COURSE SYLLABUS

Phishing and Social Engineering Defense (Self-Paced)

Spot and stop social engineering on every channel attackers use: email, text, voice, QR code, and the front door. Built to satisfy the federal annual security awareness requirement.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/phishing-and-social-engineering-defense-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Federal Policy Foundations

Understand the chain from FISMA through OMB policy, NIST standards, and agency implementation to individual awareness, including roles and accountability.

Anatomy of a Phishing Attack

Examine phishing, spear phishing, whaling, and business email compromise; the attacker playbook from reconnaissance to monetization; and the lures used against federal employees.

Social Engineering Beyond Email

Review smishing, vishing including AI-generated voice, quishing, pretexting, tailgating, badge cloning, USB baiting, social media reconnaissance, and insider threat overlap.

Recognize, Resist, Report

Apply the verification checklist, out-of-band verification methods, reporting paths and timelines, and protections for good-faith reporting.

Self-Paced Workshop: Phishing Triage

Evaluate six to eight realistic artifacts as legitimate or suspicious using an instant-feedback answer key.

Defense in Depth

Explore phishing-resistant multifactor authentication using PIV/CAC and FIDO2, Zero Trust context, Rules of Behavior, and everyday cybersecurity hygiene.