

# FMFCU's SECURITY NEWSLETTER



ALERTS | EDUCATION | PREVENTION

## STAY ONE STEP AHEAD OF ARTIFICIAL INTELLIGENCE

As artificial intelligence (AI) continues to evolve and become more powerful, we want to ensure members stay educated on the threats it can have with financial fraud and identity theft.



## GENERATIVE AI VOICE CLONING SCAMS

**Generative AI** is appealing to scammers because it enables creating more personalized and convincing scams. For example, scammers can create voice clones to impersonate a trusted individual or organization. A short audio clip of a person's voice is all that is needed to sound just like that person on the other line.

### Key Signs of the Scam

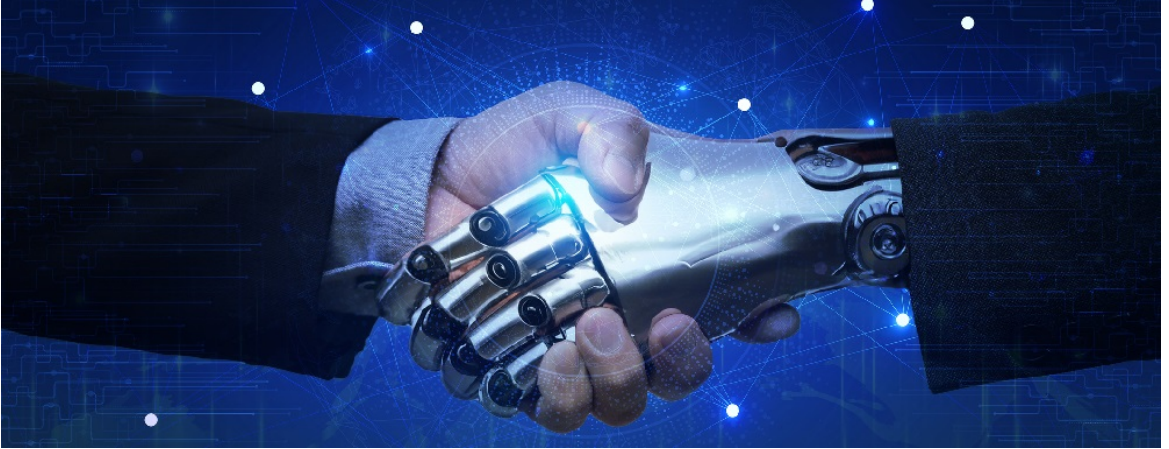
- Unexpected or out of the blue
- Pressure to act immediately
- An offer too good to be true
- Urgent requests for money by wire transfer, gift card, pay app, or crypto
- Requests sensitive, personal, or financial information

## Protect Yourself

- **Create a secret word or phrase with your family to verify their identity**
- Don't trust the voice
- Hang up and call the person from a number you know is theirs
- Do not trust caller ID, as it can be faked
- Be cautious with what you post on the internet – just 3 seconds is enough to replicate one's voice

[Learn More](#)

## AVOID BECOMING THE TARGET OF AI INVESTMENT SCAMS



Investment fraud happens when scammers try tricking you into investing money, and now are using AI – both the term and the technology – to do so.

### Be on the Lookout

- Platforms that claim to trade crypto on behalf of investors
- Claims to use AI to generate positive returns
- Promises high returns with little risks

### Protect Yourself

- Avoid investments you don't understand
- Be wary of promoted investment opportunities on online platforms
- Do not give in to pyramid schemes

[Learn More](#)

**Stay up-to-date with  
the latest information in  
FMFCU's Security Center**

[More Info](#)

[Open an Account](#) | [Apply for a Loan](#) | [Current Rates](#)  
[Visit a Branch](#) | [Digital Banking](#)