Name

Build a Security Awareness Program your Employees will Love

Date

Tuesday, June 4, 2019

Time

8:00 AM - 12:00 PM

Session Description:

Many organizations have security awareness programs, but are they looking at the emotional intelligence behind their design? Employees will not pay attention to traditional messaging and once a year Death by PowerPoint training. So, what should you do? How do you make your employees love security? How do you measure success and articulate challenges to management? You'll soon learn to shift your focus on getting employees to become your best defense and give them the tools they need to succeed.

Section 1: Introduction to Security Awareness Psychology

Security awareness starts with understanding the basics principals behind psychology and human behavior. We have to go above and beyond to make security stick and we need to have positive messaging. Changing the way we communicate information to our employees is the key to success. Marketing and advertising principals will be highlighted along with understanding metrics that matter to powerful security awareness program.

Section 2: Building Your Plan

You can't be successful in your security awareness program without a plan. We will walk through how to build your ambassador program, security awareness roadmap, and provide detailed information on how to successfully launch a phishing simulation program. Demonstrations of detailed phishing simulation tests and how to approach the ongoing exercise of phishing prevention training. We will also cover the story behind the click and how to approach employees that need extra help to defend against social engineering attacks. We will review the following guides:

- Security Awareness Program Assessment
- Security Awareness Ambassador Program
- Phishing Simulation Best Practices
- Phishing Lessons Learned
- Phishing Recovery Questions
- Metrics for Executives

Section 3: Case Study and Best Practices

Time to put all of our new knowledge to use. We will review case studies that will require thinking outside the box and being creative. The group will challenge historically predictable approaches to solving these problems! Best practices from successful security awareness programs will be discussed as well. Your new perspective will give you the insight, tools, and motivation to start making a change in your own security awareness and phishing simulation program.

Speaker

Nick Santora - Curricula

Speaker Bio(s)

Nick Santora founded Curricula after a 7-year career at the North American Electric Reliability Corporation (NERC), the enforcement agency responsible for regulating the power grid across North America. Nick spend time advocating and advising critical infrastructure utilities on how to improve their cyber security programs. Nick is internationally recognized as a cyber security expert and speaks regularly at security conferences across North America on the psychology behind influencing employees within security awareness programs.

Nick holds a Bachelor of Science and Master of Business Administration from Rider University. He also earned his CISSP (Certified Information Systems Security Professional) and CISA (Certified Information Systems Auditor). Nick also serves on the board of advisors for Veracity, and industrial control systems SDN company.

Visit Curricula at https://www.getcurricula.com