IDENTITY THEFT TODAY

Trending Threats

February 19, 2025
12pm - 1pm

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and items discussed on the February 19, 2025 session of **Identity Theft Today: Trending Threats.**

SESSION TOPICS

Fraud | Identity Theft | SIM Swapping | Scam

Click Here to Access Recorded Session ⟶

What were the top five Identity Theft Cases for 2024?

- Personal Information Compromised
- Credit Card Fraud
- Bank Fraud
- Scam Victim
- Lost/Stolen Items

Top Causes of Identity Theft Incidents

- **Phishing Attacks:** Fraudulent communications stealing personal information, data, money, or installing malware.
- **Ransomware Attacks:** Evolved to include threats of leaking stolen sensitive information for extortion.
- Synthetic Identity Theft: Combining real information (SSNs) with fake details to create hard-to-detect fraudulent identities.
- **Credential Stuffing:** Using stolen credentials from data breaches to access multiple platforms, exploiting password reuse.
- **Mobile-Related Attacks:** Targeting mobile vulnerabilities, especially SIM swapping, where criminals transfer phone numbers to access accounts.

Tips to Protect Your Data

- Use strong, unique passwords with a password vault. Create complex passwords with a mix of numbers, symbols, and upper/lowercase letters.
- Enable two-factor authentication (2FA) on all important accounts, especially financial and email services.
- Be cautious about suspicious links and attachments in emails, even if they appear to come from known contacts.
- Monitor credit reports regularly from all three major bureaus (Experian, Equifax, TransUnion) for unauthorized accounts or inquiries.
- Limit the sharing of personal information online and adjust privacy settings on social media accounts.
- Keep software and devices updated with the latest security patches to protect against known vulnerabilities.

- Consider identity protection services that provide real-time monitoring and alerts for suspicious activity.
- Freeze your credit reports when not actively applying for new credit.

Coming Up Next Month

Tackling Title Theft and Fraud

March 19, 2025
12pm - 1pm

Register at www.LRseminars.com

How to Protect Yourself from SIM Swapping

- Set up a PIN/password with your phone provider
- Use biometrics for added security
- Monitor accounts for unusual activity
- Secure financial accounts with freezes when necessary
- Contact your carrier immediately if suspicious activity occurs

Trending Scams of 2024

- **AI Voice Cloning Scams:** Using AI to mimic familiar voices for emergency money requests. Criminals can now create convincingly realistic voice replicas with just a small audio sample, often collected from social media posts or public speaking engagements. These scammers typically create urgent scenarios claiming to be in danger, arrested, or in a hospital to pressure victims into immediate action.
  - *Protection:* Verify identity with personal questions or call back known numbers. Establish a "safe word" with family members for emergency situations.
- **Fake Job Offers:** Exploiting remote work trends with fraudulent listings requiring upfront payments.
  - *Protection:* Research companies thoroughly and avoid upfront payments.
- **Subscription Renewal Scams:** Fake notices urging updates to payment details on fraudulent sites.
  - *Protection:* Access accounts directly through official websites, not email links.
- **Cryptocurrency Investment Scams:** False promises of guaranteed returns.
  - *Protection:* Use only reputable institutions and be skeptical of guaranteed returns.
- **Online Marketplace Scams:** Requesting deposits for items then disappearing.
  - *Protection:* Meet in public places and use platforms with buyer protection.
- **Romance Scams:** Building false relationships to request money.
  - *Signs:* Rapid professions of love, money requests, minimal online presence.
  - *Protection:* Verify identities and limit personal information sharing.
- **Charity Scams:** Fake donation requests.
  - *Protection:* Verify through trusted sources before donating.
- **Grandparent Scams:** Impersonating relatives to request emergency funds.
  - *Protection:* Verify identity and contact relatives through known numbers.
- **Government Impersonation Scams:** Threats of legal action unless payment is made.
  - *Protection:* Verify by contacting agencies directly through official channels.

2025 Expectations: Deepfakes and Biometric Fraud

Deepfake technology threatens authentication systems with convincing fake audio, video, and biometric data. As AI technology becomes more accessible, security experts anticipate a significant rise in sophisticated identity fraud attempts. These attacks will increasingly target facial recognition, voice authentication, and other biometric security measures that were once considered highly secure. Organizations and individuals will need to adapt quickly to this evolving threat landscape.

Protection Strategies

- **Multi-Factor Authentication:** Multiple verification methods for layered security, combining something you know (password), something you have (device), and something you are (biometrics).
- **Liveness Detection:** Identifying real humans through subtle movements like eye blinking, micro-expressions, and natural head movements that are difficult for current deepfake technology to simulate convincingly.
- **Risk Management:** Continuous monitoring, real-time fraud detection using machine learning algorithms that adapt to new threat patterns, and regular security protocol updates to address evolving threats.
- **Encryption and Secure Communication:** Using end-to-end encryption for sensitive communications to prevent unauthorized access to information that could be used for deepfake creation.

Key Attendee Questions

Q: What if you lose your phone while traveling and can't access password-protected accounts?

A: Use another device to access websites, select "forgot password," verify identity with security questions, reset passwords, and secure accounts.

Q: Can SIM swapping occur without your knowledge?

A: Yes. Setting a PIN with your carrier is the best prevention.

Resources

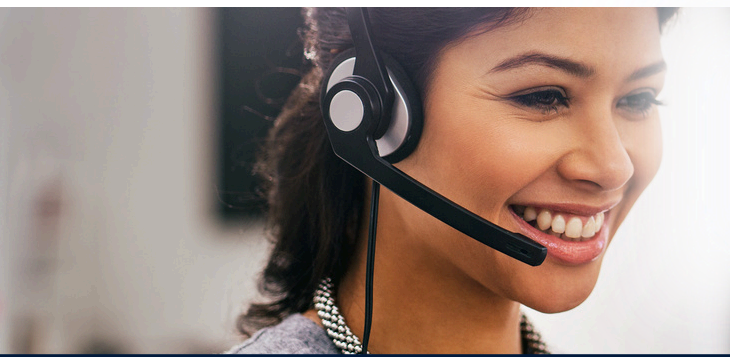
- Federal Trade Commission: **https://www.ftc.gov**
- Identity Theft Resource: **https://identitytheft.gov**
- Credit Reports: **https://www.AnnualCreditReport.com**
- Report Fraud: **https://reportfraud.ftc.gov**

ABOUT OUR SPEAKER:

SIDICK TRAORE GLOBAL SERVICE DELIVERY

Sidick Traore currently serves as Vice President of Global Service Delivery, Global Identity & Cyber Protection at Iris Powered by Generali. Sidick has also held the position of Manager at Europ Assistance USA from March 2012 to January 2022 and possesses extensive experience as an Engineman in the US Navy since July 2015, graduating top of the class. Academic qualifications include a Bachelor of Applied Science in Actuarial Science from Towson University and an Associate of Arts in Business Administration from Montgomery College.

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