



# FISSEA Poster, Website and Security Trinket Contest

## 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](mailto: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:**

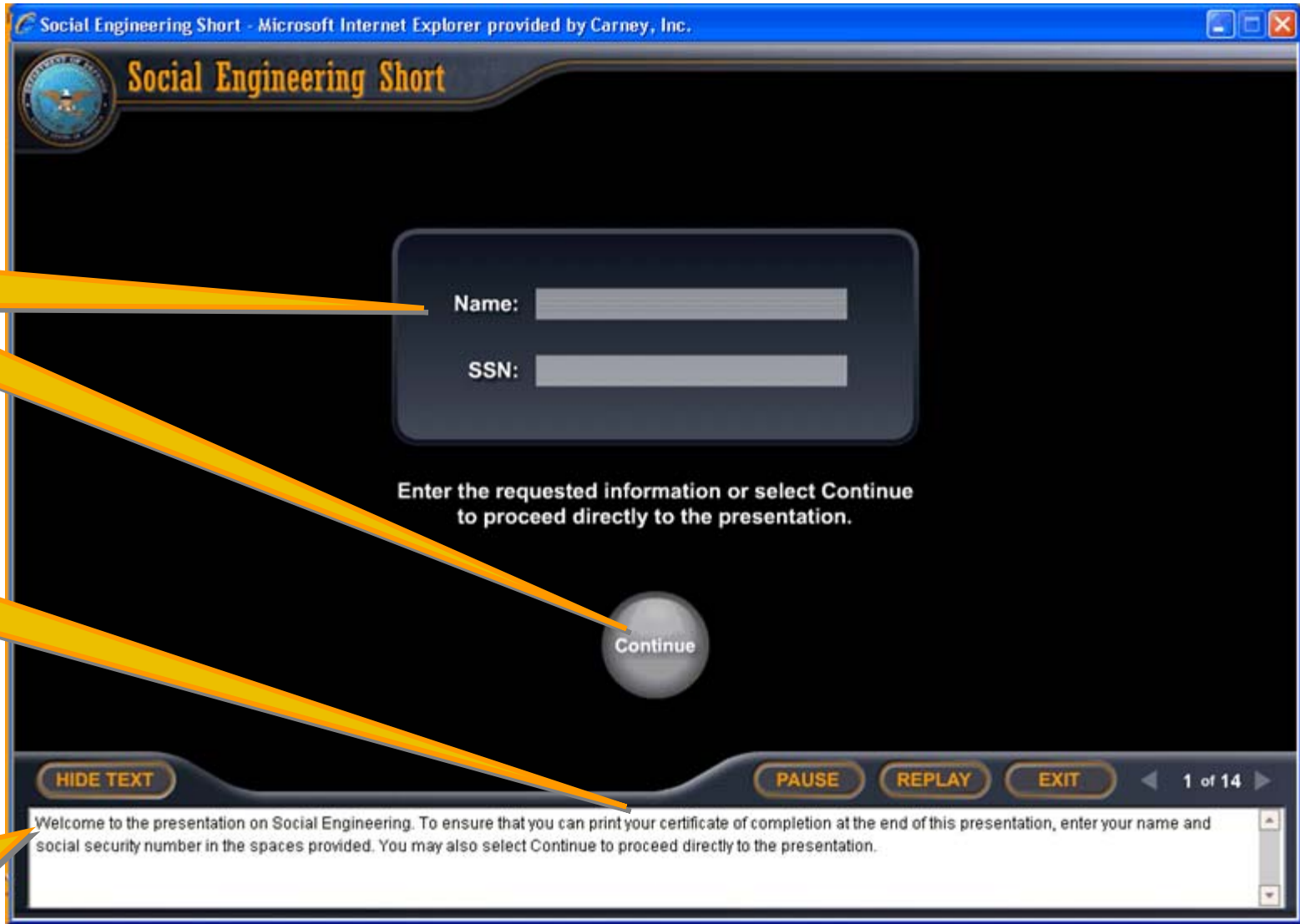
Social Engineering Short™

---

**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.



Learners have to make a decision.

Scenario presents plausible purpose

Audio narration displays in scrollable text.

The learner will then receive feedback stating that by entering the information, he or she could have become a victim of social engineering.

Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.

**Social Engineering Short**

Name:

**By entering this information, you may have become a victim of social engineering.**

to proceed directly to the presentation.

Continue

HIDE TEXT PAUSE REPLAY EXIT 1 of 14

Hold on! You should think twice before giving out your social security information or other personal information on-line or over the phone, to unknown or unverified parties. Providing that information may make you a victim of social engineering. Select the flashing forward arrow to learn more.

Immediate  
Feedback

Feedback  
Audio  
Script

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 screenshot shows a web browser window titled "Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc." The main content area is titled "Social Engineering Short" and "Social Engineering Overview". It features an illustration of a "Social Engineer" at a computer with a question mark icon. To the right, a section titled "Possible Results of Social Engineering" lists three outcomes: "Identity Theft" (with a driver's license icon), "Financial Loss" (with stacks of money), and "DoD Information Systems Access" (with a computer and padlock icon). Below this, two charcoal boxes define the "Basis for social engineering" and "Methods of social engineering". At the bottom, there are navigation buttons for "HIDE TEXT", "PAUSE", "REPLAY", and "EXIT", along with a page indicator "2 of 14".

**Consequences/ Risks**

**Possible Results of Social Engineering**

- Identity Theft
- Financial Loss
- DoD Information Systems Access

**Techniques**

**Basis for social engineering:**

- Helpfulness
- Respect for authority
- Interest in personal gain

**Methods of social engineering:**

- Conversation
- Telephone
- Email
- Internet

**Methods**

**Social Engineering Short**

**Social Engineering Overview**

**Social Engineer**

**Driver's License**  
123-456-789-012  
JOHN SMITH

**Classified**

**HIDE TEXT** **PAUSE** **REPLAY** **EXIT** 2 of 14

Social engineering is a collection of techniques intended to trick people into divulging private information, which the social engineer can then use to gain unauthorized access to an information system or to commit fraud. For example, a call from someone who claims to be a system administrator asking for your password, might be a hacker trying to gain access to your Department of Defense, or DoD, information system. Social engineering plays on human nature. It may take advantage of our desire to be friendly and helpful, or of our conditioned

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.

Office Environment



Scenario 1:  
Email Bank  
Fraud

Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.

Social Engineering Short

Tools Actions Help

Mail

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

This is to inform you that you have been recommended by a secure source to be very reliable. I want to give you 5 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 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 Oleander

HIDE TEXT PAUSE REPLAY EXIT 4 of 14

You have arrived at work and start your day at the office by checking your email. You notice an email indicating that it requires your immediate attention. The email is from William Oleander and the subject line is ATTN: Your money is waiting! The name William Oleander doesn't seem familiar to you, but you are expecting a rebate on an item you purchased a few months ago, so it's possible that it could be in reference to your rebate, or some other financial matter. You begin reading the email, and learn that Mr. Oleander is willing to give you a portion of a 35 million dollar settlement he received. The email explains that if you provide your bank account information

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.

**Social Engineering Short**

Scenario 1  
8:00 AM

From: William Oleander  
To: John Smith

**What should you do next? Select the best course of action.  
When you are finished, select Done.**

William Oleander  
Provide your banking information and plan how you will spend the money. ATTN: Your money is waiting

Forward the email to your Information Assurance Officer (IAO).  
Delete the email.  
Reply to the sender with an...

**Dangerous choice. This is a common social engineering trap that uses email to manipulate people into providing their banking information. Select the forward arrow to learn more about this type of social engineering.**

HIDE TEXT PAUSE REPLAY EXIT 4 of 14

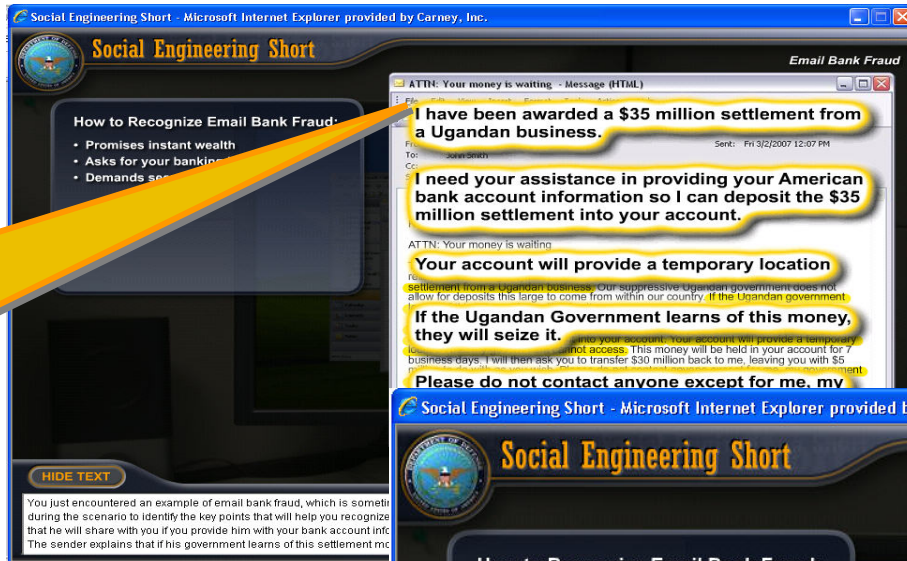
learn that Mr. Oleander is willing to give you a portion of a 35 million dollar settlement he received. The email explains that if you provide your bank account information and allow him to hold his settlement money in your account for a short amount of time, he will give you five million dollars in exchange for your cooperation and discretion about this matter. What should you do next? Select the best answer; then select Done.

What action should be taken?

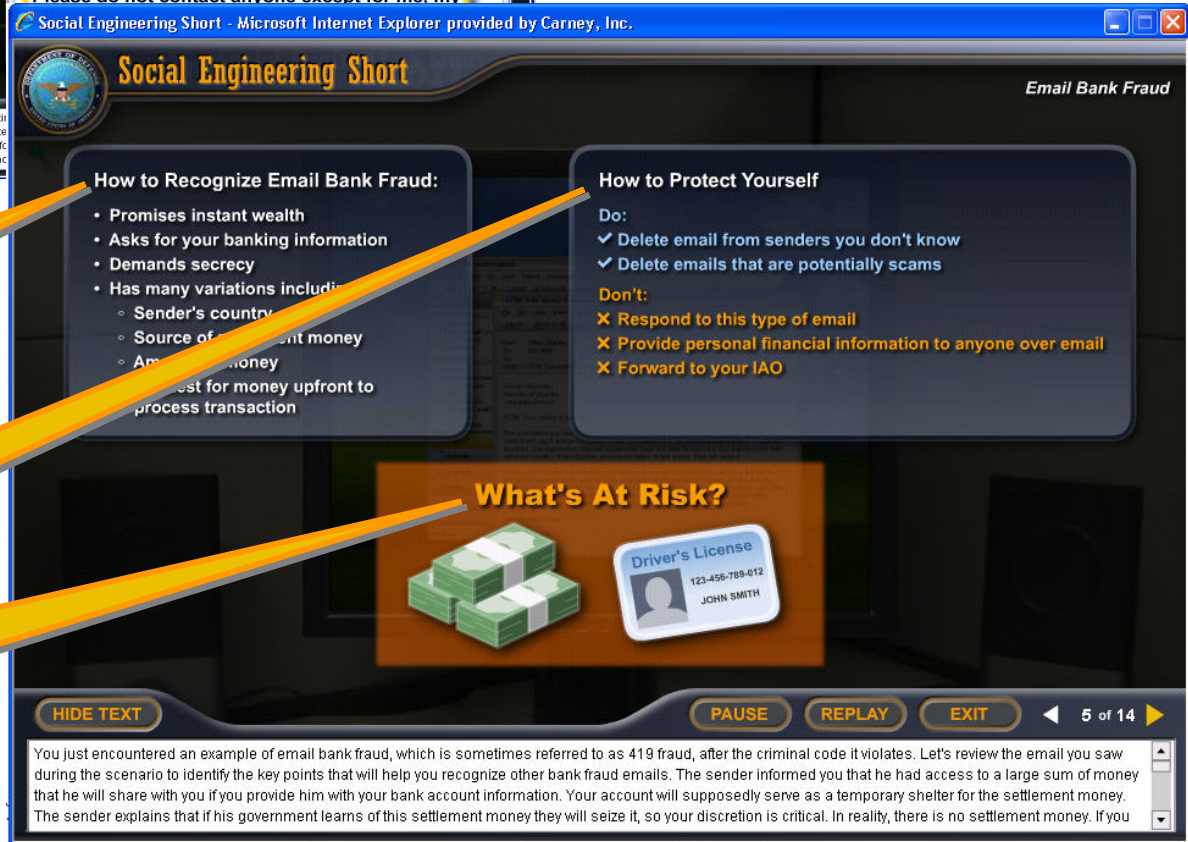
The correct answer is highlighted.

Incorrect feedback is presented.

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.



Scenario recap of salient points for recognizing email bank fraud



Summary of Techniques

Summary of Methods of Protection

Risks of Email Bank Fraud

You just encountered an example of email bank fraud, which is sometimes referred to as 419 fraud, after the criminal code it violates. Let's review the email you saw during the scenario to identify the key points that will help you recognize other bank fraud emails. The sender informed you that he had access to a large sum of money that he will share with you if you provide him with your bank account information. Your account will supposedly serve as a temporary shelter for the settlement money. The sender explains that if his government learns of this settlement money they will seize it, so your discretion is critical. In reality, there is no settlement money. If you

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.

Scenario 2:  
Telephone  
Survey  
Fraud

Positive  
Feedback

What should you do next? Select the best course of action.  
When you are finished, select Done.

Answer the caller's questions since he isn't asking about confidential or personal financial information.

Answer the caller's questions since he has more information about your computer equipment.

Do not answer any questions and end the call.

Explain that you cannot answer questions due to the highly classified nature of your work.

Smart choice! The telephone survey could be a type of social engineering. Select the forward arrow to learn more.



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

Printer Toner Scam

Risks: ISS access and financial loss from bogus orders

The screenshot shows a presentation slide titled "Social Engineering Short" with a subtitle "Telephone Survey Fraud". The slide content includes:

- How to Recognize Telephone Survey Fraud:**
  - Asks for information over the telephone
    - Personal
  - Says it is a survey
    - Could be any type of survey
- What's At Risk?** (Illustrated with a padlock, a document labeled "Classified", and stacks of money)

At the bottom of the slide, there are navigation buttons: "HIDE TEXT", "PAUSE", "REPLAY", "EXIT", and a page indicator "7 of 14". A scroll bar is visible on the right side of the slide content.

Yellow callout boxes on the left side of the image point to specific elements on the slide:

- The top callout points to the "How to Recognize Telephone Survey Fraud" section.
- The second callout points to the "Asks for information over the telephone" bullet point.
- The third callout points to the "Says it is a survey" bullet point.
- The fourth callout points to the "What's At Risk?" section.
- The fifth callout points to the "Risks" section.

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

Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.

Social Engineering Short

Urgent Action Needed Regarding Your Account - Message (HTML)

From: CountriBank  
To: John Smith  
Cc:  
Subject: Urgent Action Needed Regarding Your Account

**Countribank**

Your account with us is about to expire. If you would like to continue to use your CountriBank credit card, click the link below and verify your account information. If you don't respond within 24 hours, your account will be cancelled and you will no longer be able to use your CountriBank credit card. If you have questions regarding this request, please call 1-888-566-1212.

[www.countribank.com](http://www.countribank.com)

Lesley Shelton  
Special All-Hands Meeting

HIDE TEXT PAUSE REPLAY EXIT 8 of 14

You are working on an important project when you receive new email. You see that the email is from your credit card company and the subject line of the email says: Urgent Action Needed Regarding Your Account. Since you are concerned, you open the email. It says that your credit card is about to expire and to renew your account, you need to click the link provided to their web site and validate your account information. The email also states that your account will be canceled if you don't respond within 24 hours. What should you do next? Select the best answer; then select Done.

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.

The screenshot shows a presentation slide titled "Social Engineering Short" with a sub-header "Spear Phishing". The slide is displayed in a Microsoft Internet Explorer browser window. The slide content is as follows:

- How to Recognize Spear Phishing:**
  - Uses email or web sites
  - Appears to be a legitimate:
    - From inside your organization
    - From a position of authority
  - Is related to information systems:
    - Requests information
    - Asks you to click link
- 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?**
  - Icons of a laptop, a padlock, and a document labeled "Classified".

At the bottom of the slide, there are navigation buttons: "HIDE TEXT", "PAUSE", "REPLAY", "EXIT", and a page indicator "10 of 14". A text box at the very bottom contains the following text:

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 get

Summary of Techniques

Summary of Methods of Protection

Risk to ISS availability, confidentiality, and integrity

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.

The screenshot shows a training module window titled "Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.". The main content area displays a video of an office scene. A man in a green polo shirt with a company logo and khaki pants is standing and talking to a man in a blue striped shirt sitting at a desk. The man in green is holding a white CD-ROM. The man in blue is looking at a computer monitor. The video player interface includes a "Scenario 4 4:45 PM" indicator in the top right, a "HIDE TEXT" button in the bottom left, and "PAUSE", "REPLAY", and "EXIT" buttons in the bottom center. A progress bar shows "11 of 14".

Scenario 5:  
Impersonation  
Technique

You are trying to finish your project before the end of the day, when you are approached by a representative from your technical support vendor that you haven't seen around the office before. He informs you that your IAO has asked him to install a software upgrade package on your computer. He wants to know if you can take a short break so that he can install the upgrade. What should you do next? Select the best answer; then select Done.

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

Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.

### Social Engineering Short

Scenario 4  
4:45 PM

What should you do next? Select the best course of action.  
When you are finished, select Done.

- Tell the person that you need to finish this project, but to come back in 30 minutes and perform the install after you leave for the day.
- Step aside and allow this person to install the upgrade.
- Ask the person for identification and call your IAO to verify the request.
- Tell the person you aren't comfortable with him performing the install, but to give you instructions and you will perform the install.

**Dangerous choice. This might make you a victim of a social engineering tactic that uses impersonation to obtain information. Select the forward arrow to learn more about this type of social engineering.**

HIDE TEXT

You are trying to finish your project before the end of the day, when you are around the office before. He informs you that your IAO has asked him to break so that he can install the upgrade. What should you do next? Select

Summary of Techniques

Summary of Methods of Protection

Risk:  
ISS Access

Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.

### Social Engineering Short

Impersonation

**How to Recognize Impersonation:**

- Pretends to be someone you would trust
- Wants access to:
  - Your office
  - Information
  - Your computer systems
- May pretend to be from well-known organization
- May pretend to be or mention authority figure
- Has a plausible reason for information/access

**How to Protect the DoD**

**Do:**

- ✓ Ask for identification
- ✓ Contact your IAO or person referenced

**Don't:**

- ✗ Automatically grant access to your computer
- ✗ Disclose information system passwords or other access information to anyone

**What's At Risk?**

Classified

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.

Social Engineering Short - Microsoft Internet Explorer provided by Carney, Inc.

## Social Engineering Short

Summary and Conclusion

### Potential Losses

- Identity Theft (Driver's License icon)
- Financial Loss (Stacks of money icon)
- DoD Information Systems Access (Laptop with padlock and Classified document icon)

### Methods Used

(Illustration of a person at a computer with a speech bubble)

### Protect Yourself and the DoD

**Do:**

- ✓ Watch out for social engineering
- ✓ Contact your IAO with any questions
- ✓ Report any potential incidents

**Don't:**

**X Disclose information:**

- o Personal
- o Financial
- o Confidential/classified
- o Information system-related

### Common social engineering techniques:

- Email bank fraud
- Telephone surveys
- Phishing and spear phishing
- Impersonation

**Consequences/Risks** (Callout pointing to Potential Losses)

**Methods to Protect against Social Engineering** (Callout pointing to Common social engineering techniques)

**Social Engineering Techniques** (Callout pointing to Common social engineering techniques)

HIDE TEXT PAUSE REPLAY EXIT 13 of 14

As you learned, social engineering poses great risks to you and to the DoD. Anyone can be a victim of social engineering. When social engineering attacks succeed, it is because we are human, and social engineering takes advantage of human nature. By being aware of specific techniques and methods social engineers use to obtain information, and by following a few simple do's and don'ts, you can protect yourself and the DoD from potential losses. This completes the presentation on social engineering. Select the forward arrow to print your certificate of completion.