Entry Form

PLEASE REVIEW RULES BEFORE COMPLETING ENTRY FORM. All entries must be received by February 5, 2008. NO LATE ENTRIES WILL BE ACCEPTED. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Christina Painton, Carney, Inc., Developer. Prime Contractor: SAIC, End Customer: DISA.
Organization: Carney, Inc.

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

Training > educational exercise/scenario

Title of Entry:

Social Engineering Short™

Description of Entry:

This interactive scenario-based presentation places learners in an immersive office environment and provides them with events that represent attempts at social engineering. Questions simulate the real-life decision-making that occurs in a potential social engineering attempt. Feedback provides detailed content around social engineering. The purpose of this training is to enable learners to recognize social engineering attempts and take the appropriate actions to avoid the potential losses that social engineering can cause. This lesson is available to the DoD community of over 5,000,000 users.
The Social Engineering training begins by asking the learner to enter personal information for a plausible purpose. The learner has two options: entering the information or selecting the Continue button. All screens provide audio narration and display the audio script in the foot of the screen.
The learner will then receive feedback stating that by entering the information, he or she could have become a victim of social engineering.
An overview screen provides a definition of social engineering, animated examples of social engineering, and the types of loss that can occur from social engineering. A summary of these main points completes the animation. Learner context is reinforced throughout the courseware by using consistent icons to represent the social engineer and three major consequences that can result from falling victim to social engineering. The learning context is also maintained in summaries by placing consequences in the red text box, while techniques and methods are placed in charcoal text boxes.
The learner is situated in an animated office environment as typical workday scenarios are presented. The first scenario presents an email requesting assistance in securing a 35 million dollar settlement payout in exchange for private bank account information.

**Scenario 1: Email Bank Fraud**

From: William Oleander  
To: John Smith  
Cc:  
Subject: ATTN: Your money is waiting

William Oleander  
Republic of Uganda  
Kalangala District  

ATTN: Your money is waiting

I want to give you 3 million US dollars. I have been awarded a $35 million settlement from a Ugandan business. Our suppressive Ugandan government does not allow for deposits this large to be held within our country. If the Ugandan government learns of this money, they will seize it.

I need your assistance in providing your American bank account information so I can deposit the $35 million settlement into your account. Your account will provide a temporary location that my government cannot access. This money will be held in your account for 7 business days. I will then ask you to transfer $30 million back to me, leaving you with $5 million to do with as you wish. Please do not contact anyone except for me, my government will cause me great harm.

Very sincerely yours,  
William Oleannder
After the scenario is presented, the learner is asked what action to take. The learner receives relevant feedback and additional information on the type of social engineering encountered.
A review of key points specific to the email bank fraud scenario is presented. Information on how to protect against this type of social engineering is presented with a warning box indicating identity theft and financial loss as the consequences for being duped.
The second scenario presents a telephone survey fraud. The learner must decide how to respond. A correct decision in this case is rewarded with positive reinforcement in the feedback.
Two additional survey fraud scenarios are presented: printer buffer memory availability and a printer toner scam. These scenarios offer the learners the opportunity to expand their understanding of the implications of answering telephone survey questions.

**Scenario salient points for recognizing telephone survey fraud**

**Printer Buffer Memory Vulnerability**

- Asks for information over the telephone
  - Personal
- Says it is a survey
  - Could be any type of survey

**Printer Toner Scam**

- Risks: ISS access and financial loss from bogus orders

- Potentially a social engineering attempt. Although it may have seemed harmless to answer the types of questions presented in the scenario, your answers could have put the DoD at great risk. Divulging any information about the type of computer equipment the DoD uses jeopardizes the security of DoD information and information systems. Hackers can use this valuable information to gain access to DoD information systems and data. Even providing information about the type of printers your office uses can be dangerous because the buffer memory of printers is a known area of vulnerability that hackers try to exploit. If the hackers know the type of printer you
The third scenario addresses the prevalence of phishing as a common social engineering technique. As shown here, this method can use a seemingly legitimate bank interface and even reference a toll free number to call.

Scenario 3: fraudulent interface use as a pretext for gaining privacy information
Students are presented with another social engineering technique called spear phishing. The spear phishing scenario demonstrates how attackers attempt to hack into information systems through seemingly legitimate email queries or via web links. Here is the screen summary.

<table>
<thead>
<tr>
<th>Summary of Techniques</th>
<th>Summary of Methods of Protection</th>
<th>Risk to ISS availability, confidentiality, and integrity</th>
</tr>
</thead>
</table>

### Summary of Techniques

- **How to Recognize Spear Phishing:**
  - Uses email or web sites
  - Appears to be legitimate:
    - From inside your organization
    - From a position of authority
  - Is related to information systems:
    - Information asks you to click link

### Summary of Methods of Protection

- **How to Protect the DoD**
  - **Do:**
    - Contact your IAO with questions
    - Contact the sender directly
    - Report any incidents to your IAO
  - **Don't:**
    - Reply to the email
    - Click the link in the email

### What's At Risk?

You need to be aware of a particular variation of phishing, called spear phishing. Like phishing, spear phishing uses an email or web site to trick you into providing information. Spear phishing differs from phishing in that the email comes from someone who appears to be from inside your organization. It may even appear to be from someone in a position of authority to make it more likely that you will comply with the email's request. Spear phishing also differs from phishing in that it's usually an attempt to obtain information that can be used to hack into information systems. For example, a spear phishing attempt may ask you for your password or how to do...
A scenario of impersonation demonstrates how easily a worker can be duped by this social engineering technique. The technical support impersonator wears the company logo shirt, carries a labeled “Software Upgrade” disk, and is very personable on the approach.
This impersonation scenario emphasizes how trusting personnel can be in the workplace. It also illustrates the severe consequences to federal information security systems that can result from being duped by an impersonator.

Without this ISS training, most workers probably would select choice B.
The training concludes with an animated summary of social engineering techniques, the methods of protecting against social engineering attacks and scams, and the resulting consequences.