THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

Understanding Social Engineering Attacks

EC AWR367

DHS/FEMA Funded Course

FEMA

THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

Understanding Social Engineering Attacks

EC AWR367

DHS/FEMA Funded Course

Course Description

This online course covers topics on social engineering attack techniques and tools, while also equipping learners with a better understanding of how attackers use people as the weakest link to compromise targeted organizations. Participants will learn about social engineering and become familiar with phishing attacks, develop security awareness and take preventive measures.

This course was developed by the University of Memphis, Center for Information Assurance (CfIA) through the DHS/FEMA Homeland Security National Training Program.

Course URL

https://teex.org/class/AWR367/

Prerequisites

There are no prerequisites for this course.

Course Completion Requirements

In addition to a modern computer and internet access, learners require the following software packages (all are available at no cost from their respective manufacturers):

Adobe Flash Player 9 or later and one of the following web-browsers:

- Internet Explorer (v7.0 or later)
- Mozilla Firefox (v2.0.0.6 or later)
- Opera (v9.23 or later)
- Apple Safari (v3.0.3 or later for Windows, v2.0.4 or later for MacOS)

Attendance Requirements

To meet attendance requirements, participants must review each training module and complete all required course assignments, activities, quizzes, and/or end of course exam.

Recommended

Broadband connection

Topics

Introduction to Social Engineering Attacks

- The Psychological Aspects of Social Engineering Attacks
- Types of Social Engineering Attacks
- Social Engineering Tools
- Prevention and Mitigation of Social Engineering Attacks

Suggested Audience

This course is for Government and Business IT Professionals whose responsibilities include the regular use of computing devices to connect to and perform official duties, such as responding to incidents and events that occur in cyber or in the physical critical infrastructure within the local government, federal, and private industry. These include, but are not limited to people in the following industries:

- Emergency Management Agency
- Finance & Administration
- Health Care and Emergency Medical Services
- Fire Service
- Public health
- Public Safety Communications
- Human Resources
- Information Technology (IT)
- Risk Management
- Law Enforcement
- Legal

Government Programs

- For DHS/FEMA Funded Courses, please contact ke@teex.tamu.edu or call (800) 541-7149

FEMA