Cisco Secure Awareness Training

Flexibility and Support
Cisco Secure Awareness Training, formerly Cisco Security Awareness, provides flexibility and support to effectively deploy your phishing simulations, awareness training – or both – and measure and report results. Empower your security operations team with the ability to focus on real-time threats and not end user mitigation. Our product provides the education that helps employees to work smarter and safer.

High-quality content is central to any security awareness program and a pre-requisite to provide a training experience that is fun, compelling and relevant. Our content is developed by a team of experts using a proven pedagogical approach and methodology for adult learning that ensures the highest degree of engagement. Your users will learn about cyber security in a way that expands user knowledge and increases their affinity for your organization to help protect it.

Key Reasons To Invest in Cisco Secure Awareness Training
• People influence security more than technology or policy and cybercriminals know how to exploit human behaviors.
• No security system can be 100% effective in detecting all incoming threats. Increasing security awareness plays a critical role in an organization’s overall security and risk posture.
• Security and risk management leaders (SRM) should invest in tools that increase awareness and influence behavior that supports security business objectives through computer-based training.
• SRMs leaders must understand the diversity of people in an organization and approach security awareness training with personalization.

Reap the Benefits
Partner with a security awareness expert and leverage domain expertise including CISO coaching to develop your security awareness strategy:
• Analyze your organization’s security awareness needs and set strategic objectives
• Plan your awareness program including phishing simulation, awareness training, communication and reinforcement plan
• Optimize program performance by setting and measuring against strategic metrics and KPIs

© 2020 Cisco and/or its affiliates. All rights reserved.
Key Trends in Security Awareness Training That Are Driving Long-Term Behavioral Change

High Quality Content: Security training cannot effectively be approached with a “one-size-fits-all” approach. Content that varies in format and length promotes better participation and retention rates.

Intuitive Phishing Simulator: Out of the box phishing scenarios that reflect real-life cyber and phishing threats are integrated with training for just in time feedback.

Multilingual Content and Platform: Out-of-the-box language support (narration and text) support global security awareness programs.

Communications and Reinforcement Materials: Large libraries of predesigned content and templates for internal campaign promotion and content reinforcement; including videos, posters and newsletters.

Consultative Approach: Our approach incorporates unique offerings including CISO coaching, managed services and content customization.

Hackers attack every 39 seconds and on average 2,244 times a day*

- Over 3.4 billion email scams or phishing emails are sent every day. This adds up to one trillion email scams per year
- Data breaches exposed 4.1 Billion records in the first half of 2019 (RiskBased)
- 62% of businesses experienced phishing and social engineering attacks in 2018 (Cybint Solutions)
- 52% of breaches featured hacking, 28% involved malware and 32-33% included phishing or social engineering, respectively. (Verizon)

Learn more: cisco.com/go/emailsecurity

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. 2216435 09/21