

## **Combating Social Engineering Course Summary**

### **Description**

Social engineering is the name given to a category of security attacks in which someone manipulates others into revealing information that can be used to steal, data, access to systems, access to cellular phones, money or even your own identity. Such attacks can be very simple or very complex. Gaining access to information over the phone or through web sites that you visit has added a new dimension to the role of the social engineer. During seminar we will examine ways in which people, government agencies, military organizations and companies have been duped into given information that has opened them to attack. We will look at the low-tech as well as the newer forms of electronic theft. The attendees will participate in exercises that reinforce the concepts discussed. Once we have identified the issues related to social engineering, we will examine methods that organizations and individuals can use to combat social engineering. Because the dual issue of identity theft is so closely linked to social engineering, we will examine current concerns and issues related to this increasingly important topic.

### **Objectives**

At the end of this course, students will be able to:

- Understand common types of social engineering
- Understand how various personality traits enhance a social engineering exploit
- Understand potential security breaches and their common defenses
- Measure the effectiveness of your anti-social engineering program

### **Topics**

- Common Types of Social Engineering
- Personality Traits
- Potential Security Breaches
- Common Defenses
- Identity Theft and Social Engineering
- Measuring the Effectiveness of Your Anti-Social Engineering Program
- Case Studies and Role Playing

### **Audience**

This course is designed for anyone involved with security.

### **Prerequisites**

There are no prerequisites required for this course.

### **Duration**

Three days