



National Cyber Security Awareness Month WebEX presentations

Lunch and Learns:

October 3-7, 2016 – Every Day Steps Towards Online Safety with Stop.Think.Connect

Cybersecurity is present in every aspect of our lives, whether it be at home, work, school, or on the go. Regardless of one's technical ability or background, there are simple steps everyone can take to be more cyber secure in their digital lives. Week 1 kicks off NCSAM 2016 and reinforces basic tips for everyone to be safer online, including more secure accounts through stronger authentication and keeping security updates current.

[LUNCH AND LEARN SESSION "Online safety with STOP.THINK.CONNECT" \(click to launch webex on demand\)](#)

October 10-14, 2016 – Cyber from the Break Room to the Board Room

We are all part of protecting personal and organizational data in the workplace. From CEO to incoming entry-level employee, each organization's cybersecurity posture is reliant on a shared level of vigilance and awareness. Week 2 looks at how every employee can promote a culture of cybersecurity at work.

[LUNCH AND LEARN SESSION "From the break room to the board room" \(click to launch webex download\)](#)

October 17-21, 2016 – Recognizing and Combating Cybercrime

As technology advances, the impact of cybercrime is becoming more costly and frequent. Law enforcement, government, industry, and individual citizens all play a vital role in mitigating adverse impact to our schools, communities, and personal well-being. Incidents ensue through every day 'phishing' emails masked behind trusted sources, in infected websites that unknowingly capture personal information when entered, and as persuasive links that lock files until a ransom is paid. Week 3 focuses on the signs of criminal intent through technology and what individuals can do to detect and prevent cybercrime.

[LUNCH AND LEARN SESSION "Combating Cybercrime" \(click to launch webex on demand\)](#)

October 24-28, 2016 – Our Continuously Connected Lives: What's Your 'App'-titude?

With compounding growth of connected technologies – cars, household appliances, finances, healthcare, and more being increasingly managed by smart devices – we are confronted with the need for increased awareness to secure cutting-edge, technical innovations. Week 4 looks to the future and discusses how cybersecurity is being built into advanced technology along with areas of opportunity for individuals to operate securely in a digital society.

i. On 10/27/16 @12:30pm lunch and learn WebEx Training on "App-titude"

October 31, 2016 –Building Resilience in Critical Infrastructure

The linkage between cyber and physical security is essential to the resiliency of critical infrastructure at both the local and national level. Resilience of essential systems and assets, from power grids to banking systems, is vital to our national security, economy, and public health and safety. Week 5 looks at the sustainment of the Nation's critical infrastructure, and facilitates the transition to November's Critical Infrastructure Security and Resilience Month (CISR).

NCSAM Guest Speakers:

Thursday, October 20 @2pm. [CLICK HERE FOR WEBEX PLAYBACK](#)



Robert Leong is Director of Product Management with McAfee Labs/Intel Security and will be talking about what *greyware* is and why it's a challenge.

- What greyware is and why is it a challenge for security operations
- Which identification techniques can be leveraged to discover adversarial activity
- How to contain and remediate greyware at the endpoint
- How to fight greyware with local and global threat intelligence enabling smart, automated decisions
- How the state's investment in Intel/McAfee Security Solutions will help fight greyware.

As technology advances, the impact of cybercrime is becoming more costly and frequent. Law enforcement, government, industry, and individual citizens all play a vital role in mitigating adverse impact to our schools, communities, and personal well-being. Incidents ensue through every day 'phishing' emails masked behind trusted sources, in infected websites that unknowingly capture personal information when entered, and as persuasive links that lock files until a ransom is paid. Week 3 focuses on the signs of criminal intent through technology and what individuals can do to detect and prevent cybercrime.

- i. On 10/20/16 @12:30pm lunch and learn WebEx Training on "CyberCrime"
- ii. On demand streaming/download of this video is here.