IDENTITY THEFT TODAY

How to Spot Scams Before They Spot You

October 15, 2025
12pm - 1pm

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and items discussed on the October 15, 2025 session of **Identity Theft Today: How to Spot Scams Before They Spot You**

SESSION TOPICS

AI-Powered Scams | Detection Challenges | Romance Scams | Deepfakes | Social Media Bots
Phishing Evolution | Red Flags | Protection Strategies | Misinformation

Click Here to Access Recorded Session ⟶

AI'S IMPACT

- AI transforms scams into sophisticated tools executing multiple fraud layers with alarming efficiency
- Traditional red flags like grammar errors disappear as AI perfects language
- Detection increasingly difficult—AI creates realistic deepfakes, voice clones, and convincing phishing emails

SCAM TYPES

Romance Scams

- AI manages multiple conversations simultaneously, maintaining illusion of genuine connection
- Enables cross-language scamming; face-swapping allows video call impersonation
- "Pig butchering" slowly builds trust before shifting to investment fraud

Deepfake Scams

- Creates lifelike videos/audio using machine learning algorithms
- Example: Hong Kong clerk defrauded of $25M via fake executive video call

Social Media Bots

- Create realistic profiles with personal details, photos, and genuine-seeming activity
- Spread fake news and propaganda, especially during elections

Phishing Evolution

- AI eliminates grammar errors, creating legitimate-appearing emails
- Conversational phishing: AI chatbots continue exchanges before sending malicious payloads
- Bypasses traditional filters by avoiding obvious threats in initial messages

RED FLAGS

- **Urgency/pressure:** Demands for immediate action are suspicious
- **Identity verification:** Always confirm who's contacting you via independent channels
- **Emotional manipulation:** Exploiting fear, love, or greed to rush decisions
- **Too good to be true:** Lottery wins, unknown inheritances are typically scams
- **Sensitive info requests:** Legitimate institutions never ask for passwords/SSN via email/text
- **Unsolicited contact:** Unexpected messages should trigger verification

PROTECTION STRATEGIES

- Strong authentication: Use unique passwords; enable two-factor/multi-factor authentication
- Password managers: Generate and store unique passwords in encrypted vaults
- Verification habits: Always verify through independent channels
- Privacy management: Limit online information sharing—scammers use this data
- Technology updates: Keep systems current to fix security vulnerabilities
- AI detection tools: Use AI-based scam detection and email filters
- Credit freeze: Freeze credit through bureaus to prevent new account fraud

SPOTTING AI CONTENT

Images/Videos

- Look for anomalies: extra fingers, unusual eye reflections, overly smooth skin
- Check lighting/shadows for inconsistencies
- Watch for mismatched audio/video, lip sync issues
- Examine backgrounds for repeating patterns
- Zoom to find digital artifacts (pixelation, strange colors)

Audio

- Listen for unnatural pacing, odd pauses, mechanical intonation
- Note flat or forced emotional delivery
- Check if background noise feels authentic or looped

Text Messages

- Watch for repetitive/generic language without substance
- Note lack of personal/contextual details
- Trust instincts—if something feels off, investigate

MISINFORMATION CONCERNS

- AI creates fake images/text hard to distinguish from truth
- Bad actors mass-produce propaganda on social media
- AI-generated fakes now as common as Photoshop manipulations
- Always cross-check with credible, independent sources

VICTIM RESPONSE STEPS

1. **Stop contact:** Cease communication, block scammers on all platforms
2. **Secure finances:** Contact bank immediately to stop transactions
3. **Change passwords:** Update all affected account credentials
4. **Report:** File with FTC or IC3 to help track patterns
5. **Document:** Keep detailed records for investigations
6. **Notify law enforcement:** Contact police for significant losses

KEY TAKEAWAYS

1. AI makes scams more sophisticated and harder to detect than ever
2. Traditional red flags may no longer apply—language is now flawless
3. Always verify by reversing communication direction
4. Stay informed—identity theft constantly evolves
5. Report scams to protect others and identify trends
6. Anyone can be targeted regardless of age or intelligence

Q&A HIGHLIGHTS

1. What resources exist for someone who may have fallen victim to a Bitcoin romance scam?

A: This is difficult due to emotional manipulation. Resources include National Cybersecurity Alliance's "Then and Now" program (thenandnow.info) for older adults and caretakers. Let victims know you're available and discuss red flags—Bitcoin/crypto with online dating is a major warning sign. Rally trusted family members for conversations. AARP's Fraud Watch helpline (available to all ages) and Identity Theft Resource Center provide additional support.

Q&A HIGHLIGHTS

2. What tips help identify fake job scams requesting personal information?
A: Verify companies directly through official websites, not provided contact info. Contact HR using independently found information. Watch for too-good-to-be-true offers. Be wary of checks sent for equipment (often fake, even via FedEx). Never provide SSN until thoroughly verified. If the company and position exist, contact them directly to confirm the posting's legitimacy.

3. How can we verify a class action payout email's legitimacy?
A: Go to the company's website—they typically have class action sections. Use their "Contact Us" page for direct verification. Class action notices include law office contact info—call to verify. Check sites like classaction.org for legitimate suits. Never click email links; navigate independently to official sources.

4. What AI detection tools are recommended?
A: Several tools are available through searches. Grammarly has AI detection. Others include originality.ai and GPT0. These tools have different expertise areas—review capabilities before choosing. They analyze text, images, or audio to identify AI generation patterns.

5. What should you do if your cell phone is stolen?
A: Immediately visit your carrier (T-Mobile, Verizon, AT&T) to lock the phone. Change passwords for all logged-in accounts—banking, email, social media. If logged into accounts on the stolen device, change passwords from another device immediately. File a police report if needed. Act quickly to minimize access opportunity.

ABOUT OUR SPEAKERS:

SEWIT ESTIPHANOS | IRIS IDENTITY PROTECTION

Resolution Specialist with 8+ years in IRIS's Resolution and Consultation Specialist Department, certified in Fukura.

EUGENE NAKOUYE | IRIS POWERED BY GENERALI

Operations Manager for IRIS Resolution Center with 12 years' experience. Liaison between clients, account managers, and agents ensuring white glove identity protection service.

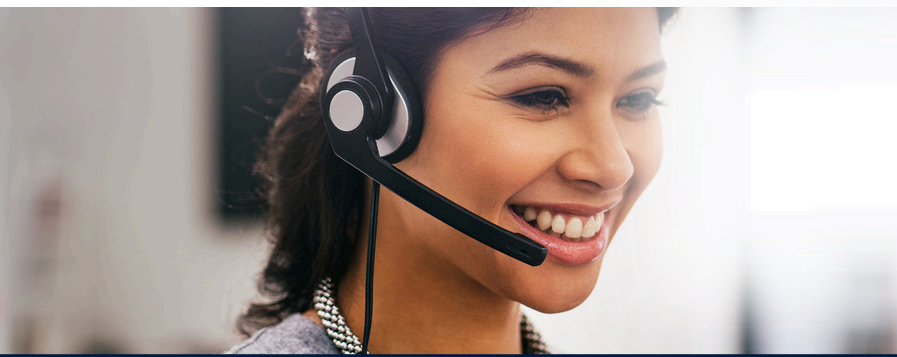
JENNIFER COOK | NATIONAL CYBERSECURITY ALLIANCE

Senior Director of Marketing at nonprofit creating free cybersecurity educational resources and campaigns including Cybersecurity Awareness Month, covering data privacy, job scams, and online safety.

SAHARA SEARS | LEGAL RESOURCES

Session moderator from Legal Resources, a legal plan and identity theft plan provider offering affordable attorney access and comprehensive identity protection services.

DISCLAIMER: This summary highlights key webinar points and questions. For comprehensive details, view the full seminar at **LRSeminars.com.**



Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com