Course Outline:

Social Engineering Deceptions and Defenses *(Course T852)*

**What is this course about?**
In this course, you gain the skills to defend against social engineering attacks that threaten organizational security. You learn the technical and psychological methods of manipulation, misrepresentation and persuasion used by social engineers. Further, this course incorporates hands-on activities designed to understand the motivations and methods used by social engineers, to better protect your organization and prevent data breaches.

Social engineering, in very broad terms, is manipulating people to achieve information, and covers many areas, including spying, running a con game and organizational espionage. A 2011 study from the Ponemon Institute found that 30% of organizational security breaches have been completely or significantly aided by social engineering. These types of attacks can include mining for information prior to an attack, sending phishing or spear phishing e-mails, spoofing websites and baiting. This course will help organizations safeguard their data, prevent unwanted access and avert Denial of Service (DoS) attacks.

**Who should attend?**
This course is valuable for site security personnel, network security personnel, project managers and anyone who wants to learn defenses against social engineering attacks.

No prior technical background is required.

**Duration:**
3 Days

**This course qualifies for:**
1.8 CEUs
17 NASBA CPEs

**Chapter 1: Introduction to Social Engineering**
- Social Engineering
- Case Studies
- Tools and Techniques of Social Engineers
- Exploring the Virtual Machines

**Chapter 2: Gathering Information**
- Goals of Information Gathering
- Gathering On-site Information
- Dumpster Diving and Linking
- Online Information Sources
- Reconnaissance Countermeasures
Chapter 3: Understanding the Communication Model
- Communication Models
- Exploiting Communication Weaknesses
- Securing Communications

Chapter 4: Gaining Physical Access
- Physical Security
- Physical Access Controls
- Cracking a Safe
- Detection Sensors
- Casing the Joint
- Physical Countermeasures

Chapter 5: Eliciting Information
- Developing Rapport
- Elicitation Tactics and Goals
- Setting Up Elicitation
- Halting Information Loss

Chapter 6: Impersonation
- In-Person Impersonation
- Remote Impersonation
- Deceiving Authentication Systems
- Indirect Impersonation
- Impersonation Countermeasures

Chapter 7: The Psychology of Persuasion
- Pretexting and Manipulating Behavior
- Mindlessness
- Social Proof and Authority
- Resisting Persuasion

Chapter 8: Countermeasures
- Assessing Vulnerability
- Legal and Social Concerns
- Inspecting a Penetration Test Report
- Developing Policies
- Building Awareness

Chapter 9: Course Summary