

---

## Protecting Yourself from AI Scam Calls

### Summary

In the era of artificial intelligence (AI), AI-powered scam calls have become increasingly sophisticated, making it more challenging to distinguish between genuine and fraudulent communication. These scams range from simple requests for personal information to elaborate schemes involving deepfake audio of loved ones. Protecting yourself from these AI-driven deceptions requires a blend of vigilance, awareness, and the use of technology. Here's how you can safeguard your privacy and financial security from these threats.

### Recognize the Red Flags

AI scam calls often follow certain patterns or scripts. Be wary of calls that:

- ▶ Pressure you to make immediate decisions or payments.
- ▶ Ask for personal information, such as social security numbers, bank account details, or passwords.
- ▶ Claim you've won a prize, owe money, or face legal action without any prior notification.
- ▶ Use generic greetings like "Dear customer" instead of your name.

### Hang Up and Call Back

If you receive a call from someone claiming to be from a legitimate organization but suspect it might be a scam, hang up immediately. Find the official contact number from the organization's official website, or your physical documents and call back. Legitimate entities will understand your concern for security.

### Be Wary of Emotional Tactics

Whether it's a social engineering scam or an AI phone call, scammers can build your trust in them and create a sense of urgency to find your weak points. Be wary of any engagement where you have a heightened sense of emotion or feel under duress. Take a moment to stop and think about the situation and don't act on impulse.

### Be Cautious of Caller ID

Scammers can spoof phone numbers, making it appear as if the call is coming from a trusted, local number, or even from a government agency. Always be skeptical of the caller ID, as it's not a reliable verification method for the caller's identity and remember that it's very easy to mimic any voice these days. Scammers use AI tools to manipulate your outgoing voicemail greeting to copy and use your voice for scams.

### Don't Engage in Conversation

Engaging in conversation with a scammer can lead to more targeted attempts. If you answer a call and it starts to seem suspicious, it's best to hang up without providing any information or confirming any details they might guess.

### Create a Secret Safe Word

Come up with a safe word that only you and your loved ones know about, that you can ask for over the phone. You can also create a phrase with your loved ones that they could use to prove who you are if in a duress situation. Calling back though or verifying via another means of communication is best but a safe word can be very helpful for young ones or elderly relatives who might be difficult to contact otherwise.

As AI technology continues to evolve, so too will the methods employed by scammers. Staying informed, being cautious and proactive are key strategies to protect yourself from falling victim to AI scam calls. Remember, it's always better to err on the side of caution and verify the authenticity of any unsolicited communication.

---