FISSEA Poster, Website and Security Trinket Contest

Entry Form

Please review rules before completing entry form including the due date. The entries must be submitted by a FISSEA member prior to the deadline of February 13, 2009. No late entries will be accepted. E-mail entries to fissea-contest@nist.gov.

Name of submitter: DISA, SAIC, and Carney

Organization: Carney, Inc.

Type of entry (poster, website, newsletter, motivational item and/or training/educational exercise/scenario):

Training & Education > Interactive scenario/exercise

Title of Entry:

DoD Information Assurance Awareness

Description of Entry:

This interactive scenario-based presentation places learners in an immersive office environment and provides them with events that represent vulnerabilities and threats to a government office’s information systems. Questions simulate the real-life decision-making that occurs in a variety of scenarios that threaten to take advantage of vulnerabilities in an information system. Feedback provides detailed content around these vulnerabilities and threats. The purpose of this training is to enable learners to recognize vulnerabilities and threats and take the appropriate actions to avoid the potential losses a successful attempt can cause. This lesson is available to the DoD community of over 5,000,000 users.
The Information Assurance Awareness training begins with an animated depiction of a doomsday scenario in which a federal government employee tries to withdraw money at an ATM and learns that he has not been paid. The animation pans through a city street to several ATM machines, then zooms into the employee’s office, where he discovers that the federal government has run out of money. This causes the financial markets to go into a free fall and sparks riots and global unrest around the world. All of these events unfold because a hacker accessed a poorly secured federal government employee’s laptop or PDA.

All screens provide lively audio narration and display the audio script in the footer of the screen.
An overview section provides a definition of information assurance and information system security and describes the importance of protecting information systems containing classified and sensitive information against threats. This overview also identifies the various types of threats, the vulnerabilities inherent in information systems, and explains that users must be responsible for protecting against those threats. Learner context is reinforced throughout the course by presenting similar types of information in a consistent manner. A sample screen from the opening module appears below.

**Information Assurance (IA):**

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

**Secure Information System**

- Confidentiality
- Integrity
- Availability
- Authentication
- Nonrepudiation
The learner is then presented with a map of a building displaying offices the learner must visit in order to protect the organization’s information systems from potential threats. The learner clicks on each highlighted office in order to complete a scenario.
Upon entering each office, the learner is presented with a different information system security threat. The scenario pictured below contains multiple mini-scenarios of various phone- and email-related threats.
The learner must complete each scenario, deciding how to handle each situation and thus learning how to recognize the various threats that an organization’s information system faces and how to respond to those threats effectively. After deciding what action to take, the learner receives relevant feedback and additional information on the type of threat encountered.
A review of key points specific to the scenario is presented. Tips on how to protect against threats is presented with a summary box describing malicious code and indicating the potential consequences of falling victim to this type of threat.
Another scenario presents a situation in which the learner must decide whether to let another employee who has forgotten her security badge into a secured area. A correct decision in this case is rewarded with positive reinforcement in the feedback.
When a scenario is successfully completed it is marked with a checkmark, so the learner can track his/her progress through the building. At any point the learner can also click on the lesson map tab at the bottom of the screen to review any content already covered.
The Lesson Map displays all course topics. Those topics that have been viewed are shown with a checkmark. At any time during the course, the learner can visit the lesson map to review any individual topic in the course.
The training concludes after the learner has successfully completed all nine scenarios, which cover threats associated with wireless technology, social engineering, internet hoaxes, phishing and spear phishing, ActiveX controls, cookies, peer-to-peer software, identity theft, and improper handling of sensitive and classified information. The last screen of the course is a summary of all the best practices learned in the course to protect information systems against these potential threats. Each of the underlined words on the screen have associated rollover text with more information.