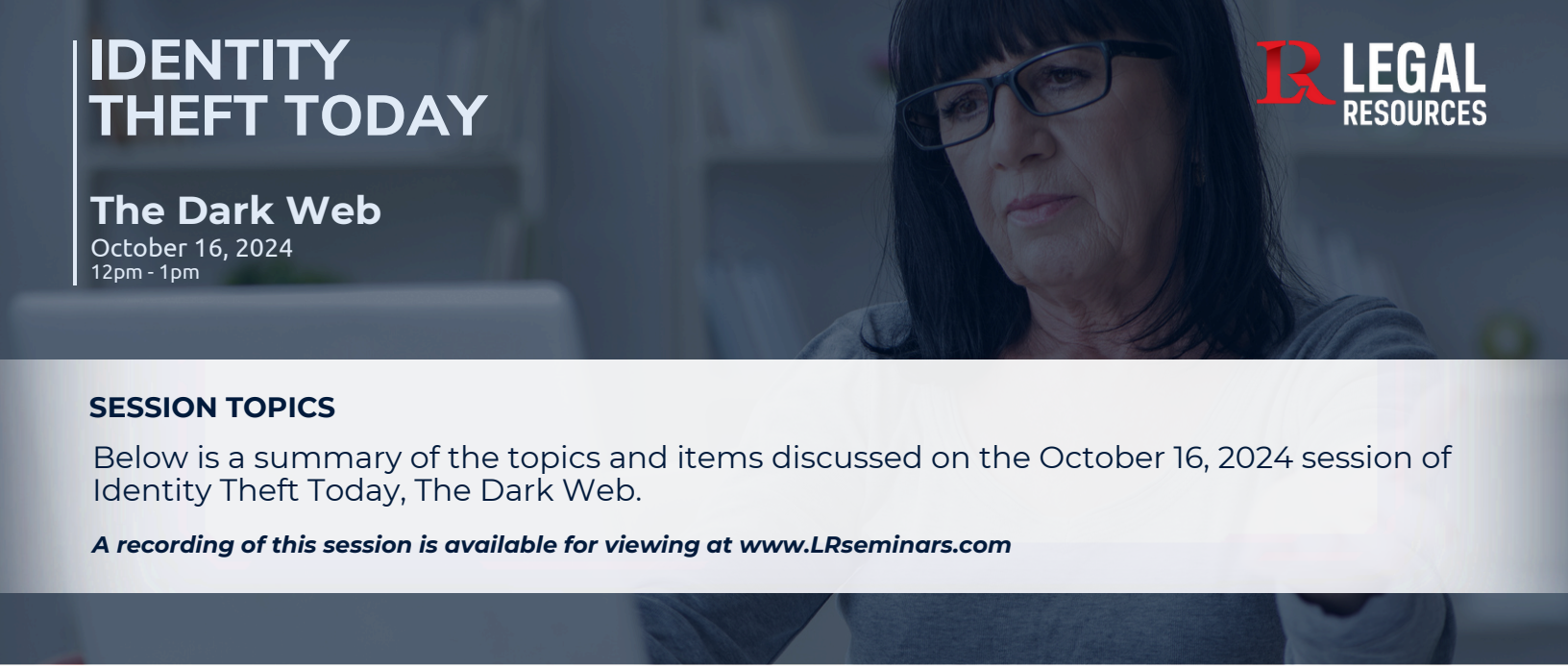


IDENTITY THEFT TODAY

The Dark Web

October 16, 2024
12pm - 1pm

LEGAL RESOURCES

SESSION TOPICS

Below is a summary of the topics and items discussed on the October 16, 2024 session of Identity Theft Today, The Dark Web.

A recording of this session is available for viewing at www.LRseminars.com

SESSION TOPICS

- Dark Web
- Phishing
- Identity Theft
- Credit Freeze
- MFA

What is the Dark Web and how is it different from the Surface Web and Deep Web?

The Dark Web is a small part of the Deep Web (about 6%) that requires specific software (like Tor) to access. It's often associated with anonymity and illicit activity such as selling personal data or illegal goods. The Surface Web includes publicly accessible sites like Google or Amazon, while the Deep Web contains content not indexed by search engines, like academic databases or corporate intranets.

What steps can you take if your identity is breached?

1. **Check your credit report** for unusual activity.
2. **Freeze your credit** with all three bureaus to prevent new accounts.
3. **Add multi-factor authentication** to sensitive accounts.
4. **Monitor your financial statements** closely for fraud.

How do phishing scams work, and how can you recognize them?

Phishing scams often arrive via email and trick users into providing sensitive information. Key warning signs include emails with urgency ("act now"), unfamiliar or misspelled domain names, grammatical errors, and requests for personal information.

What is the importance of monitoring the Dark Web for stolen information?

Monitoring the Dark Web helps identify if your personal information, such as social security numbers or email addresses, is being sold or used illegally. This gives you a chance to act before major damage occurs.

Coming Up Next Month

Final ITT for the Year

Thankful for ID Theft Resources

November 20, 2024
12pm - 1pm
Register at www.LRseminars.com

What protective software should you consider using to safeguard your personal information?

- Antivirus software to protect against malware.
- VPN (Virtual Private Network) to secure your internet connection in public spaces.
- Anti-phishing software to identify suspicious sites before you enter them.

What is a credit freeze, and how does it differ from a fraud alert?

A credit freeze completely restricts access to your credit report, preventing new credit from being opened in your name. A fraud alert asks creditors to verify your identity before opening new accounts but doesn't block access to your credit.

TIPS FOR STAYING SAFE:

- **Use multi-factor authentication** on important accounts.
- **Freeze your credit** if you suspect or experience a breach.
- **Monitor your accounts regularly** for any signs of unauthorized activity.
- **Avoid public Wi-Fi** without using a VPN.
- **Be cautious of unexpected emails** that ask for personal information.

ABOUT OUR SPEAKER:

MICHELE KRISANDA

SENIOR VICE PRESIDENT, GLOBAL CYBER & IDENTITY PROTECTION PRODUCT MANAGEMENT

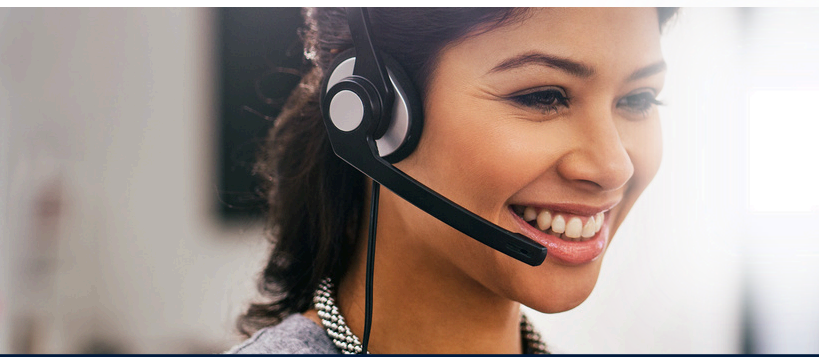
Iris Powered by Generali

Michele Krisanda holds the position of SVP Global Cyber & Identity Protection Product Management at Iris, Powered by Generali where she's worked the last 10 years.

The Iris product and design team is responsible for understanding consumer and client needs, and the evolving identity threat landscape, and working closely with Iris teams to create the best consumer solutions.

Education:

- MBA, University of Virginia Darden; BA, University of Virginia



Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com