BLACK TALON SECURITY

CALIFORNIA ASSOCIATION of ORAL & MAXILLOFACIAL SURGEONS

Safeguarding the Modern Practice:

A 3-Part Cyber Series for OMS Practices

EARN 3 CEUs

Cyber threats targeting healthcare practices have grown more sophisticated, more frequent, and harder to spot. This three-part series, presented in partnership with the CALAOMS and the security experts at Black Talon Security, gives practice owners and administrators a clear, practical roadmap for protecting their organizations against cyber criminals and data breaches.

Across three focused sessions, you will learn how attackers exploit human trust, how artificial intelligence has changed the speed and scale of attacks, and how unmanaged "Shadow AI" can quietly expose your patient data. Each session breaks down complex topics into plain language and actionable steps you can apply right away. You will walk away with practical policies, helpful tools, and a stronger understanding of where your risks really live. Whether you manage one location or many, this series will help you build a more resilient, security-aware practice.

Part 1:
PREVENTING SOCIAL ENGINEERING—The Exploitation of Human Trust

Wednesday, August 5, 6-7 p.m. PT

People are often the easiest way into a practice, and attackers know it. This session offers a non-technical look at how the cyber threat landscape has evolved, including the criminal groups actively targeting the broader dental industry.

- Understand who today's cyber criminals are and how the threat landscape has changed over time
- Recognize the most common social engineering tactics used against practices
- Identify practical policies, procedures, and tools you can put in place to lower your risk

Part 2:
STAYING AHEAD OF CYBER ATTACKS—Finding and Fixing Weak Spots Before Criminals Do

Wednesday, August 12, 6-7 p.m. PT

Every practice has weak spots in its systems, and criminals are getting faster at finding and breaking through them. This session explains in plain terms how artificial intelligence has made attackers quicker and more dangerous, shrinking the time you have to react.

- Explain how artificial intelligence has made cyber criminals faster and more dangerous
- Understand why the time between a problem being found and an attack is shrinking
- Describe why ongoing, all-the-time security works better than a periodic assessment

Part 3:
KEEPING YOUR PRACTICE PROTECTED FROM SHADOW AI

Wednesday, August 19, 6-7 p.m. PT

AI tools can boost productivity, but unapproved use can quietly put your patient data at risk. This session defines "Shadow AI" and explains the specific dangers it poses to oral surgery practices.

- Define Shadow AI and understand the risks unapproved AI tools create
- Explain how poor data organization increases your exposure when using AI
- Develop policies that support safe and responsible AI adoption in your practice

Register for the webinar series at calaoms.org/events

Presented by

Kelton Earl
Cyber Risk Specialist
Black Talon Security, LLC

Kelton brings his blend of psychological & technical expertise to the world of cybersecurity. While studying Industrial Organizational Psychology at Eastern Washington University, Kelton began his professional career in Veterinary Medicine.

After graduation, Kelton transitioned into the IT world, working for a managed service provider in Spokane, Washington. Growing into Account Management, he quickly found a passion for building successful client relationships within primarily healthcare, dental and nonprofit organizations.

Now as a Cybersecurity Risk Specialist at Black Talon Security, Kelton applies his passion for people & technology to empower business leaders with everything they need to make confident, informed decisions around their cybersecurity.