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:

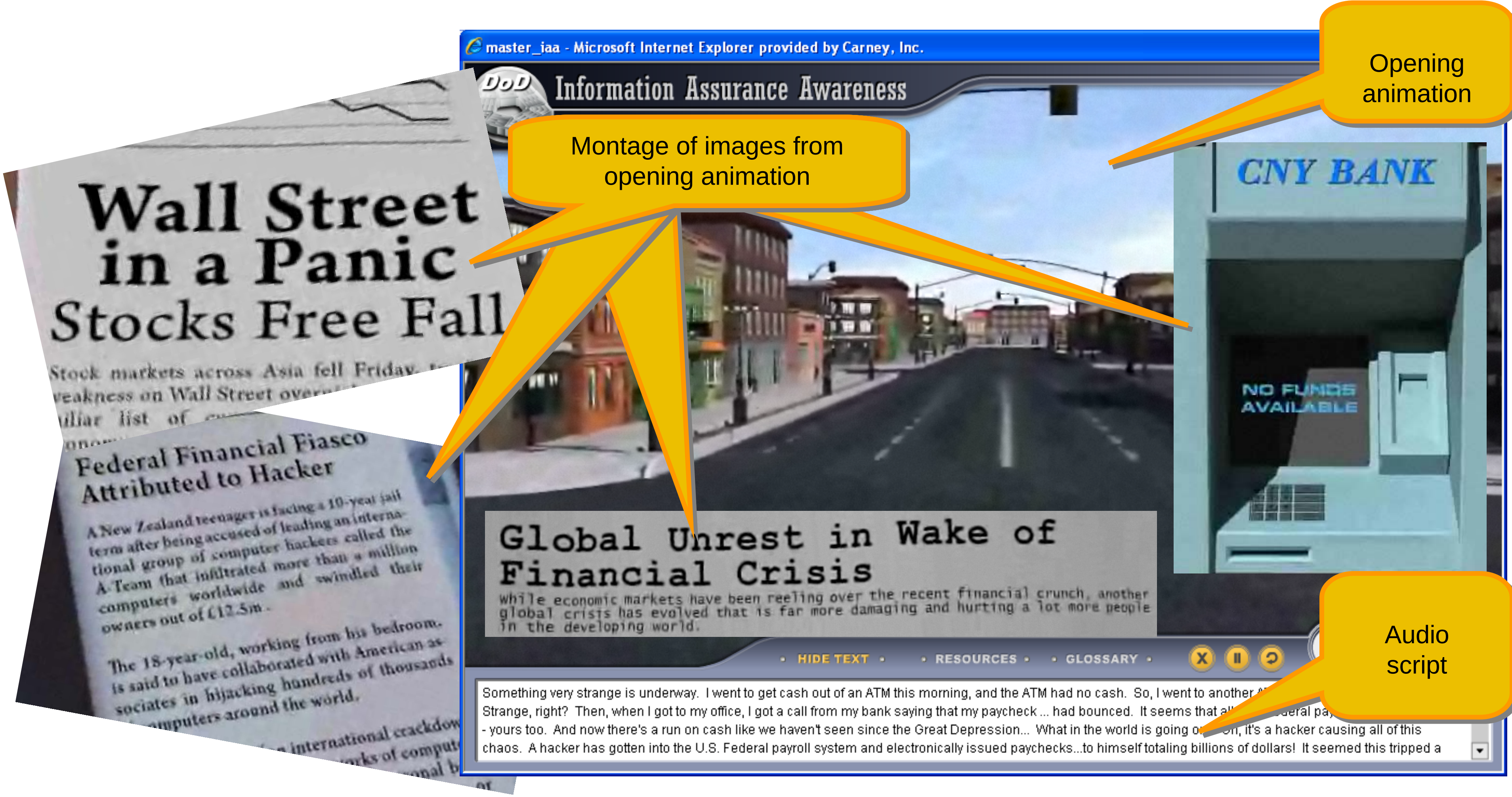
DoD Information Assurance Awareness

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.



Wall Street in a Panic
Stocks Free Fall

Stock markets across Asia fell Friday
weakness on Wall Street over
iliar list of

Federal Financial Fiasco Attributed to Hacker

A New Zealand teenager is facing a 10-year jail term after being accused of leading an international group of computer hackers called the A-Team that infiltrated more than a million computers worldwide and swindled their owners out of £12.5m.

The 18-year-old, working from his bedroom, is said to have collaborated with American associates in hijacking hundreds of thousands of computers around the world.

international crackdown
works of comput
onal b
of

master_iaa - Microsoft Internet Explorer provided by Carney, Inc.

Information Assurance Awareness

Global Unrest in Wake of Financial Crisis

While economic markets have been reeling over the recent financial crunch, another global crisis has evolved that is far more damaging and hurting a lot more people in the developing world.

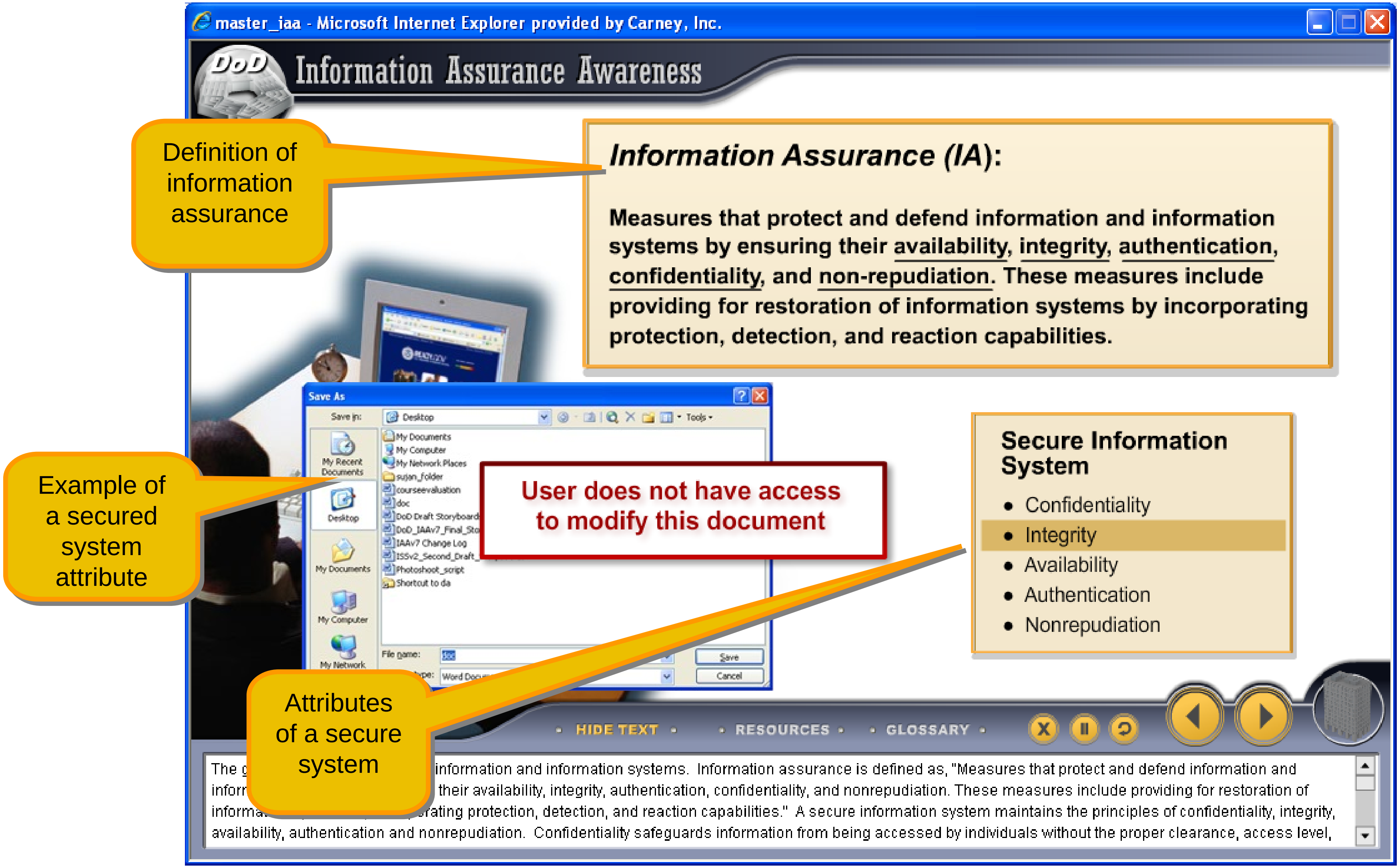
Something very strange is underway. I went to get cash out of an ATM this morning, and the ATM had no cash. So, I went to another A
Strange, right? Then, when I got to my office, I got a call from my bank saying that my paycheck ... had bounced. It seems that al eral pa
- yours too. And now there's a run on cash like we haven't seen since the Great Depression... What in the world is going o on, it's a hacker causing all of this chaos. A hacker has gotten into the U.S. Federal payroll system and electronically issued paychecks...to himself totaling billions of dollars! It seemed this tripped a

Opening animation

Montage of images from opening animation

Audio script

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.



master_iaa - Microsoft Internet Explorer provided by Carney, Inc.

DoD Information Assurance Awareness

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.

User does not have access to modify this document

Secure Information System

- Confidentiality
- Integrity
- Availability
- Authentication
- Nonrepudiation

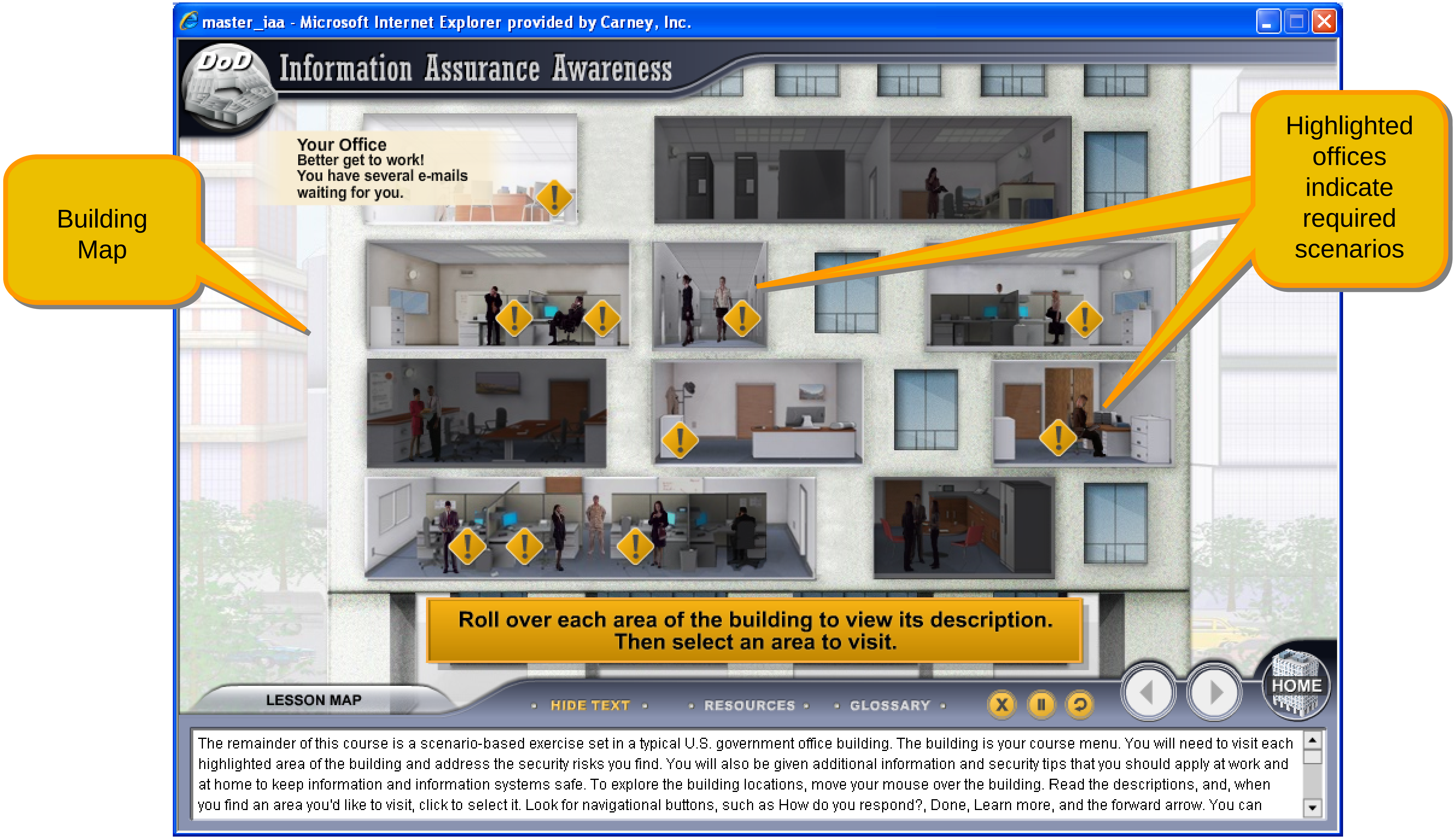
The g information and information systems. Information assurance is defined as, "Measures that protect and defend information and inforr their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of informa rating protection, detection, and reaction capabilities." A secure information system maintains the principles of confidentiality, integrity, availability, authentication and nonrepudiation. Confidentiality safeguards information from being accessed by individuals without the proper clearance, access level,

Definition of information assurance

Example of a secured system attribute

Attributes of a secure system

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.


master_iaa - Microsoft Internet Explorer provided by Carney, Inc.
DoD
Information Assurance Awareness
LESSON MAP
HIDE TEXT
RESOURCES
GLOSSARY
HOME

Building Map

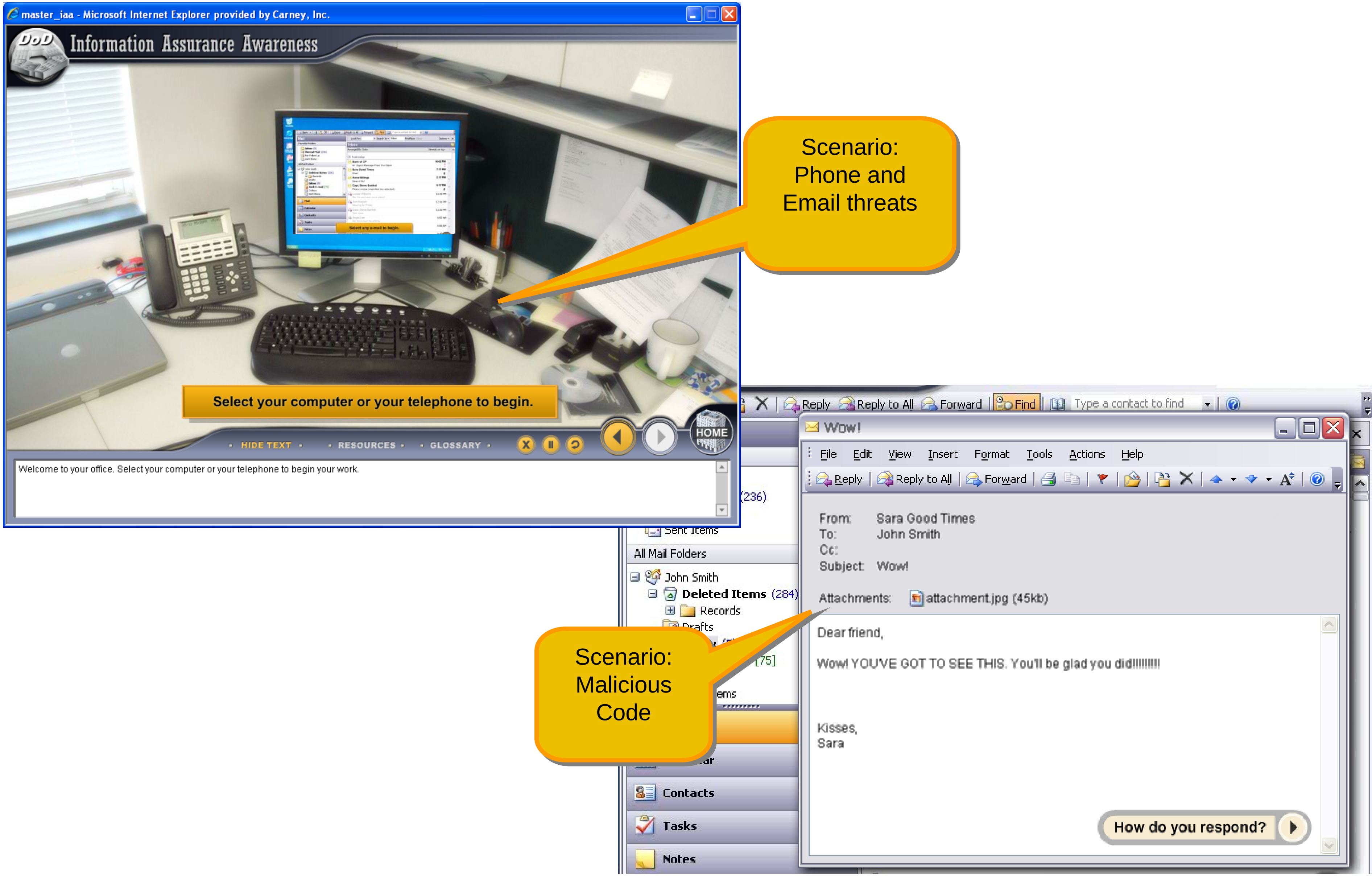
Highlighted offices indicate required scenarios

Your Office
Better get to work!
You have several e-mails waiting for you.

Roll over each area of the building to view its description.
Then select an area to visit.

The remainder of this course is a scenario-based exercise set in a typical U.S. government office building. The building is your course menu. You will need to visit each highlighted area of the building and address the security risks you find. You will also be given additional information and security tips that you should apply at work and at home to keep information and information systems safe. To explore the building locations, move your mouse over the building. Read the descriptions, and, when you find an area you'd like to visit, click to select it. Look for navigational buttons, such as How do you respond?, Done, Learn more, and the forward arrow. You can

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.



Select your computer or your telephone to begin.

Welcome to your office. Select your computer or your telephone to begin your work.

Wow!

From: Sara Good Times
To: John Smith
Cc:
Subject: Wow!

Attachments: attachment.jpg (45kb)

Dear friend,

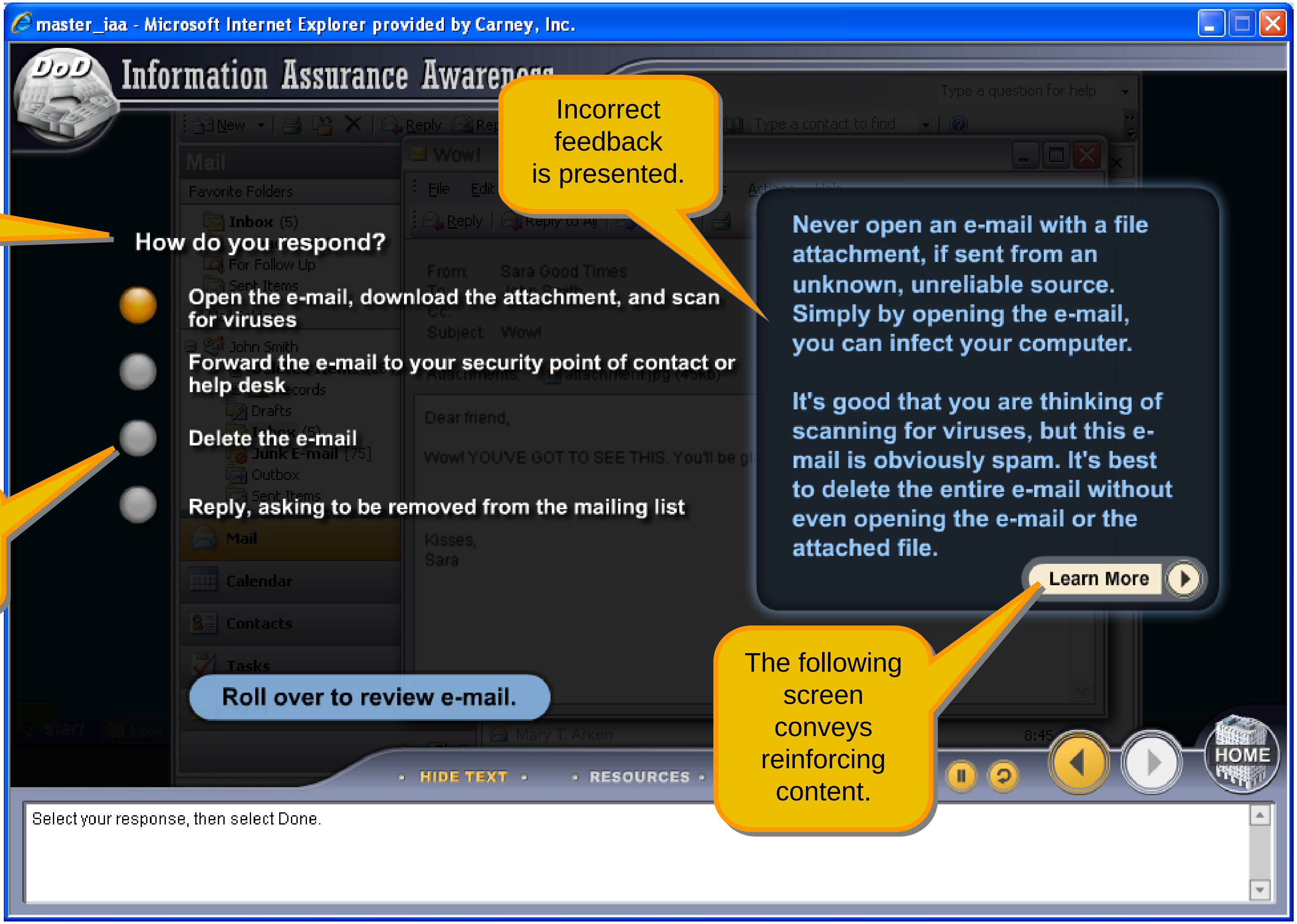
Wow! YOU'VE GOT TO SEE THIS. You'll be glad you did!!!!!!!!

Kisses,
Sara

Scenario: Phone and Email threats

Scenario: Malicious Code

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.



master_iaa - Microsoft Internet Explorer provided by Carney, Inc.

Information Assurance Awareness

How do you respond?

● Open the e-mail, download the attachment, and scan for viruses

○ Forward the e-mail to your security point of contact or help desk

○ Delete the e-mail

○ Reply, asking to be removed from the mailing list

Never open an e-mail with a file attachment, if sent from an unknown, unreliable source. Simply by opening the e-mail, you can infect your computer.

It's good that you are thinking of scanning for viruses, but this e-mail is obviously spam. It's best to delete the entire e-mail without even opening the e-mail or the attached file.

Roll over to review e-mail.

Select your response, then select Done.

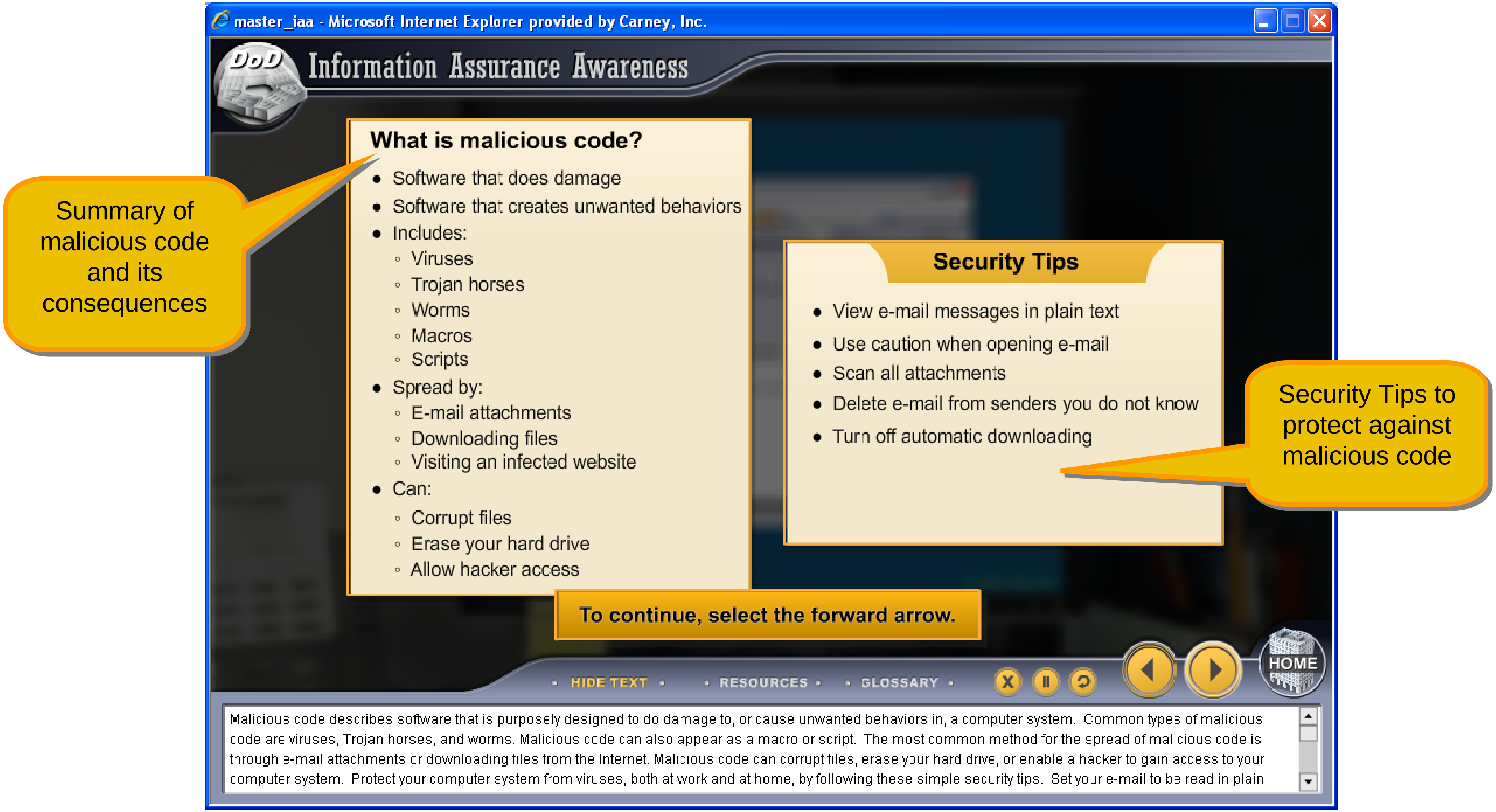
What action should be taken?

Incorrect feedback is presented.

The correct answer

The following screen conveys reinforcing content.

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.



master_iaa - Microsoft Internet Explorer provided by Carney, Inc.
DoD
Information Assurance Awareness
HIDE TEXT
RESOURCES
GLOSSARY
HOME

What is malicious code?

- Software that does damage
- Software that creates unwanted behaviors
- Includes:
  - Viruses
  - Trojan horses
  - Worms
  - Macros
  - Scripts
- Spread by:
  - E-mail attachments
  - Downloading files
  - Visiting an infected website
- Can:
  - Corrupt files
  - Erase your hard drive
  - Allow hacker access

Security Tips

- View e-mail messages in plain text
- Use caution when opening e-mail
- Scan all attachments
- Delete e-mail from senders you do not know
- Turn off automatic downloading

To continue, select the forward arrow.

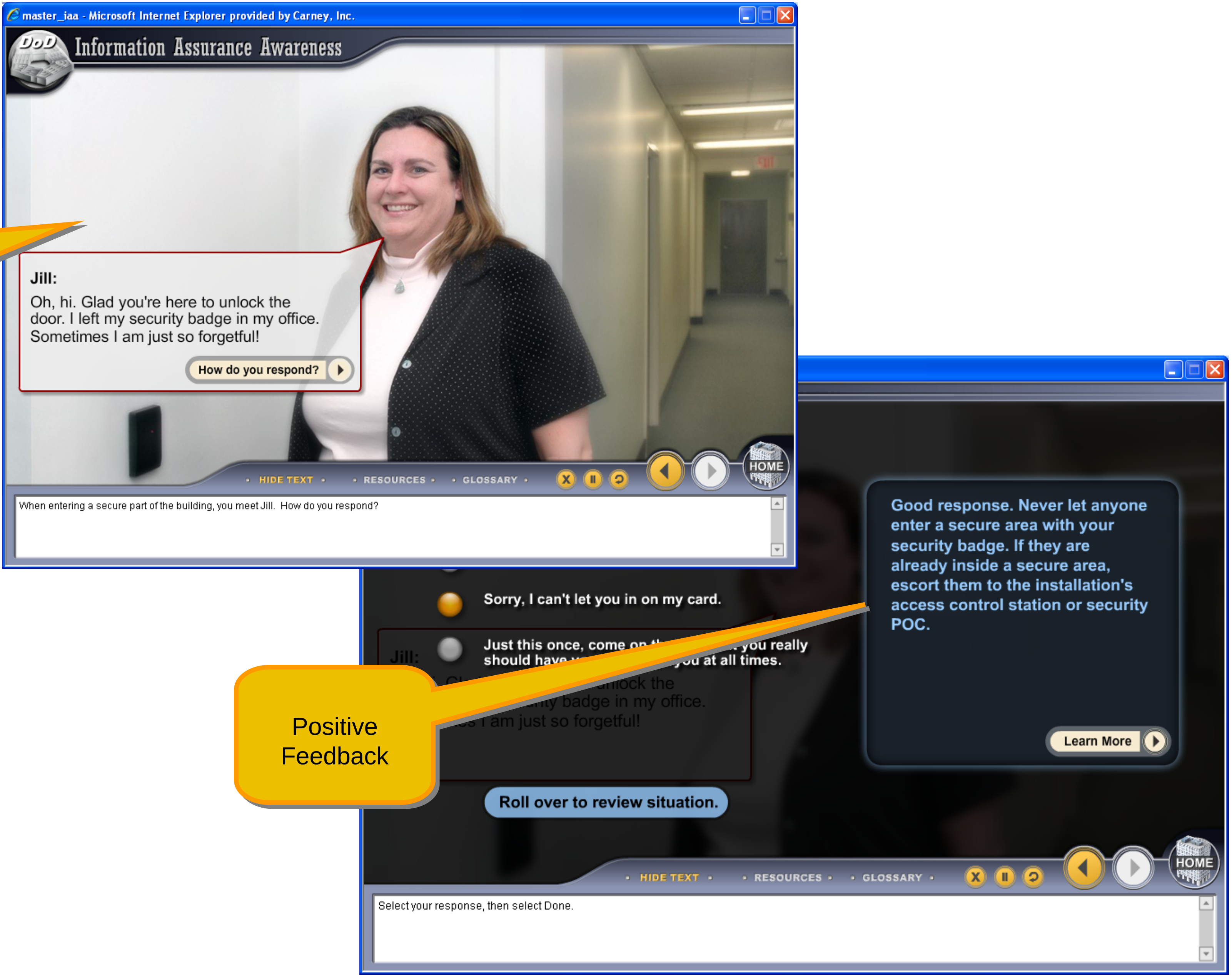
Malicious code describes software that is purposely designed to do damage to, or cause unwanted behaviors in, a computer system. Common types of malicious code are viruses, Trojan horses, and worms. Malicious code can also appear as a macro or script. The most common method for the spread of malicious code is through e-mail attachments or downloading files from the Internet. Malicious code can corrupt files, erase your hard drive, or enable a hacker to gain access to your computer system. Protect your computer system from viruses, both at work and at home, by following these simple security tips. Set your e-mail to be read in plain

Summary of malicious code and its consequences

Security Tips to protect against malicious code

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.

Scenario: Physical Security


master_iaa - Microsoft Internet Explorer provided by Carney, Inc.
DoD
Information Assurance Awareness
HIDE TEXT
RESOURCES
GLOSSARY
HOME

Jill:

Oh, hi. Glad you're here to unlock the door. I left my security badge in my office. Sometimes I am just so forgetful!

When entering a secure part of the building, you meet Jill. How do you respond?

Sorry, I can't let you in on my card.

Just this once, come on ... you really should have ... you at all times.

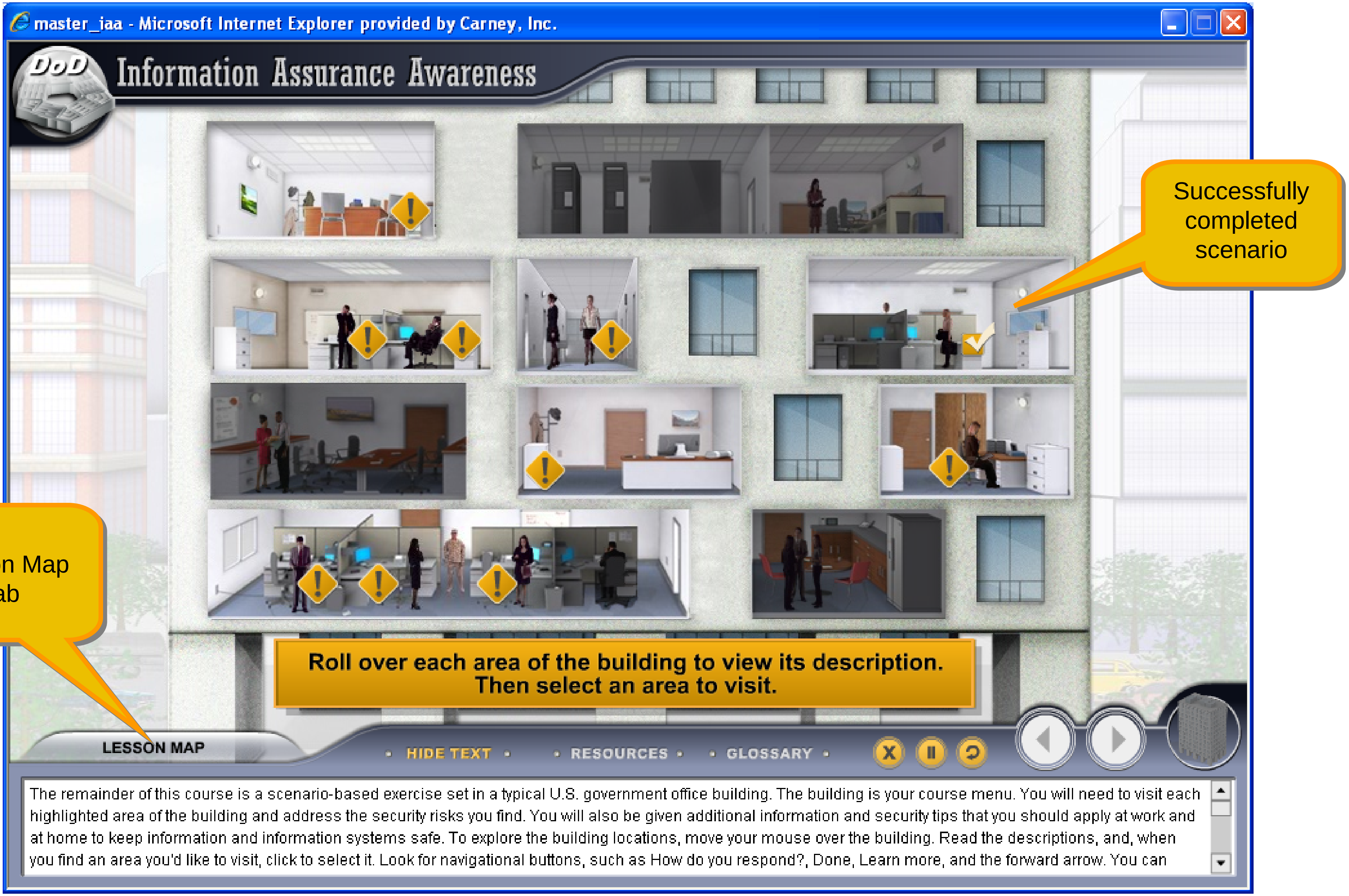
Jill: ... unlock the ... badge in my office. ... I am just so forgetful!

Good response. Never let anyone enter a secure area with your security badge. If they are already inside a secure area, escort them to the installation's access control station or security POC.

Select your response, then select Done.

Positive 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 the screen to review any content already covered.

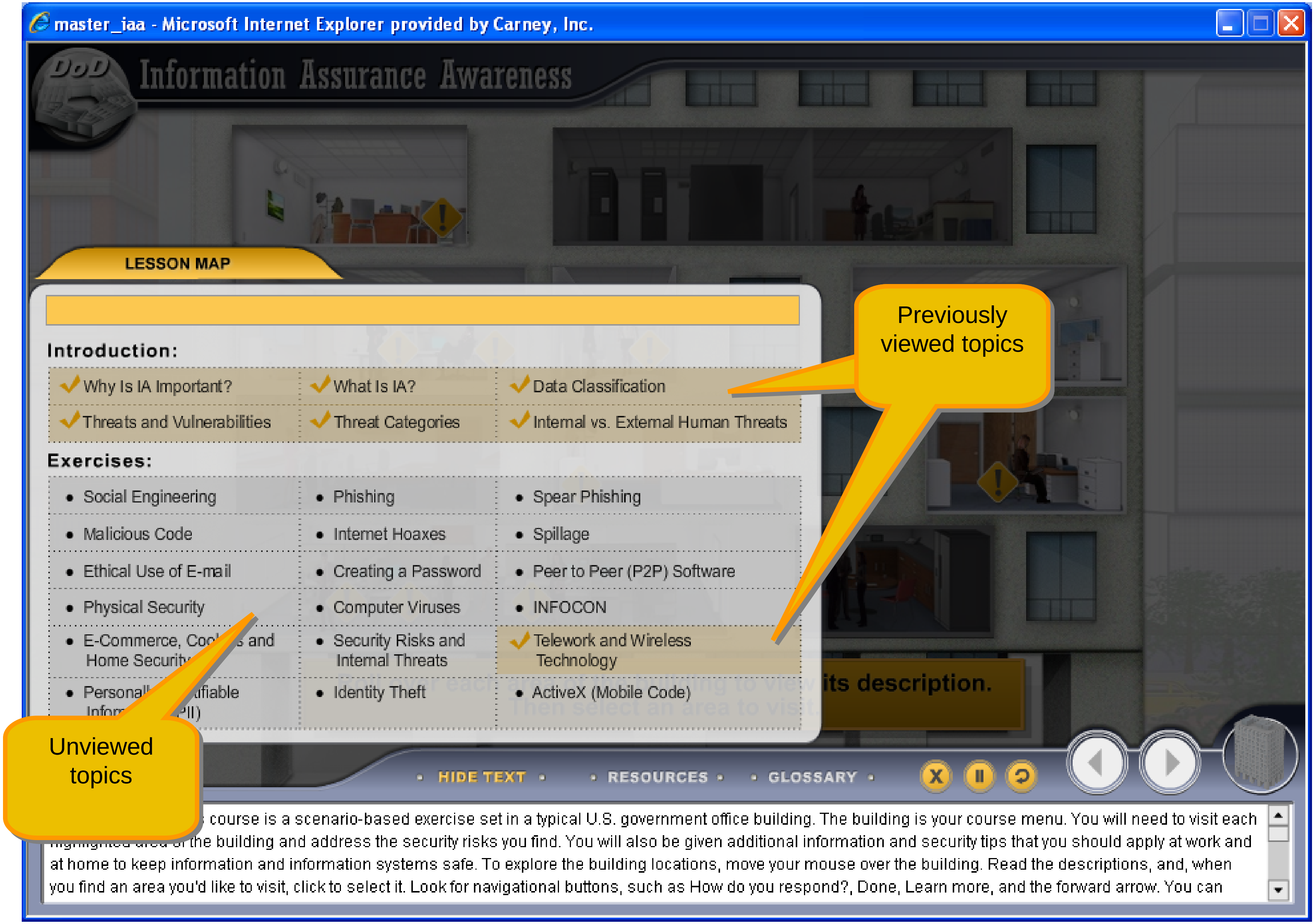


master_iaa - Microsoft Internet Explorer provided by Carney, Inc.
DoD
Information Assurance Awareness
Successfully completed scenario
Lesson Map tab
LESSON MAP
HIDE TEXT
RESOURCES
GLOSSARY

Roll over each area of the building to view its description. Then select an area to visit.

The remainder of this course is a scenario-based exercise set in a typical U.S. government office building. The building is your course menu. You will need to visit each highlighted area of the building and address the security risks you find. You will also be given additional information and security tips that you should apply at work and at home to keep information and information systems safe. To explore the building locations, move your mouse over the building. Read the descriptions, and, when you find an area you'd like to visit, click to select it. Look for navigational buttons, such as How do you respond?, Done, Learn more, and the forward arrow. You can

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.



master_iaa - Microsoft Internet Explorer provided by Carney, Inc.
DoD
Information Assurance Awareness
LESSON MAP
HIDE TEXT
RESOURCES
GLOSSARY

Introduction:

✓ Why Is IA Important?	✓ What Is IA?	✓ Data Classification
✓ Threats and Vulnerabilities	✓ Threat Categories	✓ Internal vs. External Human Threats

Exercises:

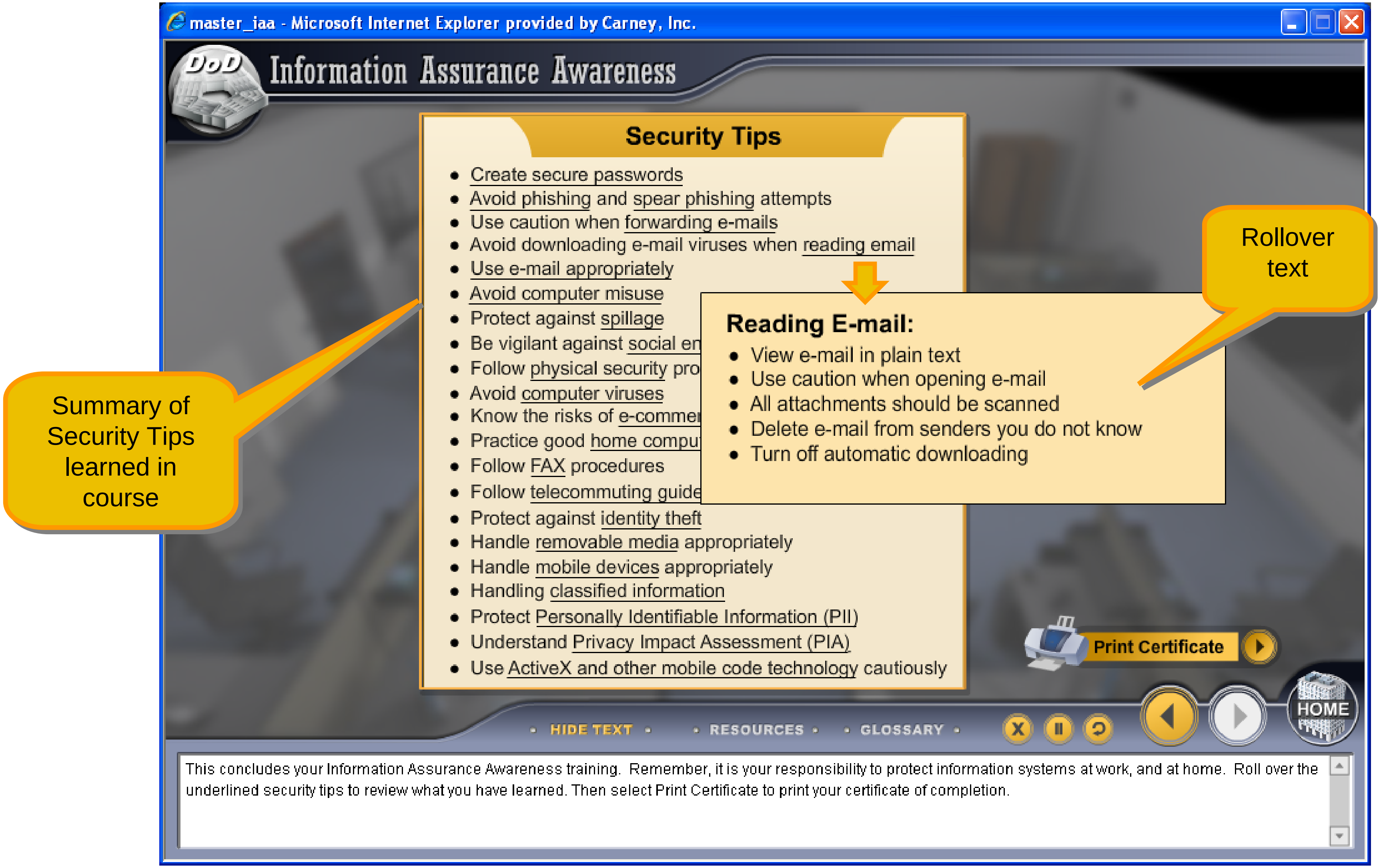
• Social Engineering	• Phishing	• Spear Phishing
• Malicious Code	• Internet Hoaxes	• Spillage
• Ethical Use of E-mail	• Creating a Password	• Peer to Peer (P2P) Software
• Physical Security	• Computer Viruses	• INFOCON
• E-Commerce, Cookies and Home Security	• Security Risks and Internal Threats	✓ Telework and Wireless Technology
• Personally Identifiable Information (PII)	• Identity Theft	• ActiveX (Mobile Code)

…course is a scenario-based exercise set in a typical U.S. government office building. The building is your course menu. You will need to visit each highlighted area of the building and address the security risks you find. You will also be given additional information and security tips that you should apply at work and at home to keep information and information systems safe. To explore the building locations, move your mouse over the building. Read the descriptions, and, when you find an area you'd like to visit, click to select it. Look for navigational buttons, such as How do you respond?, Done, Learn more, and the forward arrow. You can

Previously viewed topics

Unviewed topics

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.


master_iaa - Microsoft Internet Explorer provided by Carney, Inc.
DoD
Information Assurance Awareness
Print Certificate
HOME
HIDE TEXT
RESOURCES
GLOSSARY

Summary of Security Tips learned in course

Rollover text

Security Tips

- Create secure passwords
- Avoid phishing and spear phishing attempts
- Use caution when forwarding e-mails
- Avoid downloading e-mail viruses when reading email
- Use e-mail appropriately
- Avoid computer misuse
- Protect against spillage
- Be vigilant against social en
- Follow physical security pro
- Avoid computer viruses
- Know the risks of e-comme
- Practice good home compu
- Follow FAX procedures
- Follow telecommuting guide
- Protect against identity theft
- Handle removable media appropriately
- Handle mobile devices appropriately
- Handling classified information
- Protect Personally Identifiable Information (PII)
- Understand Privacy Impact Assessment (PIA)
- Use ActiveX and other mobile code technology cautiously

Reading E-mail:

- View e-mail in plain text
- Use caution when opening e-mail
- All attachments should be scanned
- Delete e-mail from senders you do not know
- Turn off automatic downloading

This concludes your Information Assurance Awareness training. Remember, it is your responsibility to protect information systems at work, and at home. Roll over the underlined security tips to review what you have learned. Then select Print Certificate to print your certificate of completion.