Workplace Shield™

AI Fraud Prevention Training

Duration: 15-20 minutes
Format: Interactive presentation with examples

SLIDE 1: Learning Objectives

By the end of this training, you will be able to:

- Identify common AI-powered fraud tactics
- Recognize red flags in suspicious communications
- Apply verification procedures before taking action
- Report potential fraud through proper channels
- Protect yourself and the organization from AI scams

Instructor Note: Emphasize that AI fraud is rapidly evolving and affects everyone, from entry-level employees to executives. This is not about technical skills but awareness.

SLIDE 2: What is AI Fraud?

Definition:

Criminals using artificial intelligence to create highly convincing scams

Common AI Fraud Types:

- Voice Cloning - Mimicking voices of family members or executives
- Deepfake Videos - Fake video calls that look completely real
- AI Phishing - Perfect emails with no grammatical errors
- Synthetic Documents - Fake IDs and official documents

Why It's Different:

Traditional fraud had obvious signs (poor grammar, suspicious links)

AI fraud is nearly perfect and extremely difficult to detect visually

Instructor Note: Show real examples if available. Emphasize that these scams fool even security-conscious individuals because they exploit trust, not technical vulnerabilities.

SLIDE 3: Real Examples & Red F

Case Study 1: Voice Clone Emergency

Employee received call from 'daughter' in distress needing bail money

Voice was perfect, but urgency and secrecy were red flags

Case Study 2: CEO Deepfake Video

Finance team received video call from 'CEO' authorizing wire transfer

Video looked real, but request bypassed normal approval process

Universal Red Flags:

✓ Extreme urgency or pressure to act immediately

✓ Requests to bypass normal verification procedures

✓ Demands for secrecy or confidentiality

✓ Unusual payment methods or destinations

✓ Emotional manipulation or fear tactics

Instructor Note: Encourage discussion. Ask if anyone has experienced similar situations.

SLIDE 4-5: Action & Resources

What To Do If You Suspect AI Fraud:

1. STOP - Do not take any action requested
2. VERIFY - Contact the person through a different channel
3. REPORT - Notify IT Security immediately
4. DOCUMENT - Save all evidence (emails, recordings, screenshots

Available Resources:

- Workplace Shield™ portal with fraud alerts
- 24/7 IT Security hotline: security@[company].com
- Quick reference cards at your desk
- Monthly security awareness updates
- StopAiFraud.com for latest threat intelligence

Your Vigilance Protects Everyone

Instructor Note: End with Q&A. Reinforce that reporting suspected fraud is always the right action, even if it turns out to be legitimate. Better safe than sorry.