PRECAUCIONES A SEGUIR EN LAS PÁGINAS DE INVERSIÓN *ONLINE* PARA NO CAER EN ENGAÑOS

Las inversiones *online* han ganado popularidad, pero también **han atraído a estafadores** que buscan aprovecharse de inversores desprevenidos. **Los fraudes** más comunes abarcan desde estafas piramidales, fraudes con criptomonedas hasta tácticas engañosas en redes sociales. Conocer estos fraudes te permitirá actuar con precaución y **proteger tu dinero.**

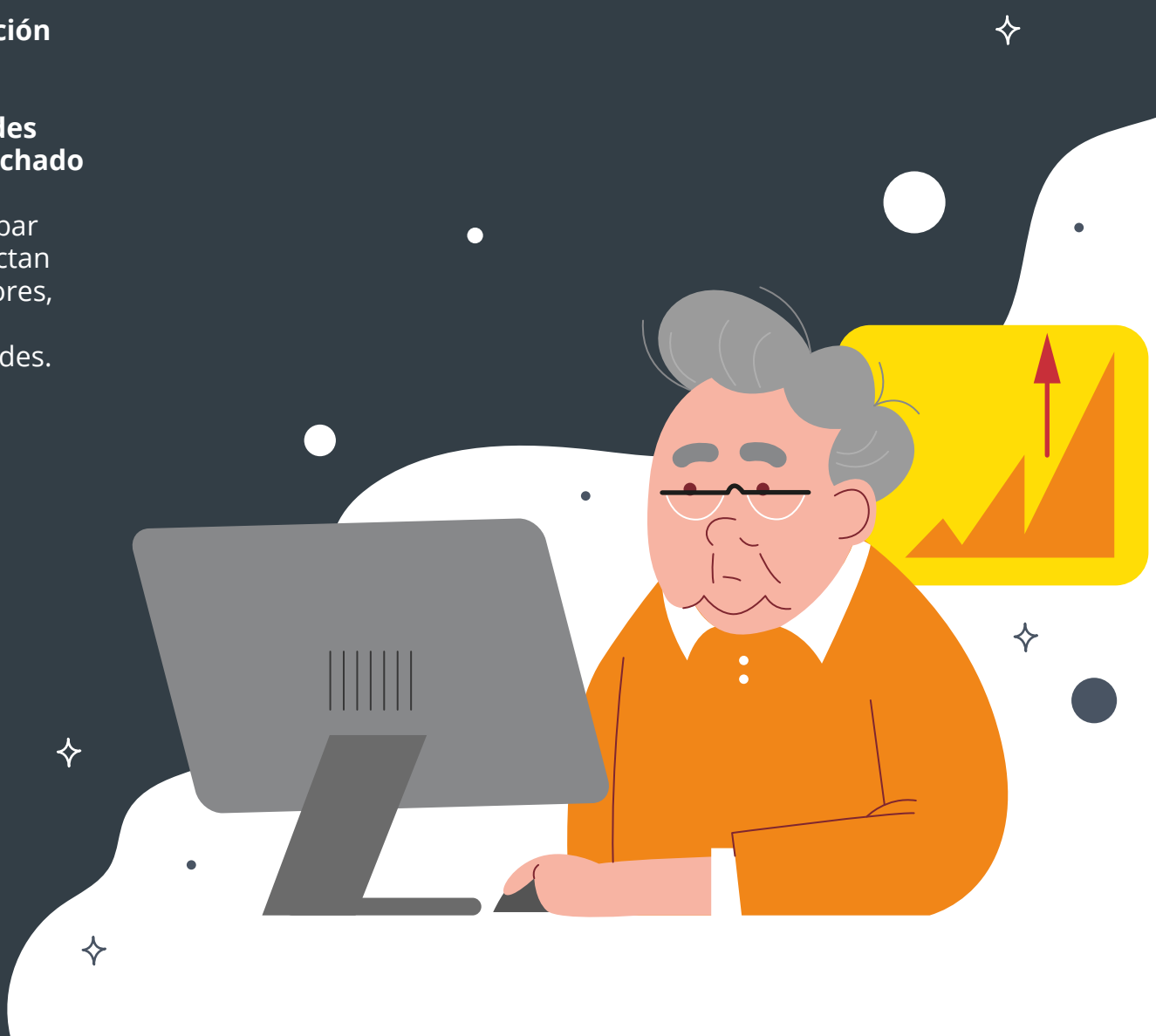
¡Adéntrate para prevenir estos engaños y poder invertir de forma segura!

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Introducción

Hoy en día, invertir por Internet se ha vuelto muy popular, pero también **es el lugar perfecto para los estafadores.** Los fraudes en inversiones *online* **prometen ganancias fáciles y rápidas,** pero su único objetivo **es robar dinero o información personal.**

Las inversiones *online* ofrecen oportunidades reales, pero también son **un espacio aprovechado por los estafadores.** Cada año, miles de personas caen en trampas diseñadas para robar ahorros o datos personales. Estas estafas afectan a todos, pero especialmente a personas mayores, quienes suelen confiar en la buena fe de los demás y desconocen cómo operan estos fraudes.



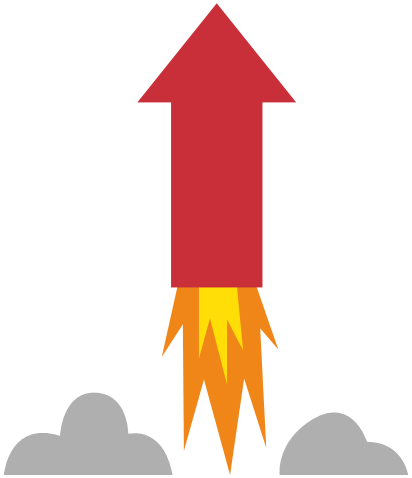
En qué consisten estos fraudes *online?*

Los fraudes financieros *online* son estafas diseñadas para **engañar a las personas** y conseguir su dinero o datos personales. Los estafadores utilizan técnicas sofisticadas para **parecer legítimos y de confianza,** de esa manera presionar a las víctimas para que estas actúen rápidamente sin **pensar demasiado en los riesgos.**

A continuación, te indicamos paso a paso como suelen proceder en estos tipos de fraudes:

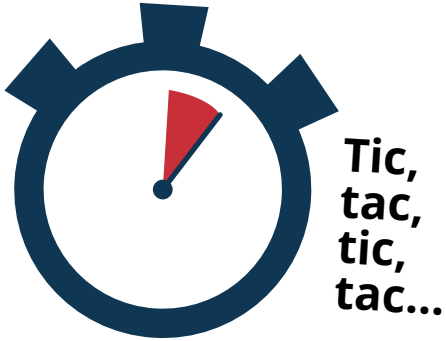
1. Atracción inicial y creación de confianza:

Usan nombres, logotipos y sitios web **que imitan a empresas o instituciones legítimas.** Se presentan como **asesores financieros** o representantes de marcas reconocidas. Además, ofrecen atención personalizada a través de correos electrónicos, llamadas telefónicas o chats.



2. Promesas tentadoras pero irreales:

Garantizan rendimientos altos y rápidos, asegurando que no hay riesgos asociados y muestran **testimonios falsos** de personas que supuestamente obtuvieron beneficios millonarios.



3. Creación de presión y manipulación emocional:

Insisten en que **la oferta es limitada y necesitan una respuesta inmediata.** Algunos estafadores van generando poco a poco una sensación de confianza con la víctima a través de muchas interacciones,**creando una relación antes de solicitar dinero.**

4. Resultados falsos iniciales:

En algunas estafas, **muestran beneficios falsos al principio** para ganarse tu confianza. Por ejemplo, te permitirán retirar pequeñas cantidades de dinero antes de que decidas invertir más.

5. Solicitud de datos personales sensibles:

Piden información personal como números de cuenta bancaria, contraseñas o copias de documentos de identidad. Una vez que tienen estos datos, los usan **para realizar transacciones no autorizadas o cometer otros delitos.**

6. Desaparición repentina o bloqueo:

Después de recibir el dinero o los datos, **los estafadores desaparecen,** cerrando sus sitios web, bloqueando a las víctimas en redes sociales u otros canales de comunicación. Además, pueden optar también por redirigir las consultas a direcciones falsas o números de teléfono inactivos.

El objetivo final es **robar dinero** directamente o **utilizar tu información personal para otros fines o delitos.**

¿Cuáles son los tipos más comunes de fraudes en inversiones *online*?

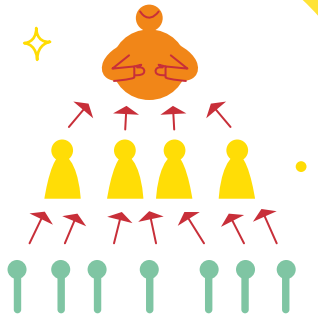
Los principales riesgos que existen a la hora de realizar una **inversión *online*** se pueden manifestar en diversas modalidades, cada una de ellas diseñada para aprovecharse de la confianza y el desconocimiento de los usuarios. A continuación, se plantean los más comunes:

Chiringuitos financieros:

Son entidades no autorizadas que **simulan ser plataformas legítimas de inversión,** utilizando como gancho **páginas web de aspecto profesional y una publicidad atractiva. Prometen rendimientos elevados sin riegos,** operando al margen de la ley. Invertir en ellos conlleva la pérdida del dinero sin posibilidad de recuperarlo, debido a que no cuentan con el respaldo de organismos regulatorios.

Esquemas Ponzi:

Las supuestas "ganancias" que obtienen los primeros inversores en estos esquemas **provienen del dinero que han aportado las personas reclutadas en niveles más bajos.** Tarde o temprano, estos fraudes colapsan al no poder mantener esta estructura fraudulenta, dejando a la mayoría de los inversores con pérdidas significativas.



Fraudes relacionados con criptomonedas:

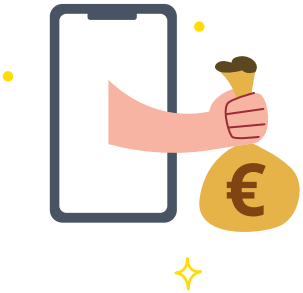
Aprovechando la creciente popularidad de **las monedas digitales,** estos fraudes prometen retornos garantizados poco realistas. Algunos "brokers" operan fuera del marco legal, lo que aumenta el riesgo para los inversores. Además, es común que **supuestos expertos** promocionen nuevas criptomonedas inflando su valor para luego vender grandes cantidades y obtener unos beneficios considerables, dejando a los inversores con pérdidas significativas.

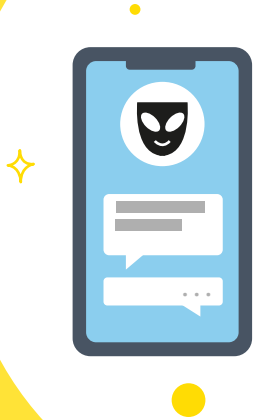
Fraudes relacionados con cuentas de trading y formaciones:

Ofrecen acceso a cuentas de inversión financiadas, pero exigen el pago previo de cursos de formación que muchas veces son inexistentes o no entregan los beneficios prometidos. Este tipo de fraude afecta especialmente a usuarios inexpertos.

Estafas de recuperación *("Recovery Room"):*

Contactan con víctimas de fraudes previos para prometerles recuperar el dinero perdido a cambio de un pago inicial. Se trata de una **segunda estafa** camuflada que aprovecha la vulnerabilidad de quienes buscan una solución rápida.





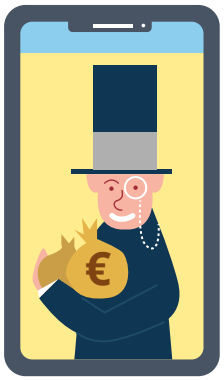
Fraudes en redes sociales:

Debido a su alcance masivo y a la facilidad para crear determinados perfiles. Entre las prácticas más comunes se encuentran los perfiles de **supuestos "influencers financieros",** quienes promueven estrategias o productos de inversión con promesas irreales, muchas veces como parte de esquemas fraudulentos. También destacan los intentos de manipulación de mercados, en los que se difunden **rumores falsos** sobre acciones o productos financieros, generando movimientos en los precios para obtener ganancias ilícitas a expensas de los inversores desprevenidos.

¿Cómo pueden llegar a ti este tipo de estafas?

Este tipo de ciberdelincuentes, utilizan estrategias sofisticadas para **ganarse tu confianza y presionarte** para tomar decisiones impulsivas. Los estafadores se presentan como empresas legítimas o expertos financieros. A menudo utilizan técnicas de ingeniería social para ganarse tu confianza.

Los métodos más habituales que suelen utilizar son:

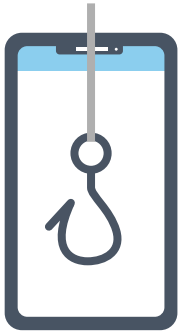


Publicidad engañosa.

Colocan **anuncios atractivos en plataformas** como pueden ser Youtube, Facebook, Instagram o TikTok, **promocionando inversiones con altos rendimientos garantizados.** Estas publicaciones suelen incluir **imágenes de lujo** y testimonios falsos de personas que supuestamente han logrado ganar mucho dinero en poco tiempo. Además, los enlaces en los anuncios redirigen a sitios web fraudulentos que están diseñados para aparentar ser sitios de confianza y profesionales.

Grupos de WhatsApp y mensajes directos.

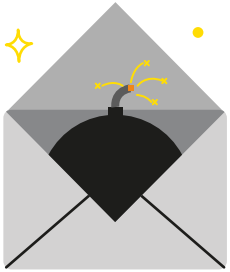
En este caso **envían mensajes a través de aplicaciones** de mensajería instantánea como WhatsApp o Telegram. Estos mensajes incluyen **enlaces a plataformas fraudulentas** de inversión o invitaciones a grupos privados donde se comparten esas supuestas oportunidades de inversión exclusivas. En ocasiones, simulan ser familiares, amigos o compañeros de trabajo para ganarse tu confianza. Dentro de los grupos privados, también hay más cómplices maliciosos que actúan como ganchos, animándo a las víctimas con experiencias ficticias prometedoras.



Llamadas telefónicas.

Los ciberdelincuentes contactan con las víctimas **haciéndose pasar por representantes de bancos,** corredores de bolsa, empresas reconocidas o profesionales del sector. Durante la llamada ofrecen asesoramiento financiero o invitan a invertir en proyectos que se supone que son exclusivos, presionando a las víctimas para que compartan información personal o bancaria.

Correos electrónicos.

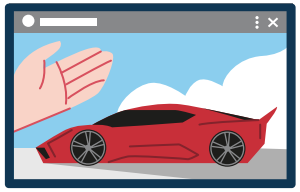


A través de correos electrónicos, envían mensajes que imitan el diseño y el lenguaje que utilizan instituciones financieras legítimas. Estos mensajes suelen contener enlaces para actualizar datos personales o iniciar sesión en cuentas que no son las reales y cuya verdadera intención es capturar los datos personales introducidos por la víctima.

Falsas plataformas y/o aplicaciones móviles de inversión.

Crean páginas web y aplicaciones móviles maliciosas, que simulan ser plataformas legítimas y legales en las que poder realizar inversiones. Estos sitios muestran gráficos falsos y balances inflados para aparentar que el dinero va a crecer con rapidez y facilidad. Sin embargo, cuando la víctima intenta retirar sus ganancias, se les solicita más dinero en forma de comisiones o se les bloquea el acceso.

Redes sociales y falsos *influencers.*



Usan perfiles en redes sociales que se hacen pasar por expertos financieros o personas de gran éxito que han conseguido grandes beneficios con inversiones clave. Suelen publicar vídeos alardeando de sus pertenencias o historias motivadoras donde invitan a los usuarios que lo visualizan a unirse a sus métodos de inversión, prometiendo que pueden conseguir los mismos resultados.

Señales de alerta en inversiones *online*

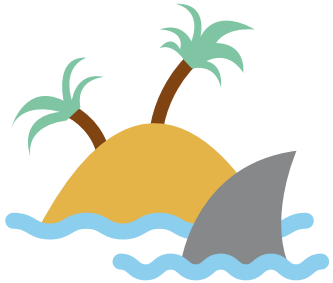
Identificar estas **señales de alerta** que suelen estar presentes en las prácticas más comunes pueden ayudarte a proteger tu dinero y datos personales.
A continuación, te mostramos las más destacables:

1. Promesas de una alta rentabilidad garantizada:

Si te aseguran rendimientos elevados, de forma fácil y sin riesgos, puede ser una clara señal de alerta. Toda inversión legítima implica un nivel de riesgo, y ninguna puede garantizar retornos desproporcionados, especialmente en corto plazo.

2. Presión para tomar decisiones rápidas:

Esto se debe a una falsa sensación que crean para que los usuarios actúen a la mayor brevedad para no **"perder la oportunidad".** De esta forma impiden consultar fuentes confiables o la posibilidad de recapacitar antes de actuar.



3. Entidades no reguladas:

Plataformas de inversión no registradas o ubicadas en **paraísos fiscales** son un riesgo. Si no encuentras información verificable sobre su regulación o están en un país con regulaciones poco claras, lo más prudente es **evitar cualquier transacción.**

4. Uso de lenguaje técnico:

Emplean **términos financieros complejos** para intimidar y confundir a los usuarios menos familiarizados, dando una **falsa sensación de credibilidad y conocimientos en el sector.**

5. Contactos no solicitados que te dirigen a sitios web sospechosos:

Recibir **ofertas de inversión inesperadas** a través de diferentes medios, como correo electrónico, redes sociales, WhatsApp u otros. Estas propuestas suelen **incluir enlaces** que redirigen a páginas fraudulentas, las cuales pueden presentar características sospechosas, como diseño poco profesional, URLs similares a las de plataformas legítimas o ausencia de medidas de seguridad, como puede ser el candado HTTPS en la barra de direcciones.

Precauciones para protegerte

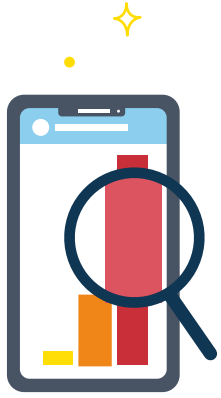
Para evitar caer en este tipo de estafas, **protégete siguiendo estas recomendaciones:**

No compartas datos personales o bancarios.

Proteger tu información personal es muy importante para evitar el robo de identidad o el acceso no autorizado a tus cuentas bancarias. **Nunca compartas datos** como tu número de cuenta, documentos de identidad, contraseñas o información bancaria con personas o empresas que no hayas verificado como de confianza. **También debes evitar hacer clic en enlaces no solicitados,** especialmente si te piden que introduzcas datos en páginas sospechosas. **Configurar alertas bancarias** en tu cuenta puede ayudarte a detectar movimientos no autorizados rápidamente y tomar medidas antes de que se produzcan daños mayores.

Busca opiniones de otros usuarios.

Si nadie conoce la página o tiene malas críticas, no confíes. Las experiencias de otras personas pueden ofrecerte una perspectiva valiosa sobre la fiabilidad de una plataforma de inversión. **Investiga en foros, redes sociales y sitios de reseñas** para conocer las opiniones de usuarios previos. Sin embargo, es importante tener cuidado, ya que los estafadores a menudo **generan comentarios falsos** o publican reseñas positivas en sus propias páginas web. Si no encuentras información suficiente sobre la empresa, o si encuentras críticas negativas consistentes, es una señal clara de que debes desconfiar y buscar alternativas más seguras.



Investiga antes de invertir.

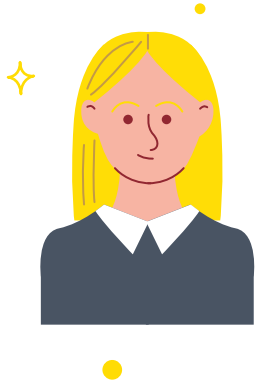
Antes de realizar cualquier inversión, es importante **que verifiques la legitimidad de la empresa o la plataforma** que deseas utilizar para hacer tus inversiones. **Consulta si está registrada en la Comisión Nacional del Mercado de Valores (CNMV)** o en entidades similares.
Además, también existen listas de advertencias donde se publican las entidades sospechosas o no autorizadas.

Evita actuar por presión.

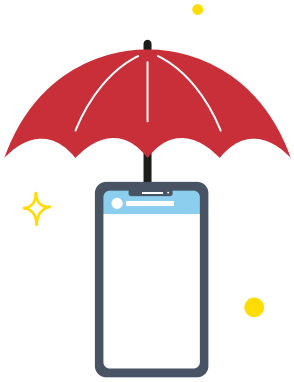
Los estafadores suelen utilizar **tácticas de presión para que tomes decisiones rápidas sin reflexionar.** Esto incluye mensajes o llamadas insistentes que te empujan a invertir con urgencia, bajo pretextos como ofertas limitadas o promociones exclusivas. **Es fundamental detenerte y evaluar** la situación con calma antes de comprometer tu dinero. Las oportunidades legítimas no desaparecen de la noche a la mañana, por lo que no hay necesidad de apresurarte. Si sientes que alguien está insistiendo demasiado, **es mejor desconfiar y cortar el contacto.**

Consulta con expertos.

Si tienes dudas sobre la legitimidad de una inversión, **es recomendable buscar asesoramiento profesional.** Puedes contactar con un organismo oficial como **CNMV para recibir orientación gratuita** y objetiva a través de su sitio web. También puedes hablar con un **asesor financiero de confianza** que tenga credenciales que puedas verificar. No te fíes exclusivamente de personas que se presentan como expertos sin pruebas claras de su fiabilidad. Obtener diferentes opiniones te permitirá tener una visión más clara y tomar decisiones fundamentadas.



Usa dispositivos seguros.



La seguridad de tus dispositivos es una parte importante **para protegerte de posibles fraudes.** Asegúrate de **mantener actualizado el sistema operativo,** los navegadores y aplicaciones de seguridad, como pueden ser **antivirus o *firewall* de tus dispositivos.** Además, utiliza conexiones seguras, **evitando las redes Wi-Fi públicas** para realizar operaciones financieras.
Instalar un antivirus y configurar contraseñas fuertes para tus cuentas son medidas adicionales que refuerzan la protección. También es recomendable **activar el doble factor de autenticación (2FA)** o la autenticación multifactor (MFA) si es posible, en tus cuentas para evitar accesos no autorizados.

Desconfía de ganancias garantizadas.

En el mundo de las inversiones, ninguna oportunidad legítima puede garantizar ganancias, ya que todas conllevan riesgos. **Si una plataforma asegura resultados garantizados y sin esfuerzo,** como duplicar tu dinero en pocos días o semanas, **es muy probable que se trate de un fraude.** También debes desconfiar ante términos como "sin riesgos" u "oportunidad única", ya que son tácticas diseñadas para captar tu atención y crear falsas expectativas.

¿Qué puedes hacer si crees que ya has sido víctima?

Si sospechas que **has caído en un fraude financiero *online* debes actuar de forma inmediata** para minimizar los daños y así proteger tu información personal y bancaria. Te detallamos los pasos clave que debes seguir:

- **Corta la comunicación con el estafador y reúne todas las evidencias:**
  Deja de interactuar de inmediato con la persona o entidad sospechosa para evitar mayores daños. A continuación, **recopila toda la información** relacionada con el fraude, como capturas de pantalla, correos electrónicos, mensajes y enlaces. **Estos documentos serán clave para presentar una denuncia.**

- **Notifica a tu entidad bancaria:**
  Informa a tu banco sobre el incidente para que tomen medidas preventivas, como **bloquear tarjetas asociadas, detener transferencias o vigilar posibles movimientos sospechosos en tus cuentas.** También debes revisar regularmente el estado de tus cuentas en busca de movimientos no autorizados.

- **Denuncia el fraude:**
  Ponte en contacto con **las Fuerzas y Cuerpos de Seguridad del Estado y presenta una denuncia.** Ellos te guiarán para que puedas formalizar la denuncia y proporcionar toda la documentación necesaria. Además, te pondrán en contacto con la CNMV para que adviertan a otros usuarios.

- **Aumenta tu concienciación y conocimientos en inversiones *online***
  Para futuras inversiones, **dedica tiempo a investigar** sobre la empresa o plataforma que hay detrás y verifica que esté registrada en organismos oficiales. Participa en actividades educativas ofrecidas por instituciones confiables. Esto no solo te ayudará a tomar decisiones más informadas, sino que también reducirá la probabilidad de caer en futuros fraudes financieros.

Conclusión

Invertir *online* ofrece grandes oportunidades, pero también conlleva **riesgos significativos.** El conocimiento y la prudencia son tus mejores aliados para evitar fraudes y proteger tus fondos. Asegúrate de realizar una investigación exhaustiva, utilizar plataformas legítimas y tomar decisiones basadas en información confiable. **En caso de duda, siempre es preferible consultar con un profesional** para garantizar que tus inversiones sean seguras y rentables a largo plazo.

Para más información escanea el código:

O sigue este enlace:

https://www.incibe.es/ciudadania.