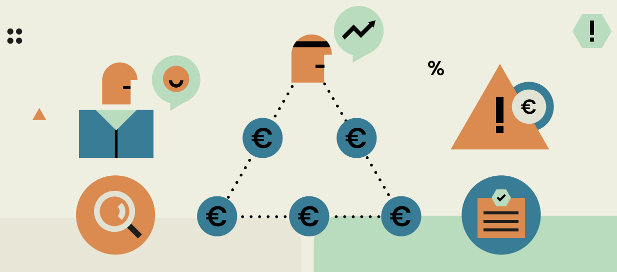
¿En qué consiste?

Cibercrimen por el que los ladrones introducen en el equipo informático un malware que redirige el tráfico de sitios web legítimos a sitios web falsos, creados para recabar datos confidenciales.

¿Qué hacer?

- Instala programas antivirus y antimalware y actualiza tus dispositivos. Utiliza también un gestor de contraseñas.
- Desconfía si el sitio web parece extraño, si la URL se ve distinta o si la página pide 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.

6. Estafa piramidal o esquema Ponzi



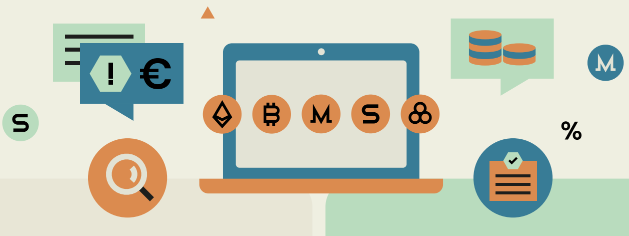
¿En qué consiste?

Es una estafa que atrae a inversores con promesas de altas rentabilidades. El dinero aportado no se invierte o se invierte solo en parte. El chiringuito financiero paga "beneficios" a los primeros clientes, utilizando para ello el dinero de los nuevos inversores.

¿Qué hacer?

- Desconfía siempre del reclamo principal: rentabilidades demasiado altas con respecto a las que ofrece el mercado.
- No bases las decisiones de inversión únicamente en la confianza o recomendaciones de amigos o familiares.
- Utiliza las recomendaciones personalizadas de inversión de profesionales o entidades autorizadas para ello.

7. Fraude relacionado con criptoactivos



¿En qué consiste?

Inversiones en criptoactivos falsos ofrecidos por estafadores que prometen increíbles ganancias en poco tiempo y sin riesgo, presionando a tomar decisiones rápidas con el objetivo de «no perder la oportunidad».

Se anuncian de manera agresiva en redes sociales, mensajes de texto, correo electrónico, etc.

¿Qué hacer?

- Nunca inviertas tu dinero en algo que no entiendes.
- 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.
- Sospecha de propuestas de inversión que utilizan un lenguaje técnico difícil de entender.
- Desconfía si te presionan para tomar decisiones de inversión precipitadas.

8. Fraude financiero en redes sociales

¿En qué consiste?

Multitud de estafadores operan en redes sociales de diferentes formas: creando perfiles falsos, suplantando la identidad de entidades legítimas, o diseminando rumores falsos o información engañosa sobre una empresa para afectar a la cotización de sus acciones.

¿Qué hacer?

- Desconfía 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.
- Nunca tomes decisiones de inversión basadas únicamente en recomendaciones de celebridades.
- Acude a un intermediario autorizado para recibir recomendaciones personales que encajen con tu perfil, objetivos y tolerancia al riesgo.

9. Recovery room

¿En qué consiste?

Son empresas que contactan con víctimas de chiringuitos financieros para supuestamente gestionar la recuperación de su dinero. Son fraudes sobre engaños anteriores.

¿Qué hacer?

- Desconfía si contactan contigo y te piden dinero 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.
- Sospecha 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.

¿Qué hacer si has sido víctima de una estafa?

Pon los hechos en conocimiento de la CNMV y denuncia lo ocurrido a la Policía, Guardia Civil o al Juzgado correspondiente.

CNMV
Comisión Nacional del Mercado de Valores

Descárgate la guía completa aquí:

www.cnmv.es/Portal/Publicaciones/Guias.aspx

www.cnmv.es