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.

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

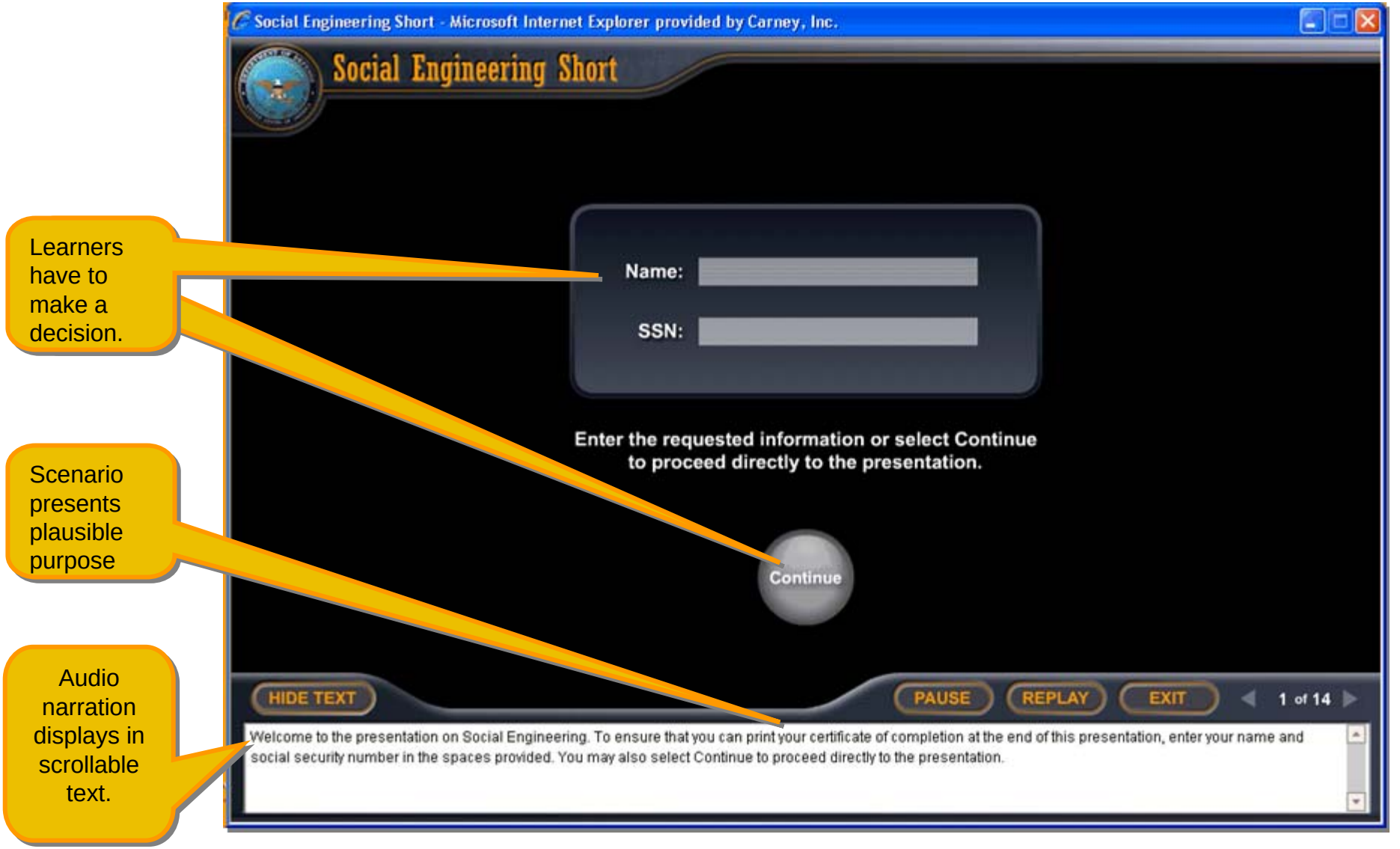
Title of Entry:

Social Engineering Short™

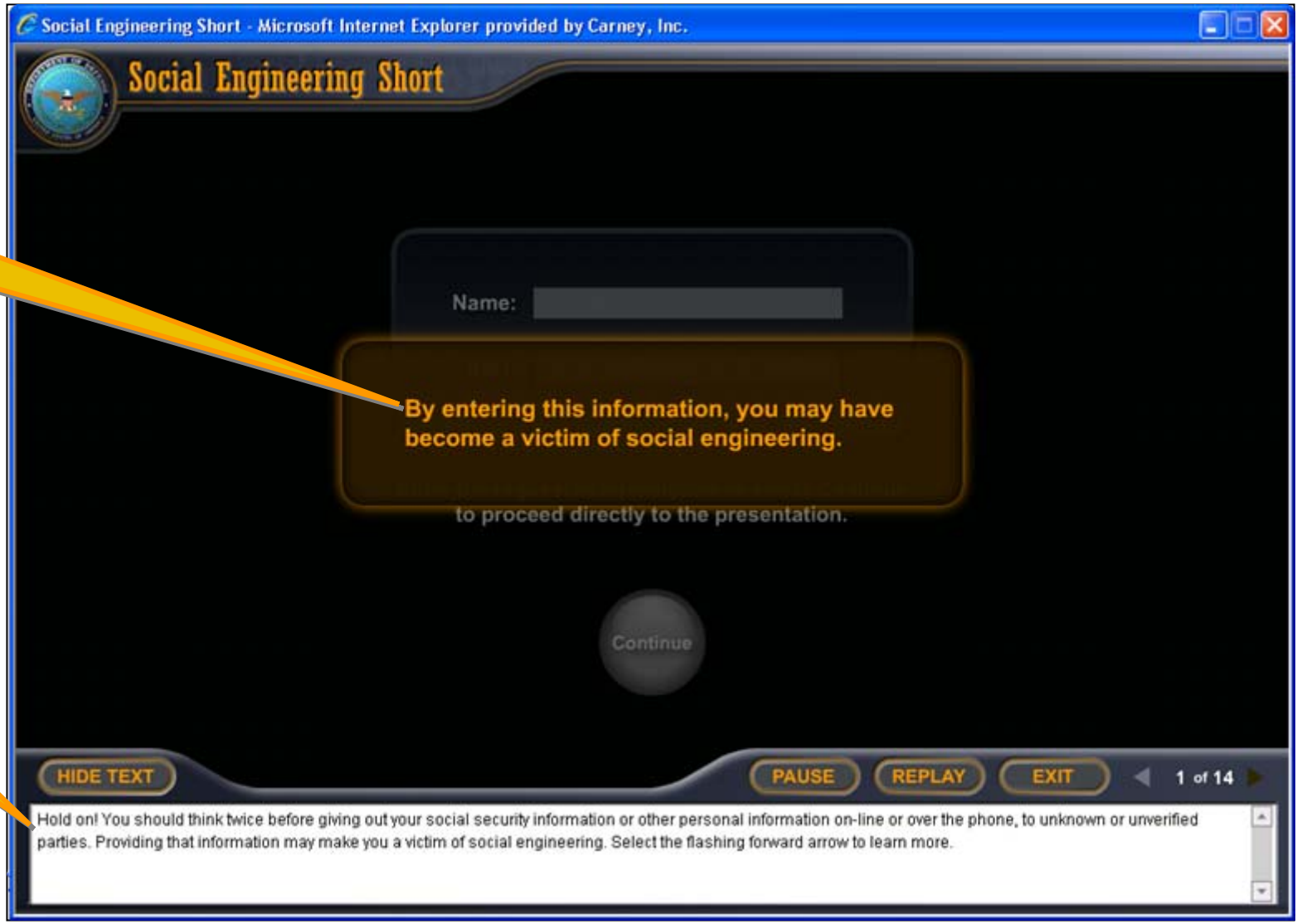
Description of Entry:

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 plausable 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.



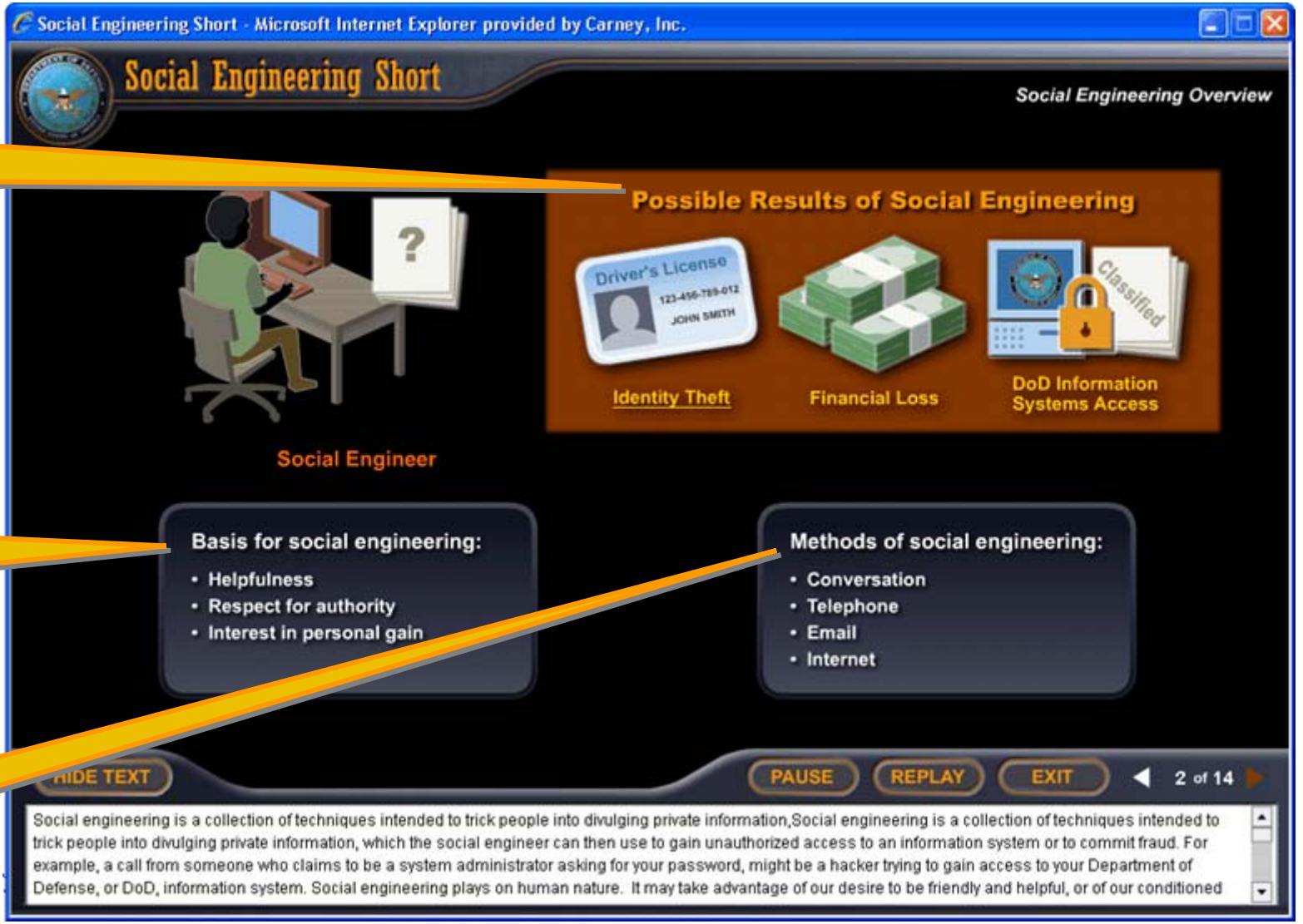
The learner will then receive feedback stating that by entering the information, he or she could have become a victim of social engineering.



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.



Consequences/ Risks

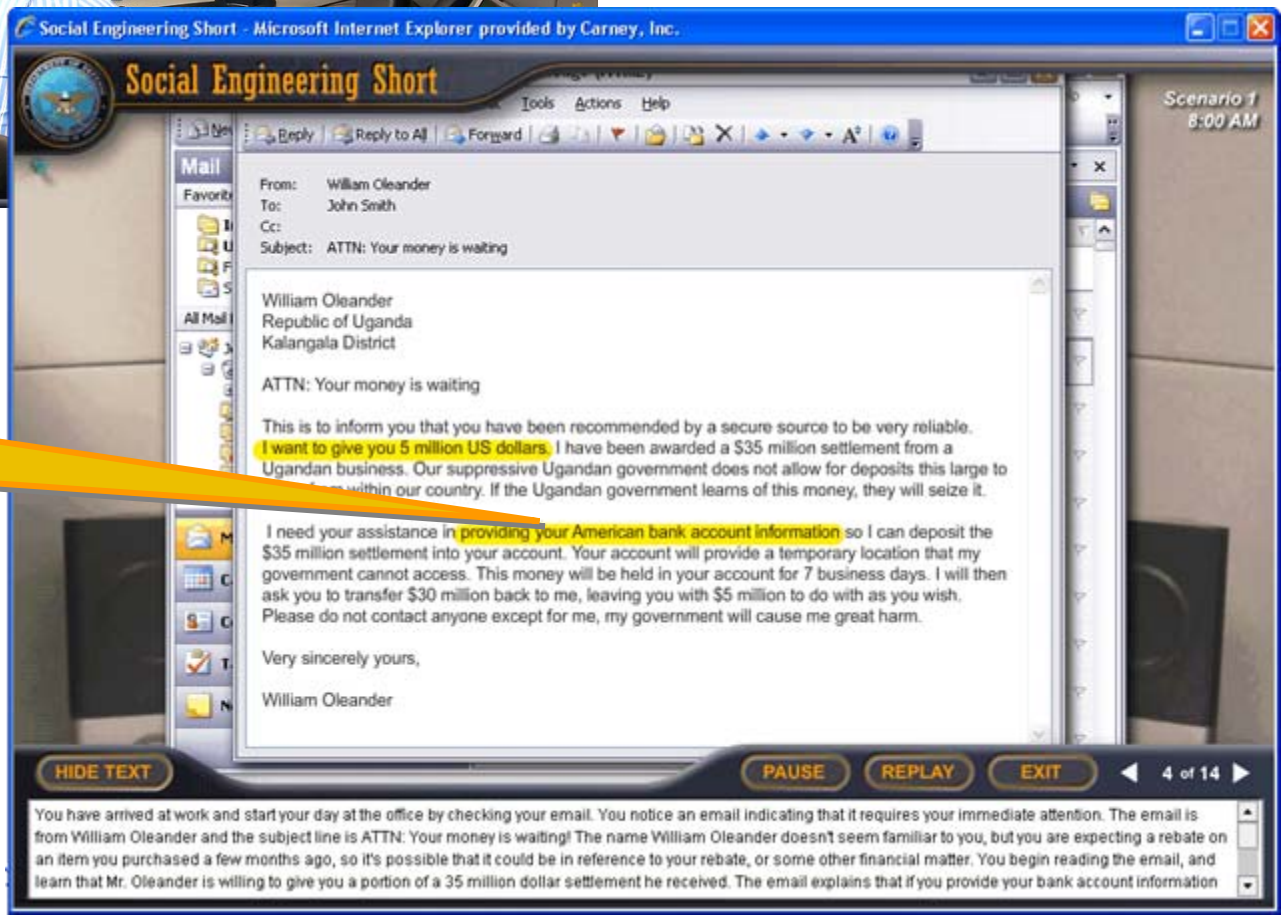
Techniques

Methods

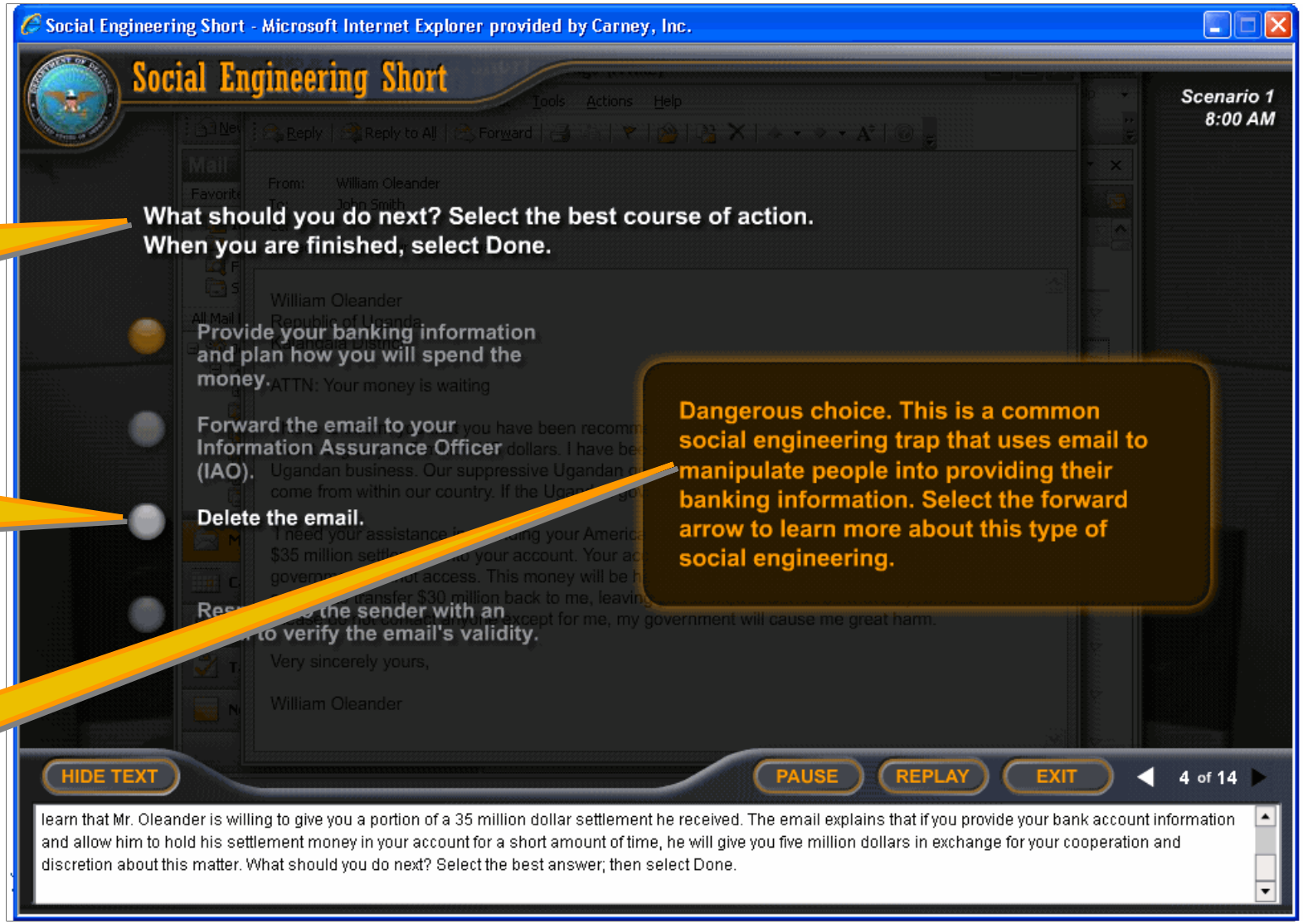
The learner is situated in an animated office environment as typical workday scenarios are presented. The first scenario presents an email requesting assistance in securing a 35 million dollar settlement payout in exchange for private bank account information.

Office Environment

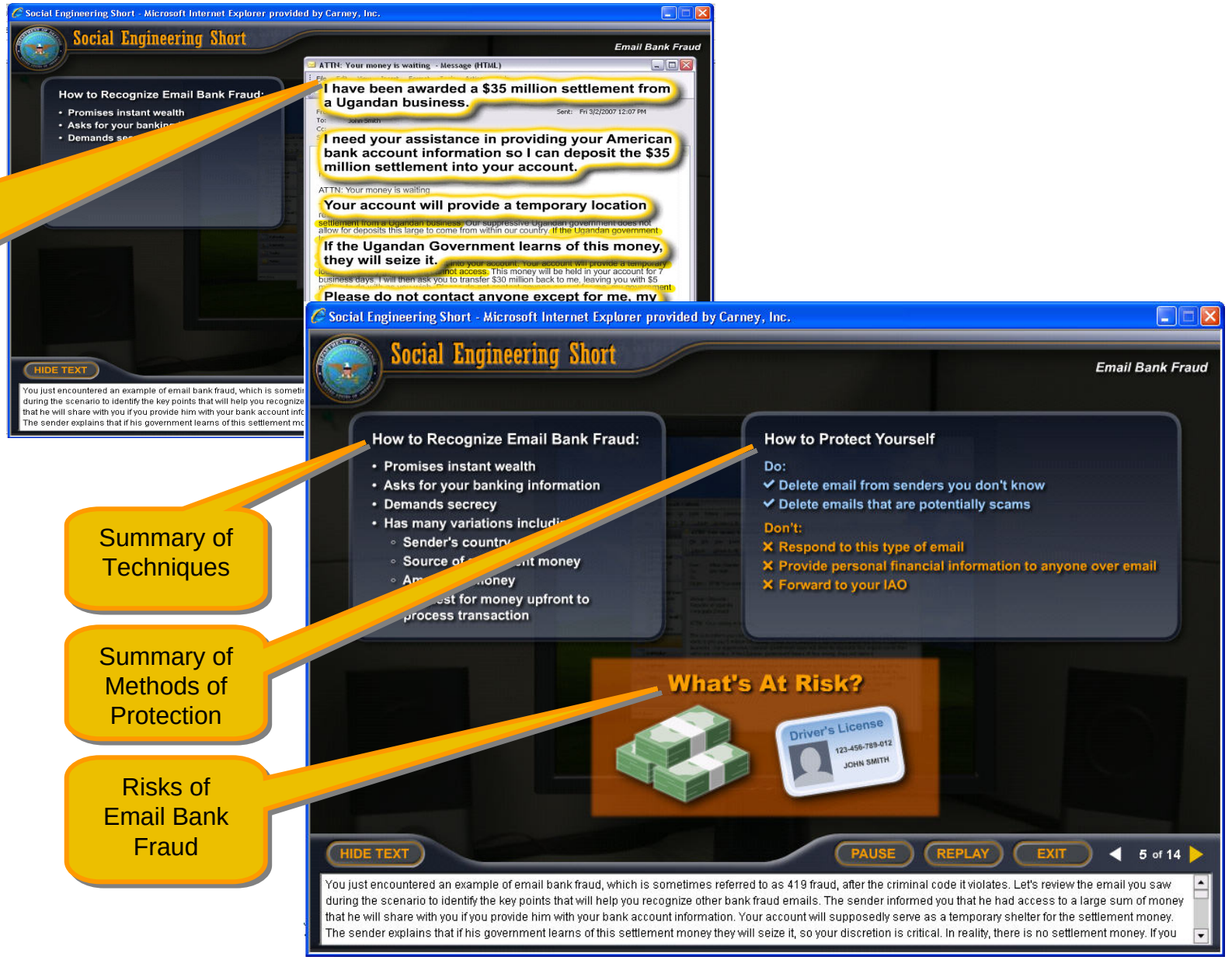
Scenario 1: Email Bank Fraud



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.

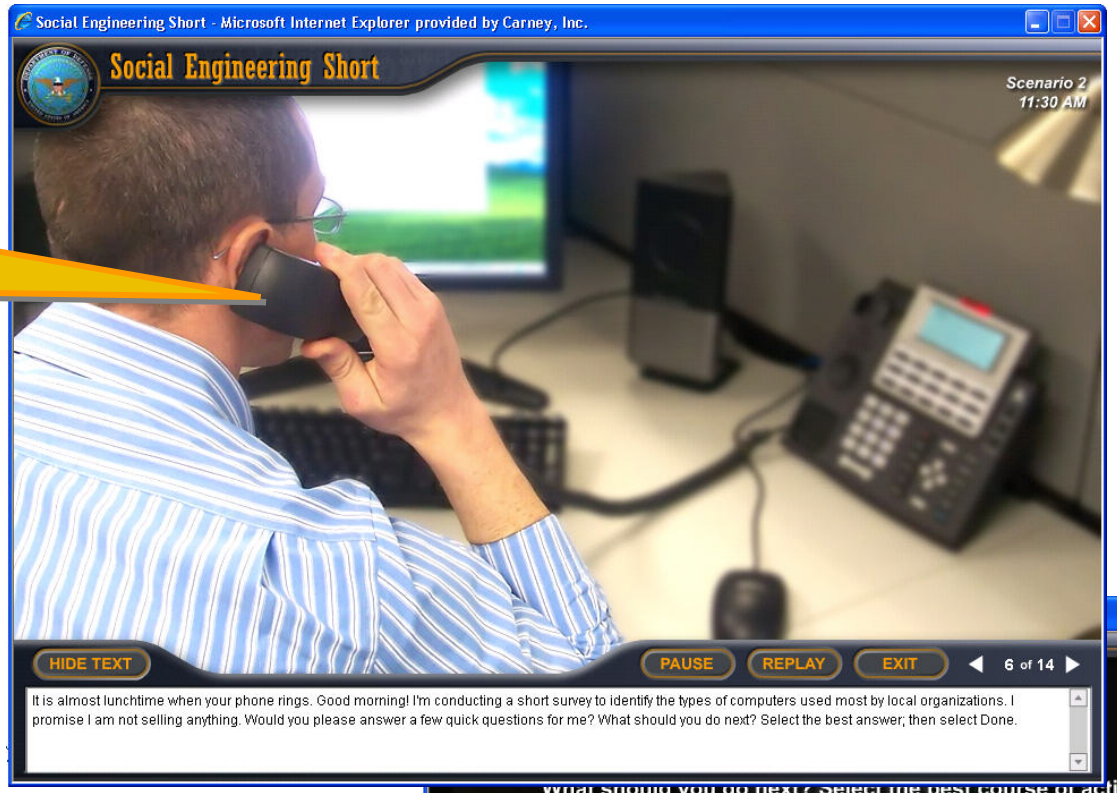


A review of key points specific to the email bank fraud scenario is presented. Information on how to protect against this type of social engineering is presented with a warning box indicating identity theft and financial loss as the consequences for being duped.

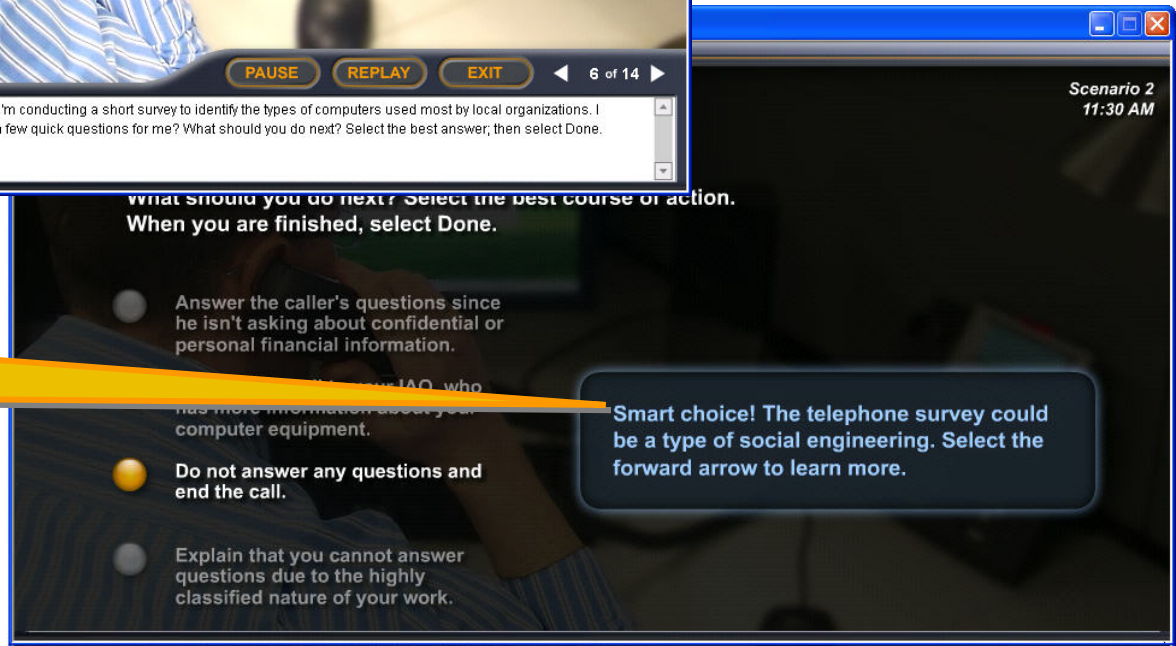


The second scenario presents a telephone survey fraud. The learner must decide how to respond. A correct decision in this case is rewarded with positive reinforcement in the feedback.

Scenario 2: Telephone Survey Fraud



Positive Feedback



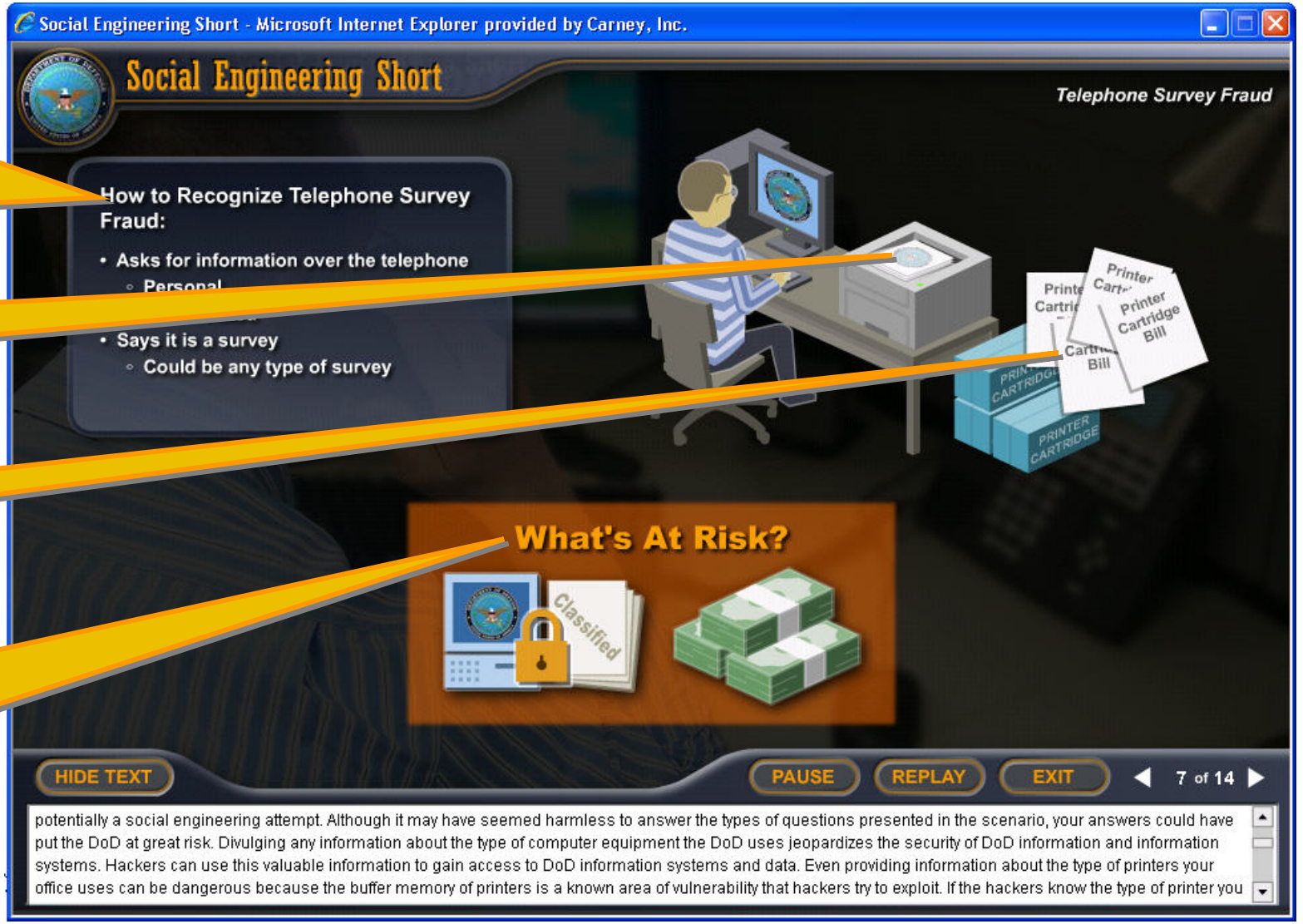
Two additional survey fraud scenarios are presented: printer buffer memory availability and a printer toner scam. These scenarios offer the learners the opportunity to expand their understanding of the implications of answering telephone survey questions.

Scenario salient points for recognizing telephone survey fraud

Printer Buffer Memory Vulnerability

Printer Toner Scam

Risks: ISS access and financial loss from bogus orders



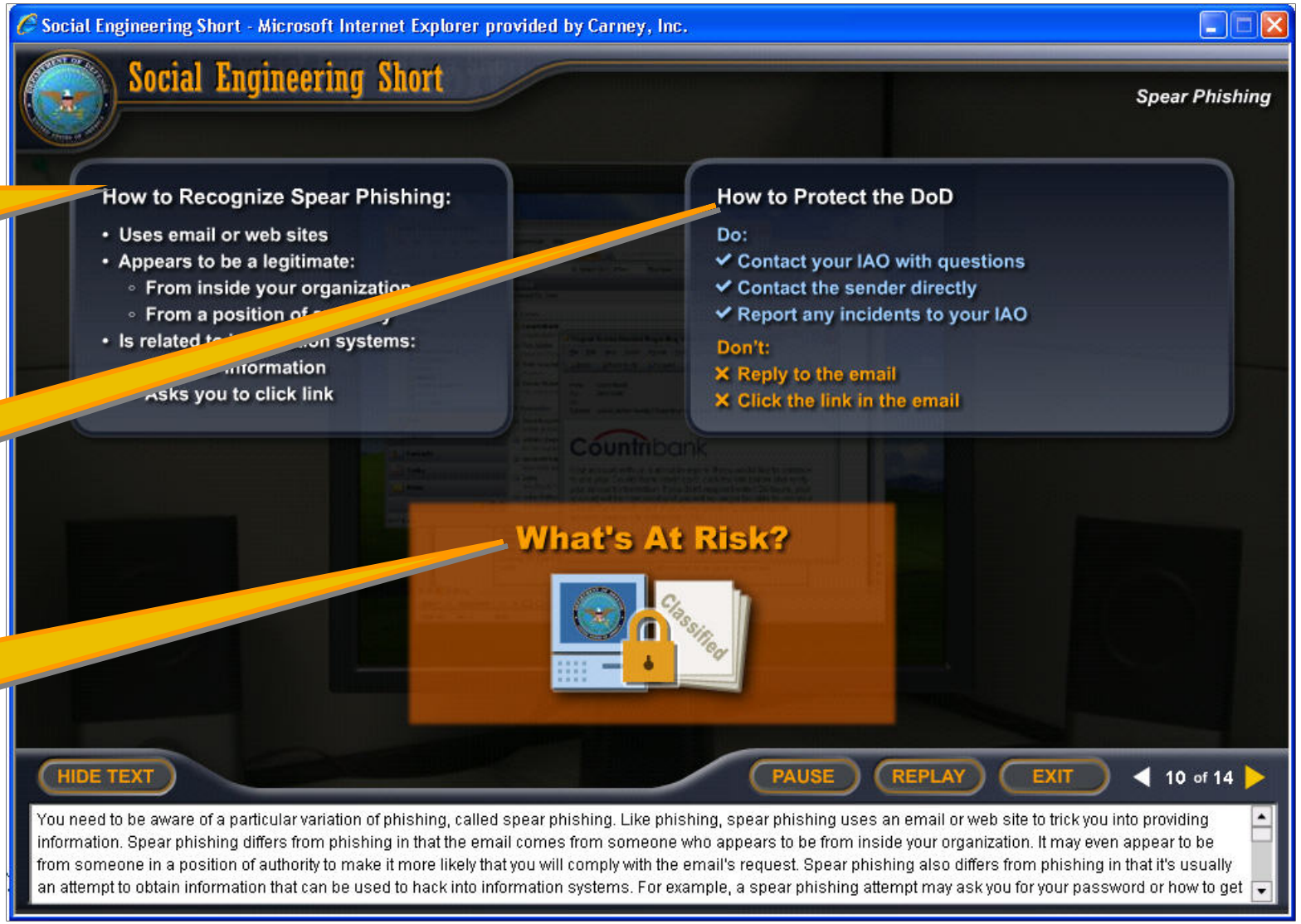
The third scenario addresses the prevalence of phishing as a common social engineering technique. As shown here, this method can use a seemingly legitimate bank interface and even reference a toll free number to call.

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.

Summary of Techniques

Summary of Methods of Protection

Risk to ISS availability, confidentiality, and integrity

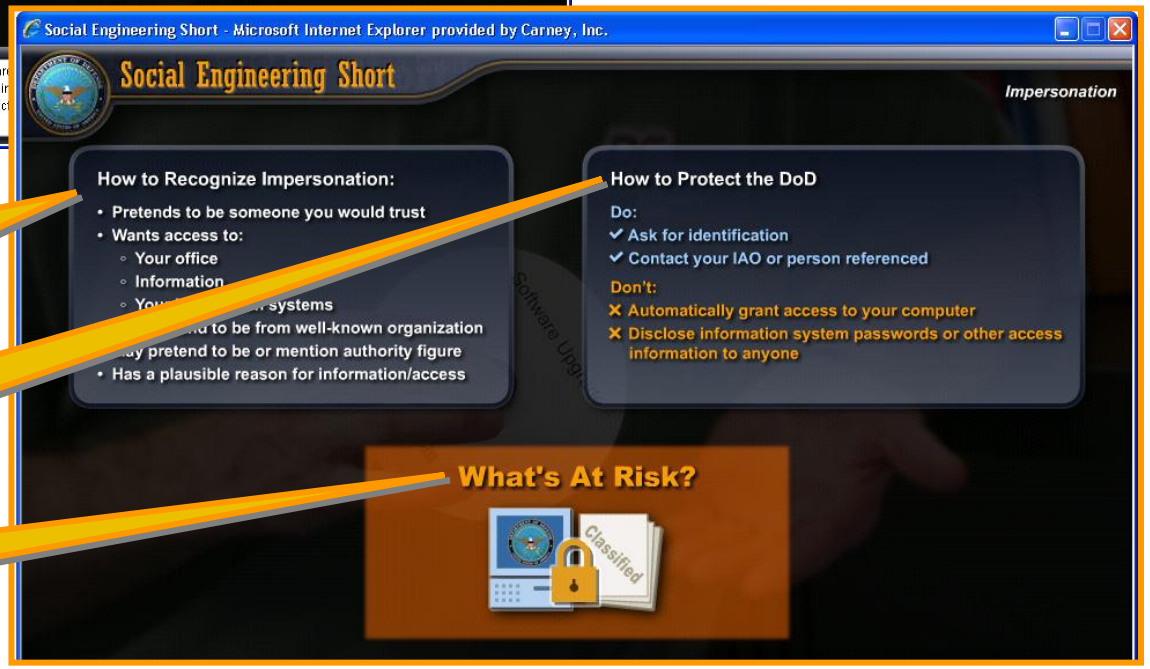


A scenario of impersonation demonstrates how easily a worker can be duped by this social engineering technique. The technical support impersonator wears the company logo shirt, carries a labeled “Software Upgrade” disk, and is very personable on the approach.

Scenario 5: Impersonation Technique

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



Summary of Techniques

Summary of Methods of Protection

Risk: ISS Access

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.

Consequences/ Risks

Methods to Protect against Social Engineering

Social Engineering Techniques