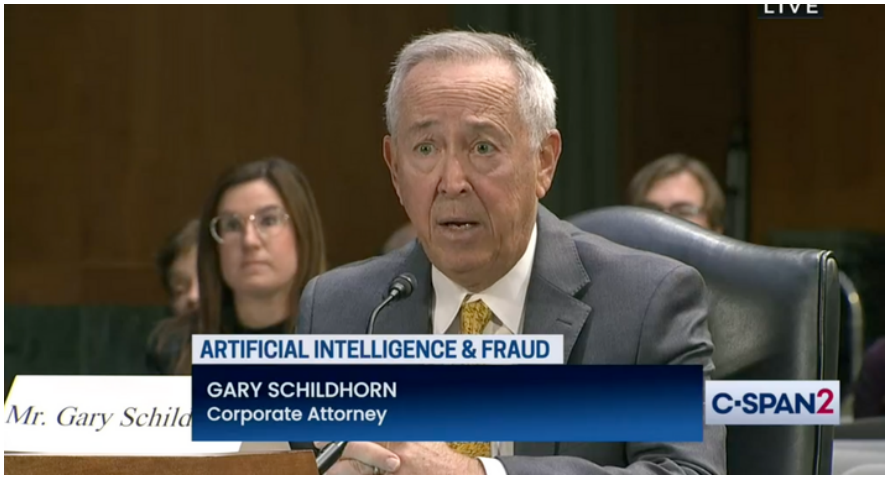
November 19, 2023

“There was no doubt in my mind that it was his voice on the phone — it was the exact cadence with which he speaks”



AI Scam

What’s been reported?

<u>According to Fox News:</u>

Gary Schildhorn, a Philadelphia-based attorney and another targeted victim of an AI voice clone scam. He almost sent $9,000 to the scammer until he confirmed with his daughter-in-law it was an extortion attempt.

The scammer, posing as an attorney, called Schildhorn requesting funds to bail his son out of jail for causing a car accident and failing a breathalyzer test.

"There was no doubt in my mind that it was his voice on the phone — it was the exact cadence with which he speaks," he said. **"I sat motionless in my car just trying to process these events. How did they get my son’s voice? The only conclusion I can come up with is that they used artificial intelligence, or AI, to clone his voice… it is manifestly apparent that this technology… provide[s] a riskless avenue for fraudsters to prey on us."**

Since no money was sent, however, law enforcement told Schildhorn that no crime had been committed and no further action was taken.

©Senior Shield 2023

November 19, 2023

In-Depth Scam Analysis

- *How These Scams Work:*
  - ***AI Voice Cloning:*** *Scammers use sophisticated AI technology to clone the voices of loved ones. This technology can create highly realistic voice replicas with just a few seconds of recorded audio. (maybe taken from social media)*
  - ***Emotional Manipulation:*** *The scammers create scenarios where the fake family member seems to be in urgent need, often claiming they are in legal trouble or danger.*
  - ***Urgency and Secrecy:*** *They press for quick action and often insist on keeping the matter secret, which prevents the victim from seeking advice or verification from others.*

- *Why They Are Effective:*
  - ***Realistic Voices:*** *The cloned voices are convincingly real, leading victims to believe they are genuinely talking to a family member.*
  - ***Trust Exploitation:*** *The elderly often have a deep sense of trust and a willingness to help their family members, making them more susceptible to these scams.*
  - ***Lack of Awareness:*** *Many seniors are not aware of AI voice cloning technology and its capabilities, leaving them unprepared for such scams.*

Protection Strategies:

Actionable Strategies:

1. ***Verify Independently:*** *Always verify the situation by contacting the family member or friend through a different phone number or communication method.*
2. ***Education on Technology:*** *Stay informed about new AI technologies and common scam tactics.*
3. ***Family Protocols:*** *Establish a family code word or question that can be used to verify a family member's identity in urgent situations.*
4. ***Limit Personal Information Online:*** *Be cautious about sharing personal information, especially voice recordings, on social media or other public platforms.*

November 19, 2023

Expert Insights

Emerging Trends and Preventive Measures:

- ***Ongoing Evolution:*** *Experts note that AI technology is rapidly evolving, leading to more sophisticated scams.*
- ***Importance of Reporting:*** *Reporting these scams to authorities can help in tracking trends and developing countermeasures.*
- ***Building a Support Network:*** *Seniors should have a trusted network of family, friends, and professionals they can consult when they suspect a scam.*
- ***Using Technology Wisely:*** *Implementing tools like caller ID, spam filters, and consulting with tech-savvy family members can provide additional layers of protection.*

Take Action

1. *Contact Your Senators and Representatives:*
    - *Express Concerns: Reach out to your local senators and representatives to express your concerns about AI-powered scams targeting seniors. Personal stories, like the incident involving Gary Schildhorn, can be particularly impactful.*
    - *Request Legislative Action: Urge them to support or introduce legislation that increases protection against these scams and funds educational programs about AI technology for seniors.*
    - *Follow Legislative Developments: Stay informed about any bills or actions being taken at the state and federal levels regarding AI scams.*
2. *File Reports with Relevant Authorities:*
    - *Federal Trade Commission (FTC): Report any instances of AI scams to the FTC. This helps them track scam trends and take action where possible.*
    - *Local Law Enforcement: Inform your local police if you or someone you know falls victim to such scams. They can provide immediate assistance and advice.*
3. *Utilize Resources:*
    - *Follow Senior Shield's Facebook Page*
    - *Public Libraries and Senior Centers: Use these community hubs for disseminating information and resources on scam prevention.*

©Senior Shield 2023