Protecting Yourself from AI Scams

How to Identify, Avoid, and Report AI-Powered Fraud

WOLFGANG CAPITAL

WEDNESDAY WISDOM | MAY 6, 2026

COMMON AI SCAM TACTICS

- **Deep fake voice cloning:** Scammers can replicate a family member's voice—your "son" or "parent" may call asking for emergency money, but it's not really them
- **Deep fake videos:** Celebrities or people you follow appear to endorse investments or products—these videos are AI-generated and completely fake
- **AI phishing emails and texts:** Messages that look legitimate from trusted companies (banks, Apple, the IRS) asking you to click a link or provide information
- **Fake investment websites:** Temporary sites showing amazing returns, designed to collect your information before disappearing
- **Romance scams:** AI chatbots on dating apps build fake relationships, eventually asking for money or investment help

RED FLAGS TO WATCH FOR

- **Urgency and pressure:** "Act now," "immediate action required," or threats of consequences
- **Unusual payment methods:** Requests for gift cards, wire transfers, or cryptocurrency
- **Too good to be true:** Promises of high returns with zero risk
- **Requests for secrecy:** "Don't tell your family" or "keep this between us"
- **Visual glitches in videos:** Extra fingers, strange eye movements, lips slightly out of sync—AI isn't perfect yet
- **Suspicious email addresses:** Always click on the sender's name to reveal the actual email address behind it

VERIFYING LEGITIMATE COMMUNICATIONS

- **When in doubt, hang up:** If someone calls claiming to be from a company or government agency, hang up and call them back at their official number
- **Go directly to the source:** Don't click links in emails—go to the company's website directly by typing the address yourself
- **Check the email address:** Double-click on sender names to see the actual email—if it's not from an official domain, it's spam
- **Remember:** The IRS, police, and government agencies typically contact you by mail—not phone, email, or text

Protecting Your Family

- **Create a family safe word:** A secret word only your family knows—if someone calls claiming to be a relative, ask for the safe word
- **Have open conversations:** Talk with elderly parents and family members about these scams without judgment
- **Don't shame victims:** People who've been scammed are often emotionally hurt—let them know they're the victim, not the one at fault
- **Help less tech-savvy family members:** If they won't learn the technology, help them set up protections yourself

ESSENTIAL TAKEAWAYS

- ✓ **When in doubt, hang up**—then verify by calling the official number yourself
- ✓ Create a **family safe word** to verify identity during suspicious calls
- ✓ Use **authenticator apps** instead of text message codes for 2FA
- ✓ **Freeze your credit** at all three bureaus
- ✓ Don't click links in emails—go to websites **directly**
- ✓ Government agencies contact you by **mail**, not phone or email
- ✓ **Update software** on all devices immediately when available
- ✓ Avoid writing **paper checks**—use digital payment methods
- ✓ Use a **password manager** for strong, unique passwords

> **Action Item:** This week, enable two-factor authentication on your most important accounts and freeze your credit at all three bureaus.

TWO-FACTOR AUTHENTICATION

- Enable 2FA on all important accounts—banks, email, financial accounts
- **Authenticator apps are best:** Google Authenticator or Microsoft Authenticator are more secure than text message codes
- Authenticator apps generate new codes every 30-60 seconds, making them nearly impossible to intercept

FREEZE YOUR CREDIT

- Freeze your credit at all three bureaus: **Experian, Equifax, and TransUnion**
- This prevents anyone from opening loans or credit cards in your name
- Temporarily unfreeze when you need to apply for credit, then freeze again

ADDITIONAL BEST PRACTICES

- **Update your software:** Install updates on phones and computers as soon as they're available—they patch security vulnerabilities
- **Use a password manager:** Generates and stores complex, unique passwords so you don't have to remember them
- **Avoid paper checks:** Checks contain your name, address, routing number, and account number—use Zelle or Venmo instead
- **Set up account alerts:** Enable notifications for credit card transactions so you're aware of any suspicious activity
- **Be cautious with links:** Never click links in unexpected emails—one click can install software that tracks everything you type

IF YOU'VE BEEN TARGETED

- **Stop all contact** with the scammer immediately
- **Contact your bank** and freeze affected accounts
- **Freeze your credit** at all three bureaus
- **Report the scam:** File a report at **IC3.gov** or call **1-833-FRAUD-11**
- Reporting helps authorities track patterns and may protect others, even if recovery is unlikely

951.200.5084 | INFO@WOLFGANGC.COM | WWW.WOLFGANGC.COM