Computer Networking Virtual Learning

Network Security - 3.5 - Social Engineering

May 7, 2020

Lesson: 5/7/2020

Objective/Learning Target:

- Identify and ignore email hoaxes to protect system resources.
- Train users to identify phishing scams.

Focus Questions

- How is passive social engineering different from active social engineering?
- What methods do attackers use to make an interaction appear legitimate?
- How is employee awareness training the most effective countermeasure for social engineering?
- What specific countermeasures should be implemented to mitigate social engineering?
- How is tailgating different from piggybacking?
- What is a watering hole attack?

Learning Tasks

- Navigate to TestOut.com & log on using your credentials
- Navigate to Security Pro Chapter 3 - Policies, Procedures, & Awareness, Section 5 - Social Engineering
- Review Vocabulary words for 3.5 before starting into Section
- Read Fact Sheets located in sections 3.5.3
- Watch videos located in sections 3.5.1, 3.5.2, 3.5.4
- Complete Lab Simulation located in section 3.5.5
- Answer/Review Practice Questions located in section 3.5.6

Time Breakdown

Videos = 25 Minutes
Fact Sheets = 5 minutes
Lab Simulation = 5
Practice Questions = 15 minutes
Total Time = 50 minutes

Reference: TestOut Security Pro Lesson Plan Document