COURSE SYLLABUS

Mobile Device Security & Secure Telework: Work Anywhere, Secure Everywhere Course

A half day live on mobile and telework security written for the device user, not the administrator — phishing-resistant authentication, MFA abuse, home networks, and what to do when something goes wrong.

> 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/mobile-device-security-and-secure-telework

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

Course Outline

Module 1

- Security Beyond the Office: Mobile & Telework Foundations
- Defining mobile device security, telework, remote access and bring-your-own-device
- Government-furnished versus personally owned versus third-party-managed devices
- How telework moves the security boundary
- What the learner is personally responsible for
- Obligations under the telework agreement and rules of behavior

Module 2

- The Device Is an Endpoint: Mobile Device Security
- Malicious apps, smishing, spyware and untrusted accessories
- Screen lock, biometrics, automatic locking and device encryption
- What mobile device management enforces, verifies and can wipe
- Prompt updates and limiting permissions, sideloading and unapproved cloud or AI apps
- Protecting data on devices being lost, transferred, repaired or retired

Module 3

- Connect with Confidence: Secure Remote Access
- Approved methods including VPN, virtual desktop and zero trust network access
- Verifying encryption and responding to certificate and captive-portal warnings
- Phishing-resistant authentication with PIV, derived credentials and passkeys
- Refusing unexpected authentication prompts and recognizing push bombing and one-time-code theft

- Assessing public, hotel, shared and home networks

Module 4

- Home Is Part of the Attack Surface: Secure Telework Practices
- Securing the home router through default credentials, updates and current wireless encryption
- Separating work from personal accounts, personal devices and smart-home equipment
- Recognizing phishing, smishing, QR-code lures and voice or video impersonation
- Protecting information from unauthorized viewing, printing, storage and sharing
- Physical and privacy practices in shared, public and travel settings

Module 5

- Lost, Stolen, Compromised: Monitoring & Response
- Indicators of a compromised device or account including unexpected access alerts
- What compliance checks, logging and monitoring actually detect on a managed device
- Reporting within required timeframes
- Remote lock, wipe and credential revocation and their effect on personal data
- Recovery steps through credential changes, re-enrollment and return to service