CONSEJOS PARA PREVENIR EL FRAUDE EN OPERACIONES DE INVERSIÓN

Iniciativa Educativa del Banco de España

Esta es una iniciativa del Banco de España destinada a divulgar conocimientos básicos de Educación Financiera entre la ciudadanía española.

Por favor, tenga en cuenta que **la modificación de los contenidos no está autorizada**.

Esta presentación se ha realizado con la colaboración de la Comisión Nacional del Mercado de Valores, a quienes mostramos nuestro agradecimiento.

Gracias.

A. COLECTIVOS DESTINATARIOS: toda la población, a un nivel básico.

B. OBJETIVOS:
- Tomar conciencia del aumento del fraude en el entorno digital, particularmente en las operaciones de inversión y en qué manera puede afectar a nuestro bolsillo
- Informar de los métodos más habituales que utilizan los estafadores para engañarnos
- Proponer consejos para protegernos contra el fraude en operaciones de inversión
- Recalcar que el uso del sentido común es el arma más eficaz contra el fraude, habida cuenta de los nuevos métodos de fraude que van apareciendo

C. CONTENIDOS

1. Chiringuitos financieros
2. Estafa de "recovery room"
3. Cuentas de trading ligadas a cursos de formación
4. Estafa piramidal o esquema Ponzi
5. Fraudes con criptoactivos
6. Fraudes en redes sociales
7. Cuentas "mula"
8. Precauciones
9. ¿Qué hago si he sido víctima de un fraude?

Inversiones – Web CNMV

---

1. Chiringuitos financieros

El término **«chiringuito financiero»** define de manera informal a aquellas entidades que ofrecen y prestan servicios de inversión o financiación 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 sometidas a las normas que regulan los mercados de valores y a estrictos controles por parte de los organismos supervisores (CNMV y Banco de España), los chiringuitos financieros actúan al margen de la legalidad. Sus víctimas tampoco tienen la cobertura de los Fondos de Garantía de Inversiones o de Depósitos.

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

Precauciones

- Comprueba siempre que la entidad está autorizada para prestar los servicios financieros que ofrece.
- Pide información a la CNMV o al Banco de España.

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 los servicios financieros que ofrece. Lo más rápido y sencillo es pedir información la autoridad competente — la CNMV (servicios de inversión) o el Banco de España (servicios bancarios y de financiación).

Para más información, conviene consultar el Decálogo para Evitar Chiringuitos Financieros, de la CNMV, así como el Portal del Cliente Bancario del Banco de España.

2. Estafa 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.

Precauciones

- 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.

3. Cuentas de trading ligadas a cursos de formación

Una cuenta de trading es una cuenta de operaciones abierta a nombre del cliente en una compañía bróker. En ella se almacena el dinero real del cliente, cual necesita para realizar operaciones de compra y venta de instrumentos financieros

Existen páginas web que ofrecen la posibilidad de acceder a una cuenta de valores para realizar operaciones de diversa naturaleza (bursátiles, CFDs, Forex…). Las cuentas de trading financiadas tienen la particularidad de 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, teniendo que superar unas pruebas operativas en un entorno simulado y dentro de unos parámetros operativos (pérdida máxima diaria, nivel de riesgo…). Dicho curso exige el abono de una cantidad previa, en ocasiones de varios miles de euros, para poder asistir.

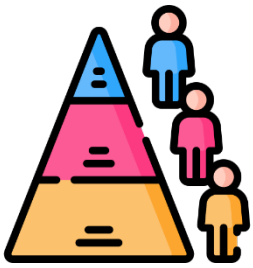
Precauciones:

- 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/supervisión de la CNMV.

4. Estafa piramidal o esquema 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 para 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.

Precauciones

- 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.

5. Fraudes 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. Los estafadores utilizan diferentes técnicas, prometiéndote increíbles ganancias y presionándote a tomar decisiones rápidas para no «perder la oportunidad». La información suele ser poco clara y llena de tecnicismos sobre nuevas y complejas tecnologías para confundir al inversor.

Precauciones

- No te fíes nunca de promesas de ganancias extraordinarias en poco tiempo.
- Asegúrate de que las empresas 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.

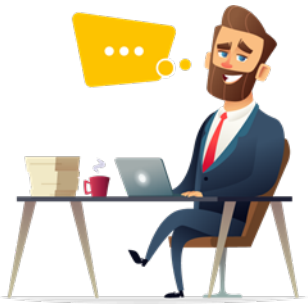
¡Recuerda! Al no ser instrumentos financieros, depósitos o cualquier otro producto regulado, los criptoactivos quedan fuera de la protección que ofrecen las normas vigentes en la Unión Europea sobre servicios financieros.

6. Fraudes 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.

Otro fraude en redes es la utilización de la imagen de personas famosas, actores, cantantes o incluso responsables públicos cuya identidad se utiliza asignándoles declaraciones que nunca han hecho. Entre los formatos utilizados, destacan vídeos falsos en los que se simula la voz de un personaje o de un responsable público para recomendar estas inversiones fraudulentas, lo que se conoce como **deepfake**. También se utilizan los diseños y apariencia de medios online para acreditar falsas informaciones sobre esos personajes. Finalmente, esos anuncios y páginas no reales enlazan a la página de entidades no autorizadas para prestar servicios de inversión en las que se intenta captar datos y fondos de inversores. La CNMV recuerda a todos los inversores que la utilización de personajes famosos con promesas de fáciles y rápidas ganancias o la simulación de medios o imágenes reales son señales inequívocas de que se trata de un fraude financiero por lo que recomienda que no se faciliten ningún tipo de dato personal (incluidos email o teléfono), y mucho menos fondos, a estas entidades.

Precauciones

- 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.

7. Cuentas "mula"

¿Qué es una cuenta mula?: Es una cuenta corriente, como cualquier otra, pero que se utiliza total o parcialmente para transferir dinero de origen dudoso a otras cuentas, o para hacer pasar por legal (blanquear) el dinero obtenido de actividades criminales- ingresas dinero que te ha dado otro, y luego lo sacas y se lo das, quedándote una parte. Es un dinero que hay que mover rápidamente.

¿Y cómo me convierto en "mulero" ? Pues casi sin darme cuenta, porque se capta fácilmente la atención de los jóvenes. Las redes sociales son un campo muy amplio (Instagram, Tik Tok…) ya que es difícil saber quién está actuando de buena fe y quién no. También captan por la facilidad y poco esfuerzo que supone obtener unos euros – solo das un dato, dejas usar una cuenta o abres cuentas por internet, que roba muy poco tiempo. O se ofrecen criptomonedas o moneda que sirve para determinados videojuegos sin que cueste nada. O te captan amigos o compañeros, que ya forman parte de esta red y a los que prometen más dinero cuantas más personas convenzan. Y otro sistema es hacerte creer que si participas alguien va a mostrar interés por ti, o si ya está contigo, te propone participar como prueba de confianza.

¿Cómo se abre, o se usa? Con solo dar tu número de cuenta a alguien – voluntaria o involuntariamente-, o incluso dando un dato como puede ser el DNI – mucho más si pones a disposición una fotografía del mismo- se puede abrir una cuenta en tu nombre o muchas cuentas, que luego se emplean para blanquear dinero. Y también puedes ser tú quien directamente uses tu cuenta para esta actividad -además de las normales que haces-, o abras cuentas que se usen para esto.

MUY IMPORTANTE: Muchos no lo saben, pero si colaboras con quienes están usando tus cuentas o tus datos para blanquear dinero, eres cómplice de ellos y te conviertes en delincuente. Y puedes ser juzgado y condenado. Facilitar mover el dinero a criminales no sale gratis.

Precauciones

- Desconfía de las ofertas atractivas con las que consigues dinero, criptos u otras cosas de manera fácil, sin esfuerzo.
- Fundamental: no dar tus datos bancarios o personales a nadie, salvo que estés seguro de que quien los pide tiene derecho a ello (por ejemplo, a tu banco si se los tienes que dar), o vas acompañado de tus responsables (padres, tutores…).
- No se debe confiar en quien te dice que hace esto y es algo normal, o no pasa nada. No es verdad.
- Tienes que evitar pinchar enlaces de mensajes (SMS/WhatsApp) o que aparezcan en redes sociales, aun en forma de propaganda. Y no te dejes convencer para dar información o acudir a citas con quien no conoces. Nunca se debe bajar la guardia, porque no sabes realmente quién está detrás de las mismas. (Recordar casos recientes de influencers condenados)
- Y si piensas que alguien te está queriendo captar, díselo a un adulto de confianza, que te ayudará.

8. Precauciones

- 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. Por muy tentadora que sea la oferta, es casi seguro que se trata de un fraude. Los intermediarios financieros autorizados no se dirijan a personas que no son clientes con ofertas de inversión.

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

- Igualmente, debes desconfiar 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. Suelen ser páginas web falsas.

- Desconfía de ofertas de inversión no solicitadas que te llegan por redes sociales

- Desconfía siempre de ofertas de inversión que aseguran rentabilidades muy por encima del promedio del mercado para productos similares, o alta rentabilidad sin riesgo. Estas promesas son falsas. La inversión en bolsa siempre tiene riesgo. En general, a mayor rentabilidad potencial, mayor es el riesgo.

- Desconfía también 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 fantasma que te pedirán que envíes una cantidad de dinero que no recuperarás.

- 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 que la CNMV nunca recomienda inversiones.

- 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.

- Vigila SMS o mail sospechosos: Comprueba la dirección electrónica de cualquier mensaje cuyo remitente sea desconocido. Si contienen enlaces, verifícalos con el cursor sin pinchar antes de acceder, y evita abrir archivos adjuntos.

- Utiliza tarjetas prepago en comercios online: Pagar con este tipo de tarjetas te permite limitar la pérdida de dinero en caso de un posible fraude.

- Establece un límite en tu tarjeta de crédito: Ajusta el límite de tu tarjeta en función de tu nivel de gasto para proteger tu dinero.

- Usa el sentido común: El fraude suele producirse cuando tú recibes una llamada, un SMS o un mail en que te acaban pidiendo algo y metiéndote prisa. Nunca atiendas las peticiones de realizar ninguna acción en ese momento y dirígete tú a tu entidad para asegurarte de con quien estás hablando.

Nota: Comentar a la audiencia que el Banco de España y la CNMV reciben reclamaciones o consultas en las que el banco no puede hacer nada ante la estafa que han sufrido determinados clientes porque no son responsables de las pérdidas (es decir, no pueden reembolsarles el dinero que han perdido o compensarles de alguna manera). Este no siempre es el caso, pero es importante que como usuarios seamos conscientes de los riesgos que podemos sufrir o las pérdidas que podemos tener. ¡Seamos prudentes!

9. ¿Qué hago si he sido víctima de fraude?

1. Denuncia el caso a las Fuerzas y Cuerpos de seguridad del Estado.
2. Si se han producido cargos en tu cuenta por el uso fraudulento de la tarjeta:
   - Solicita el bloqueo a la entidad y modifica la clave de acceso a la banca electrónica.
   - Acude a la entidad y cumplimenta el formulario de cargos no reconocidos.
   - En su caso, plantea reclamación ante el Servicio de Atención al Cliente, y en última instancia, ante el Banco de España o ante la CNMV.

Inversiones – Web CNMV

- Guía sobre Estafas y fraudes
- Infografía
- Guía sobre Chiringuitos financieros
- Podcast sobre estafas
- Guía sobre Estafas y fraudes
- Infografía sobre Estafas y fraudes
- Infografía Chiringuitos financieros
- Guía sobre Chiringuitos financieros
- Podcast sobre estafas
- Curso online sobre estafas
- Reel @natcher