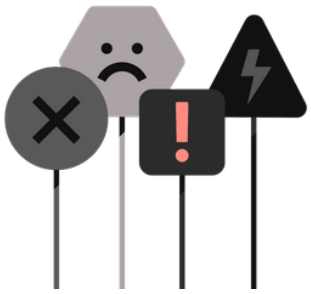
AI Investment Scams

Helping investors protect their assets

From deepfakes to fake trading platforms, scammers are using artificial intelligence to craft convincing investment traps. Learn how to spot the red flags and protect your hard-earned money.

Signs of an AI investment scam

- **A public figure promoting an investment opportunity**
- **Unusual lip or body movements in videos**
- **Unexpected phone calls or messages**
- **Strange phrasing**
- **Inability to meet in person**
- **Fake websites**



Fraud warning signs

1. **High return, no risk - guaranteed**
2. **Fear of missing out (FOMO)**
3. **The trust trap**
4. **Pressure to buy**
5. **Questions not answered**

Arizona Corporation Commission - Securities Division
azcc.gov/securities

NASAA

AI-Related Investment Scam

Arizona Corporation Commission - Securities Division
azcc.gov/securities

Scam:
Imitating a person (family or friend) in a call or in a message

What can you do:

- Have a code word between family and friends. Check with caller to see if they know the code word to verify if the caller is the person that they say they are.
- Put the caller on hold and text a person you trust to verify if the crisis they are sharing is true.
- Don't answer calls from unknown numbers. If a call is answered from an unknown number the scammer may now know to target that number
- Change your voicemail to not include your name or voice. Change it to the telephone carrier automated voicemail message. Don't give scammers your name or voice to use later.
- Check if your social media is public or private. The caller may be using information they found on your public social media. Consider making your social media private.
- Reverse image search the image or picture they sent. If the picture is attached to other profiles or names, then it may be a scam.
- Don't click on the links or websites sent to you. Hover over the link to check for any grammar/ spelling mistakes, or different web address.

Verify an investment opportunity or report a financial scam to the ACC Securities Division - Investigator on Duty by calling 602-542-0662 or emailing at SecuritiesDiv@azcc.gov.

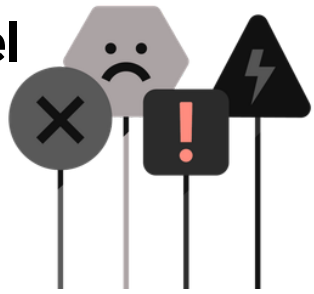
Estafas de inversión que utilizan la inteligencia artificial

Ayudamos a los inversores a proteger sus bienes

Desde los deepfakes hasta las plataformas de trading falsas, los estafadores están utilizando la inteligencia artificial para crear trampas de inversión muy convincentes. Aprende a detectar las señales de alerta y a proteger el dinero que tanto te ha costado ganar.

Señales de una estafa de inversión que utiliza la inteligencia artificial

- **Una figura pública que promociona una oportunidad de inversión**
- **Movimientos extraños de los labios o del cuerpo en los vídeos**
- **Llamadas o mensajes inesperados**
- **Expresiones extrañas**
- **No poder reunirse en persona**
- **Sitios web falsos**



Señales de alerta de fraude

1. **Alta ganancia, sin riesgo - garantizado**
2. **Miedo a perderse algo (FOMO)**
3. **La trampa de la confianza**
4. **La presión para comprar**
5. **Preguntas sin respuesta**

Arizona Corporation Commission - Securities Division
azcc.gov/securities

NASAA

Estafa de inversión relacionada con la inteligencia artificial

Arizona Corporation Commission - Securities Division
azcc.gov/securities

Estafa: Hacerse pasar por otra persona (un familiar o un amigo) en una llamada o en un mensaje

¿Qué puede hacer?:

- Acuerda una palabra clave con tus familiares y amistades. Pregunta a la persona que llama si conoce la palabra clave para comprobar que es quien dice ser.
- Pon a la persona que llama en espera y envía un mensaje de texto a alguien de confianza para verificar si la situación de emergencia que te está contando es cierta.
- No contestes llamadas de números desconocidos. Si contestas una llamada de un número desconocido, el estafador podría saber que debe dirigirse a ese número.
- Cambia tu buzón de voz para que no incluya tu nombre ni tu voz. Cámbialo por el mensaje automático de la compañía telefónica. No des a los estafadores tu nombre ni tu voz para que los utilicen más adelante.
- Comprueba si tus perfiles en redes sociales son públicos o privados. Es posible que la persona que te llama esté utilizando información que ha encontrado en tus perfiles públicos. Considera la posibilidad de cambiar tus perfiles a privados.
- Realiza una búsqueda inversa de la imagen o foto que te han enviado. Si la imagen aparece asociada a otros perfiles o nombres, es posible que se trate de una estafa.
- No hagas clic en los enlaces ni en los sitios web que te envíen. Pasa el cursor por encima del enlace para comprobar si hay errores gramaticales o ortográficos, o si la dirección web es diferente.

Verifique una oportunidad de inversión o reporta una estafa financiera a la División de Valores de la ACC —investigador de guardia— llamando al 602-542-0662 o enviando un correo electrónico a SecuritiesDiv@azcc.gov.