Building a Comprehensive Security Awareness Program:

If You Build It, They Will Listen

Sherri Balderson, PMP

Federal Reserve Bank of Richmond

© Federal Reserve Bank of Richmond-2008

Key Points

- Federal Reserve Overview
- Awareness Model
  - Decentralized vs. Centralized
- Management Support
- Comprehensive Awareness Program
- Summary
  - Lessons Learned

© Federal Reserve Bank of Richmond-2008

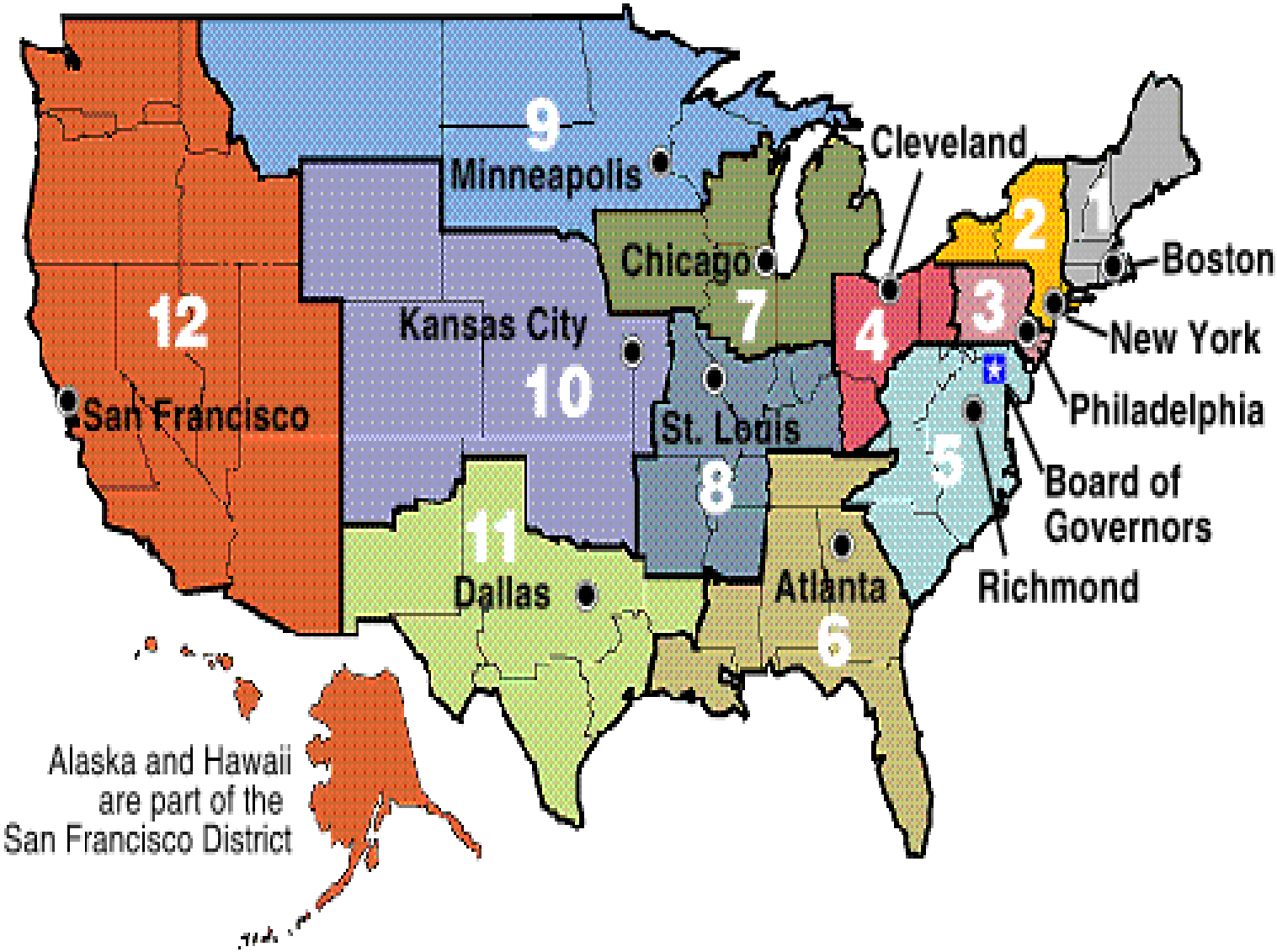
Federal Reserve Overview

Game Show

- We'll have
  - Game Show Host
  - Super Model
- Divide into 2 teams
  - "Security Gurus"
  - "Security Aces"
  - Each team answers 2 questions about the Fed
  - Winning team – prizes!

© Federal Reserve Bank of Richmond-2008

Federal Reserve System Structure



© Federal Reserve Bank of Richmond-2008

Decentralized Awareness Model

- Before 2004, 12 Districts conducted separate awareness programs
- Results:
  - Inefficiencies and redundancies
  - Inconsistent content
  - Inconsistent knowledge

© Federal Reserve Bank of Richmond-2008

Centralized Awareness Model

- 2004 – Centralize national awareness training
  - Target over 20,000 employees/contractors in 37 offices
- Program Goals
  - Centralize training/aid development and procurement
  - Standardize security awareness and understanding
  - Increase efficiency
  - Capitalize on System expertise where possible
- Results:
  - Efficiencies and Economies of Scale
  - Standard
    - Content based on Policy
    - Training
    - Reporting
    - Communications

© Federal Reserve Bank of Richmond-2008

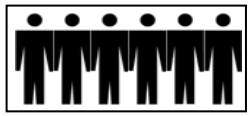
FR Awareness and Training Overview

Security Training

Specialized (Periodic)

Training Based on Job Function and Responsibility

Build knowledge and skills



Targeted Employees and Contract Workers

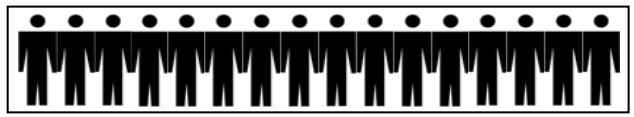
Security Awareness

Baseline (Ongoing)

Awareness Programs | **Access Agreement** | **New Employee**

Newsletter | **IS Web Site** | **Materials** | **Awareness Campaign**

Focus on good security practices



All Employees and Contract Workers

© Federal Reserve Bank of Richmond-2008

National Support
Upper-Level Management

- Obtained commitment and agreement
- Led to increased funding
- Continue seeking support by constantly soliciting feedback

© Federal Reserve Bank of Richmond-2008

Local Support
District Management

- Information Security Officer
  - Executive level staff responsible for all aspects of information security in the District
- Information Security Awareness Contact(s)
  - Responsible for national awareness program implementation locally

© Federal Reserve Bank of Richmond-2008

Infrastructure SMEs/Approvals

Training Developers

Groupware/ E-mail

Remote Access

Hard Disk Encryption

ISOs 1 – 12

Instructional Designers

Internet

Standard Software

Help Desk Managers

National Information Security Awareness Program (4.5 FTE)

ID Management

DCLs 1 – 12

LMS Administrator

Penetration Testing

Business Executives

Web site Developers

Corporate Communicat.

Graphic Designers

Legal Counsel

Vendors

FR Central IT

Printing Services

Distribution Services

© Federal Reserve Bank of Richmond-2008

Newsletter

- In publication since 2004
- Produced quarterly
- Distribute hard copy
- PDF posted to internal Web site
- Subscription service

WINTER 2006

Security Bits & Bytes

Information Security News for Federal Reserve Employees

Destination: Internet - Travel with Care

Information Security Week 2006 is coming soon to a Fed near you! Visit the National Information Security Awareness web site (https://nisap.frb.org) every day during your District's week (*see complete list at right*) and learn more about safe Internet travels. Play interactive games and answer the question of the day for a chance to win a prize!

IS Week activities will guide you through safe Internet travels by focusing on kids' safety, blogging, malware, phishing and avoiding common web pitfalls.

Information Security Week Schedule:

Monday - Kids' Internet safety
Tuesday - Phishing
Wednesday - Avoiding common Internet pitfalls
Thursday - Blogging
Friday - Malware (viruses, spyware and other bad stuff)

February 27-March 3	March 6-10	March 13-17
Cleveland	Chicago	Atlanta
Dallas	St. Louis	Boston
FRIT	San Francisco	Minneapolis
Kansas City		New York
Richmond		Philadelphia

Phishing Hits Home

Were you one of the 73 million adults who received a phishing e-mail between May 2004 and May 2005? Gartner, a leading technology research firm, estimates that nearly 2.4 million online shoppers lost money as a direct result of phishing. Do you know how to avoid being the next victim?

The e-mail message on the right was submitted by an FR employee and is a real example of a phishing e-mail. See if you can find the subtle clues that prove this message is a hoax. Check the back page for answers.

Source: www.cio.com

From: payments-messages@amazon.com
Sent: Wednesday, October 19, 2005 3:28 AM
Subject: Amazon Payments Billing Issue

Greetings from Amazon Payments .

Your bank has contacted us regarding some attempts of charges from your credit card via the Amazon system. We have reasons to believe that you changed your registration information or that someone else has unauthorized access to your Amazon account Due to recent activity, including possible unauthorized listings placed on your account, we will require a second confirmation of your identity with us In order to allow us to investigate this matter further. Your account is not suspended, but If in 48 hours after you receive this message your account is not confirmed we reserve the right to suspend your Amazon registration. Amazon is committed to assist law enforcement with any Inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.

To confirm your identity with us click here:
https://www.amazon.com/exec/obidos/flex-sign-in/ref=pd_irl_gw_r/103-3177084-7567864?opt=pa&page=recs/sign-in-secure.html

After responding to the message, we ask that you allow at least 72 hours for the case to be investigated. Emailing us before that time will result in delays. We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

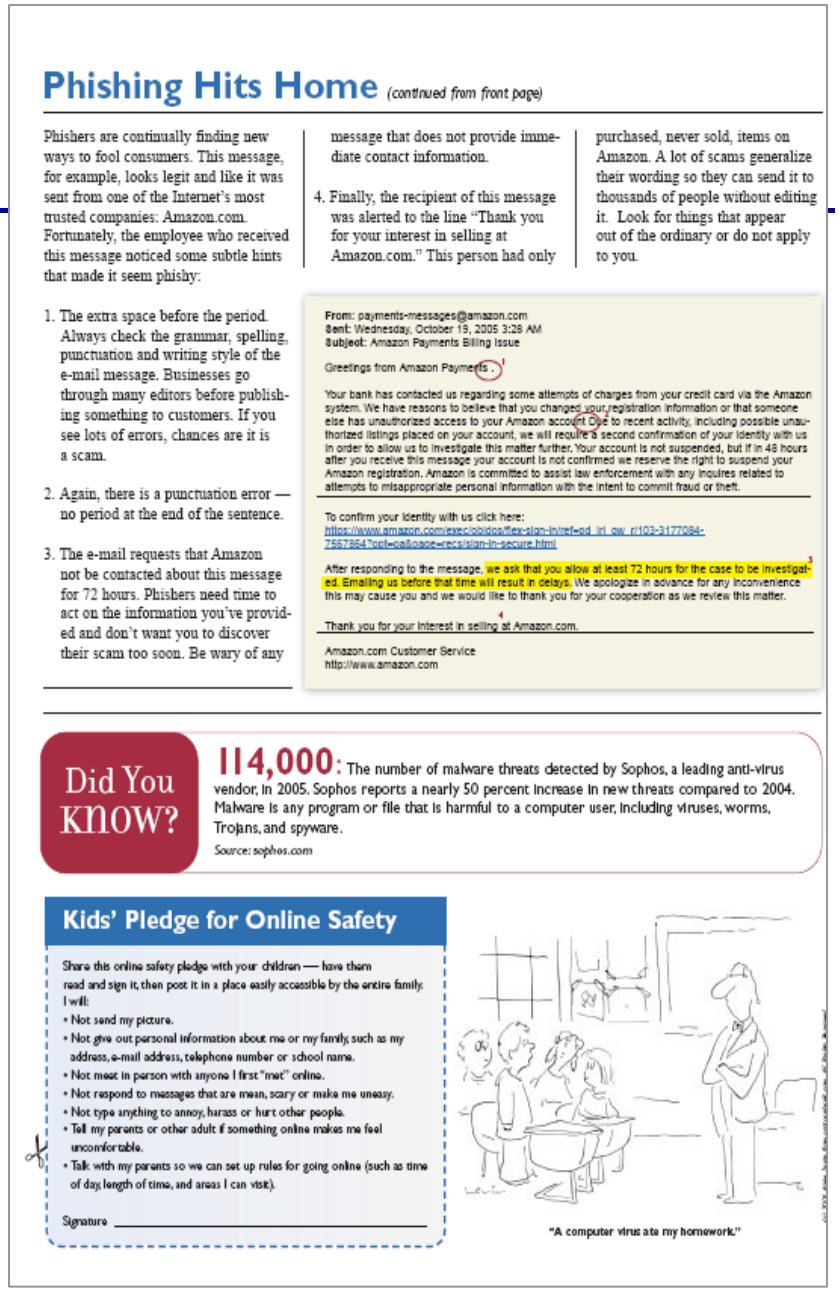
Thank you for your interest in selling at Amazon.com.

Amazon.com Customer Service
http://www.amazon.com

© Federal Reserve Bank of Richmond-2008

Newsletter

- Columns include
  - Did You Know?
  - Business Continuity Buzz
  - Fresh Facts
  - What's Bugging You?
  - On the Home Front
  - Technical Corner
  - Cartoon
  - Several Fed articles



Phishing Hits Home *(continued from front page)*

Phishers are continually finding new ways to fool consumers. This message, for example, looks legit and like it was sent from one of the Internet's most trusted companies: Amazon.com. Fortunately, the employee who received this message noticed some subtle hints that made it seem phishy:

1. The extra space before the period. Always check the grammar, spelling, punctuation and writing style of the e-mail message. Businesses go through many editors before publishing something to customers. If you see lots of errors, chances are it is a scam.
2. Again, there is a punctuation error — no period at the end of the sentence.
3. The e-mail requests that Amazon not be contacted about this message for 72 hours. Phishers need time to act on the information you've provided and don't want you to discover their scam too soon. Be wary of any message that does not provide immediate contact information.
4. Finally, the recipient of this message was alerted to the line "Thank you for your interest in selling at Amazon.com." This person had only purchased, never sold, items on Amazon. A lot of scams generalize their wording so they can send it to thousands of people without editing it. Look for things that appear out of the ordinary or do not apply to you.

From: payments-messages@amazon.com
Sent: Wednesday, October 19, 2005 3:28 AM
Subject: Amazon Payments Billing Issue

Greetings from Amazon Payments.

Your bank has contacted us regarding some attempts of charges from your credit card via the Amazon system. We have reasons to believe that you changed your registration information or that someone else has unauthorized access to your Amazon account. Due to recent activity, including possible unauthorized listings placed on your account, we will require a second confirmation of your identity with us in order to allow us to investigate this matter further. Your account is not suspended, but if in 48 hours after you receive this message your account is not confirmed we reserve the right to suspend your Amazon registration. Amazon is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.

To confirm your identity with us click here:
https://www.amazon.com/exec/obidos/flex-sign-in/ref=pd_irl_gw_r/103-3177084-7567864?opt=oa&page=recs/sign-in-secure.html

After responding to the message, we ask that you allow at least 72 hours for the case to be investigated. Emailing us before that time will result in delays. We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

Thank you for your interest in selling at Amazon.com.

Amazon.com Customer Service
http://www.amazon.com

Did You KNOW?

114,000: The number of malware threats detected by Sophos, a leading anti-virus vendor, in 2005. Sophos reports a nearly 50 percent increase in new threats compared to 2004. Malware is any program or file that is harmful to a computer user, including viruses, worms, Trojans, and spyware.

Source: sophos.com

Kids' Pledge for Online Safety

Share this online safety pledge with your children — have them read and sign it, then post it in a place easily accessible by the entire family.
I will:

- Not send my picture.
- Not give out personal information about me or my family, such as my address, e-mail address, telephone number or school name.
- Not meet in person with anyone I first "met" online.
- Not respond to messages that are mean, scary or make me uneasy.
- Not type anything to annoy, harass or hurt other people.
- Tell my parents or other adult if something online makes me feel uncomfortable.
- Talk with my parents so we can set up rules for going online (such as time of day, length of time, and areas I can visit).

Signature _____

"A computer virus ate my homework."

© Federal Reserve Bank of Richmond-2008

Internal Web site

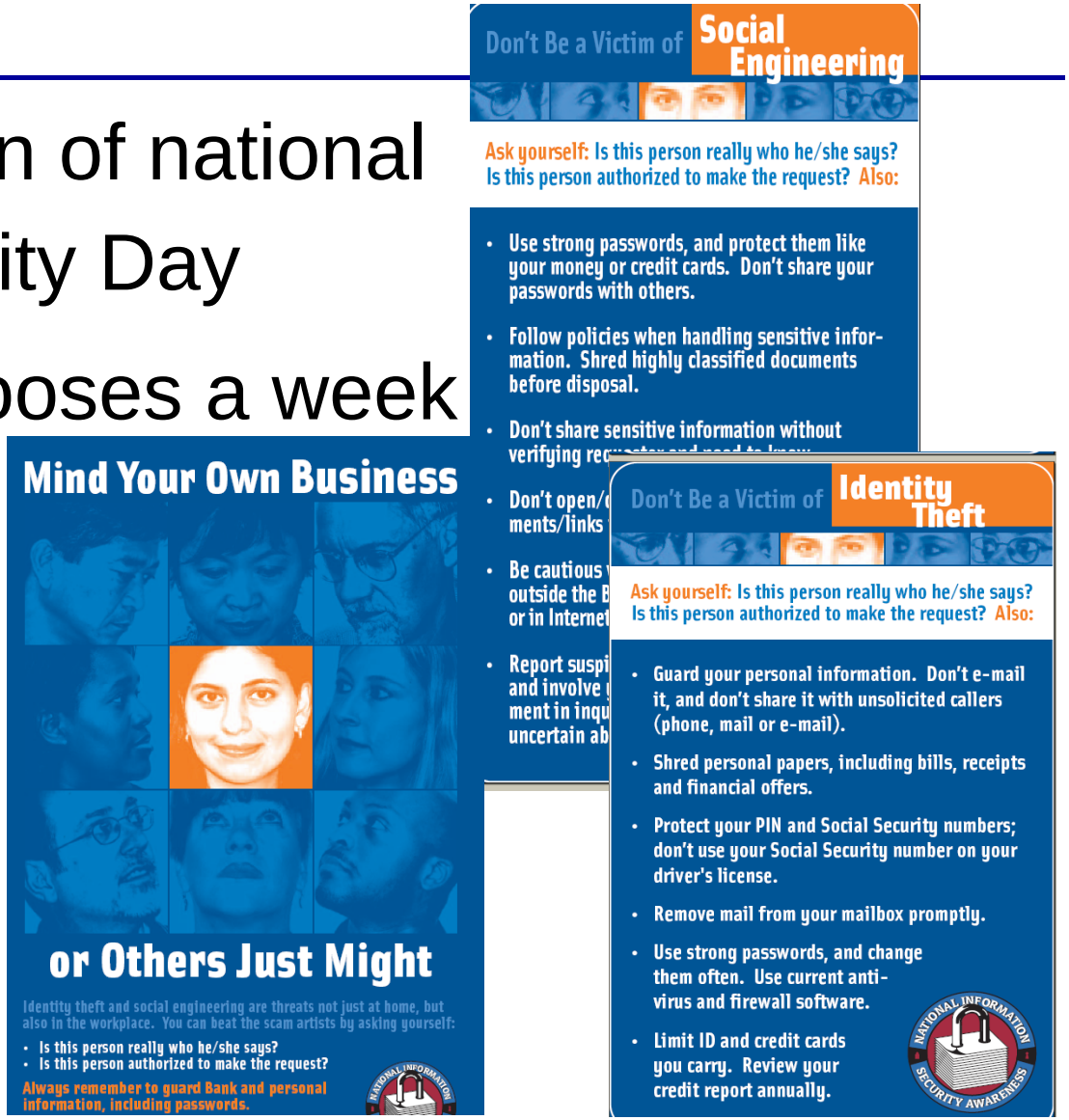
2007 FISSEA Website Winner

- IS Week
- Internet Safety
  - Kids' Safety
  - Phishing
  - Blogging
  - Malware
  - Other Pitfalls

© Federal Reserve Bank of Richmond-2008

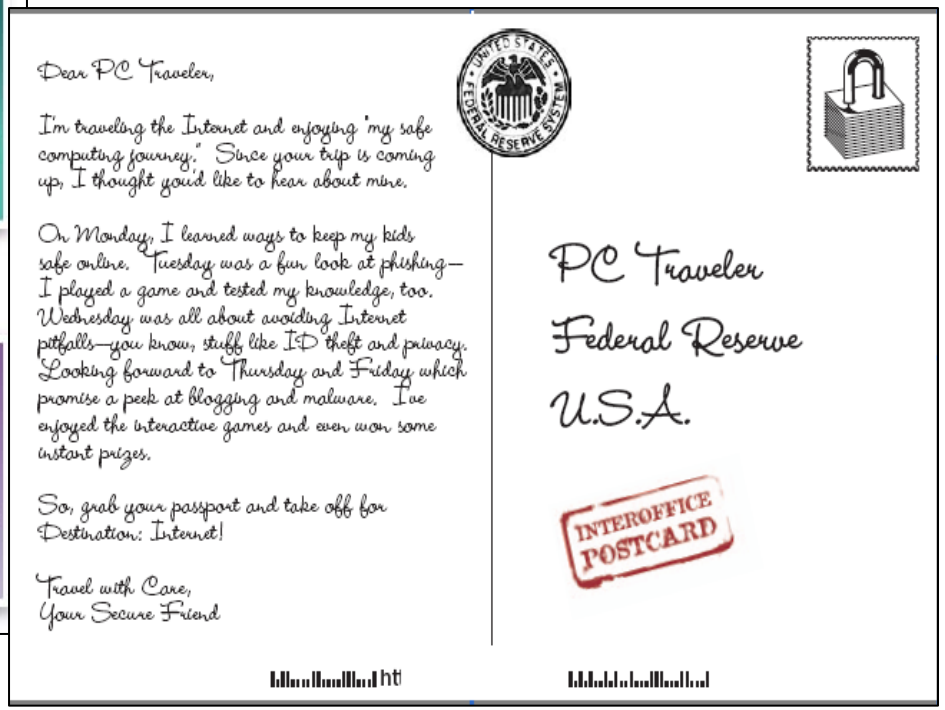
Annual Awareness Campaign

- Our interpretation of national Computer Security Day
- Each District chooses a week for campaign
- Fun
- Prizes



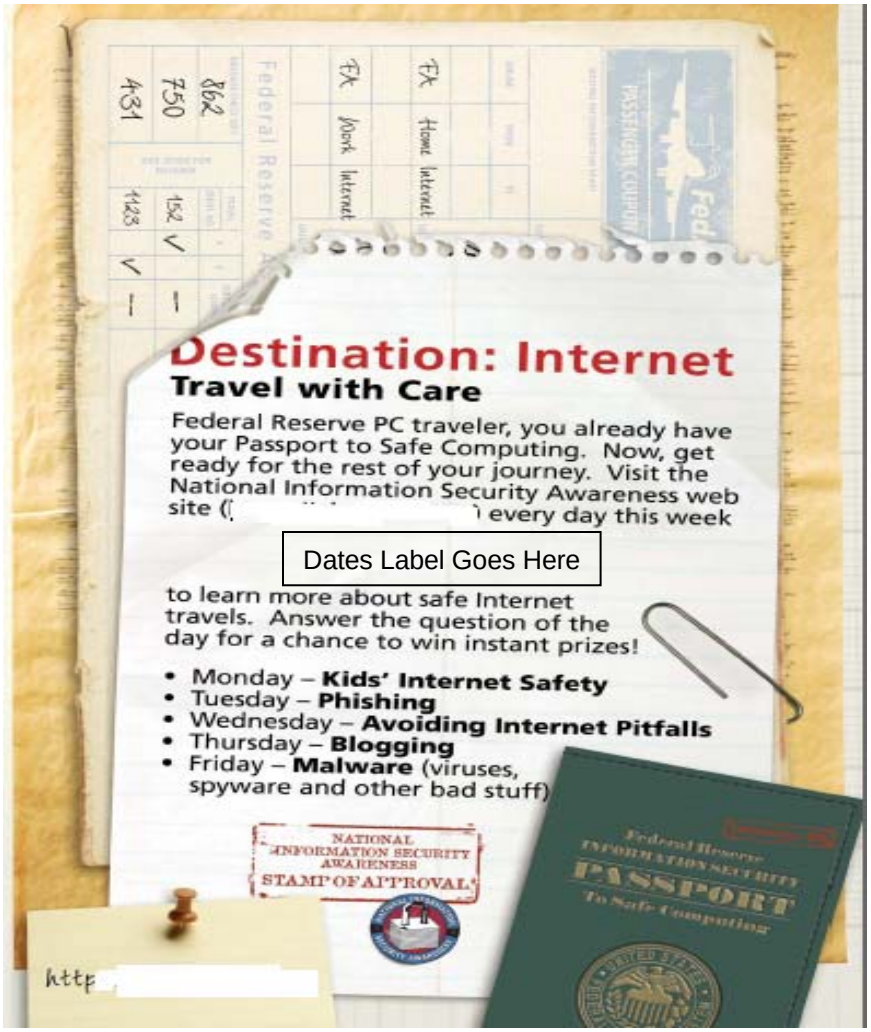
© Federal Reserve Bank of Richmond-2008

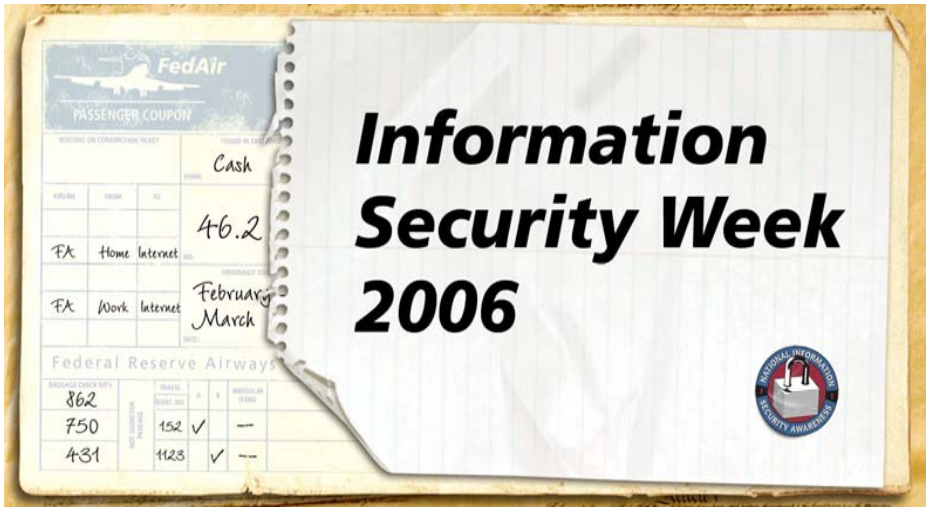
Awareness Materials



© Federal Reserve Bank of Richmond-2008

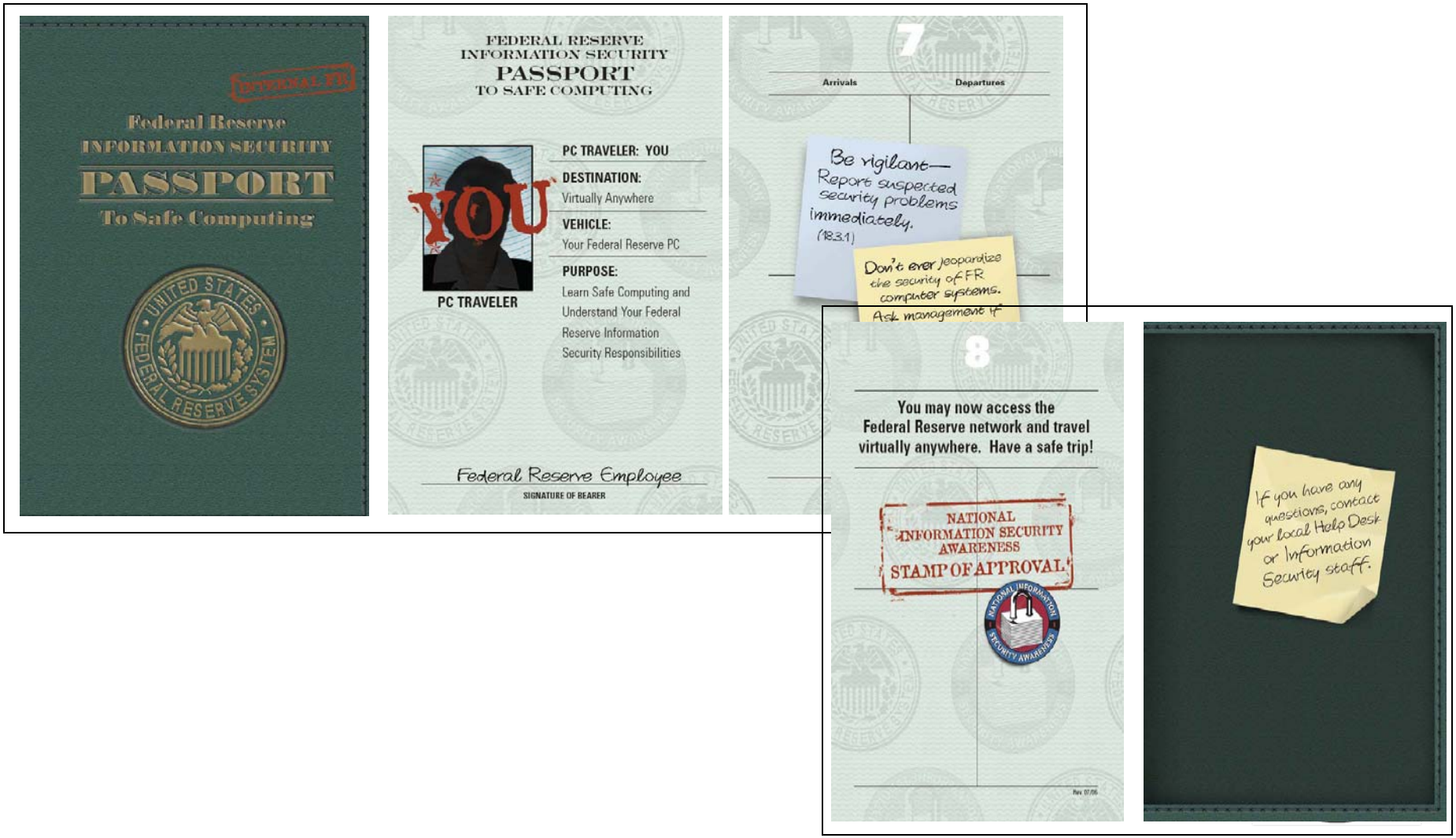
Awareness Materials





© Federal Reserve Bank of Richmond-2008

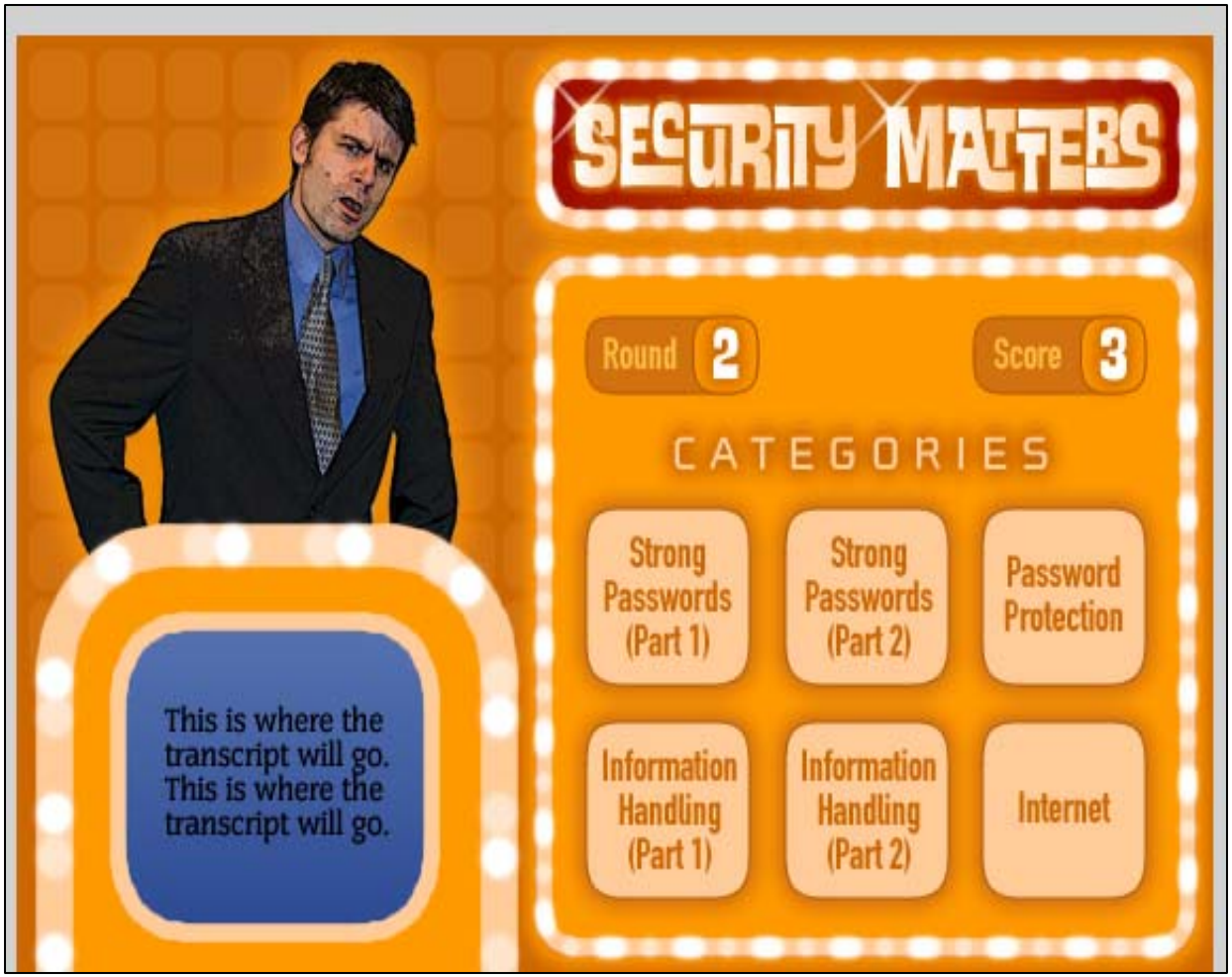
Awareness Materials



© Federal Reserve Bank of Richmond-2008

Require All-Employee Training

"Security Matters"

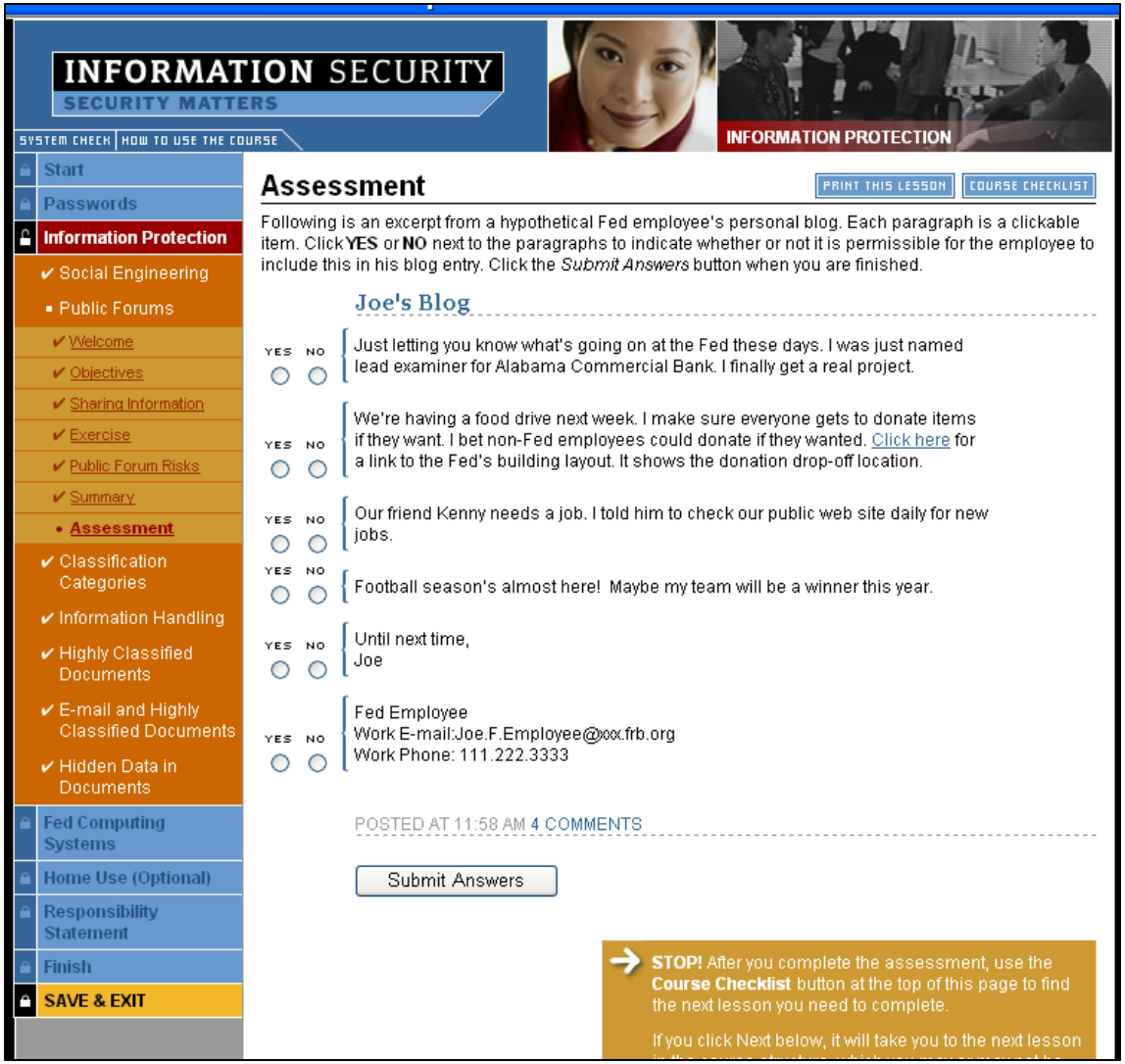


- Pretest
  - 16 Questions
  - Gameshow or Text
  - Test out or N/A
- 18 Lessons
- Runs in LMS
- Access Agreement
- Summary
- Evaluation
- Certificate

© Federal Reserve Bank of Richmond-2008

Required All-Employee Training

"Security Matters"

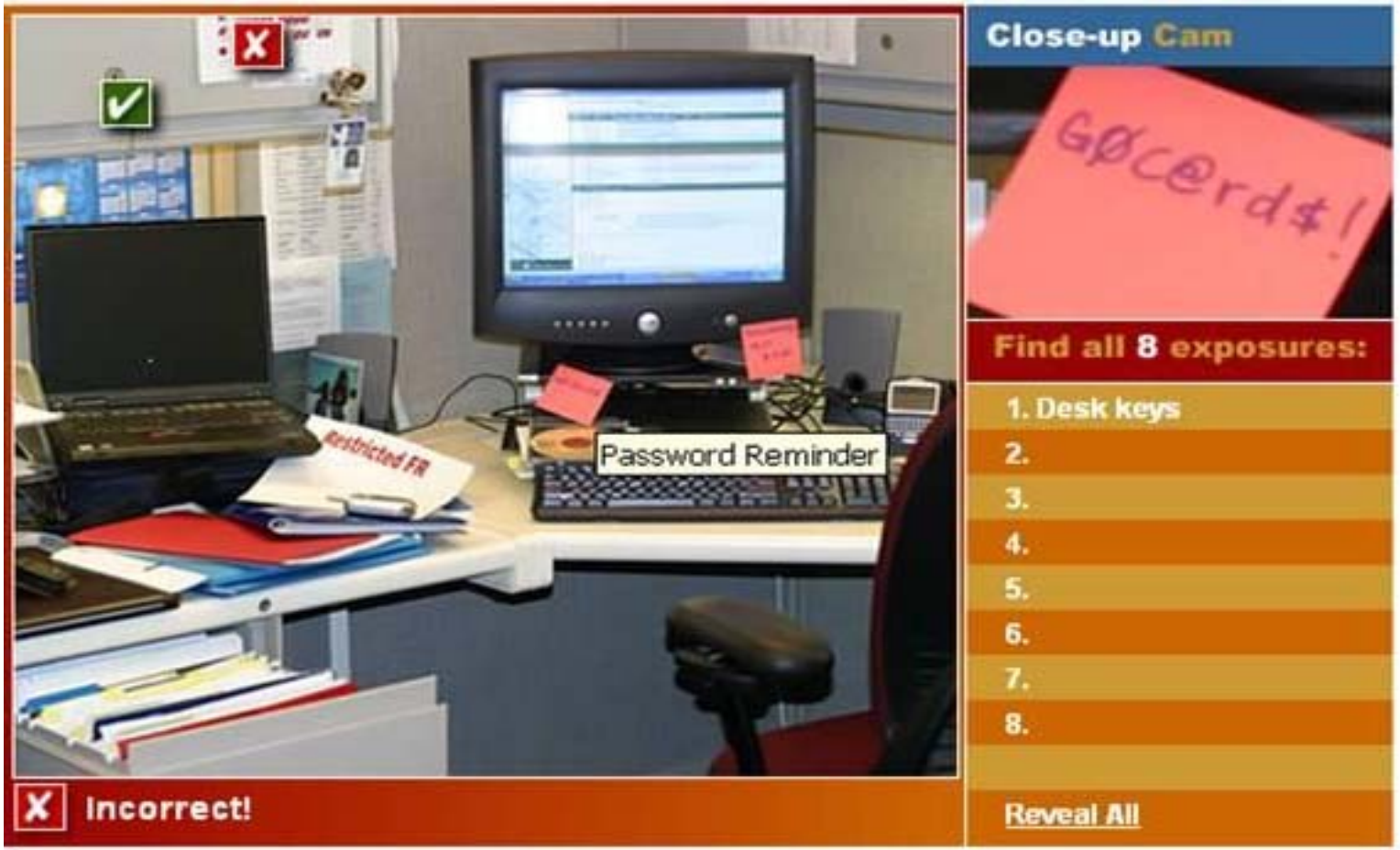


- Passwords
- Internet
- Public Forums
- E-mail
- Classified Information
- Personal Use
- Unauthorized Software
- Social Engineering
- Workstations Security
- Tokens/Smart Cards
- Mobile Devices
- Home Use…

© Federal Reserve Bank of Richmond-2008

New Employee Training

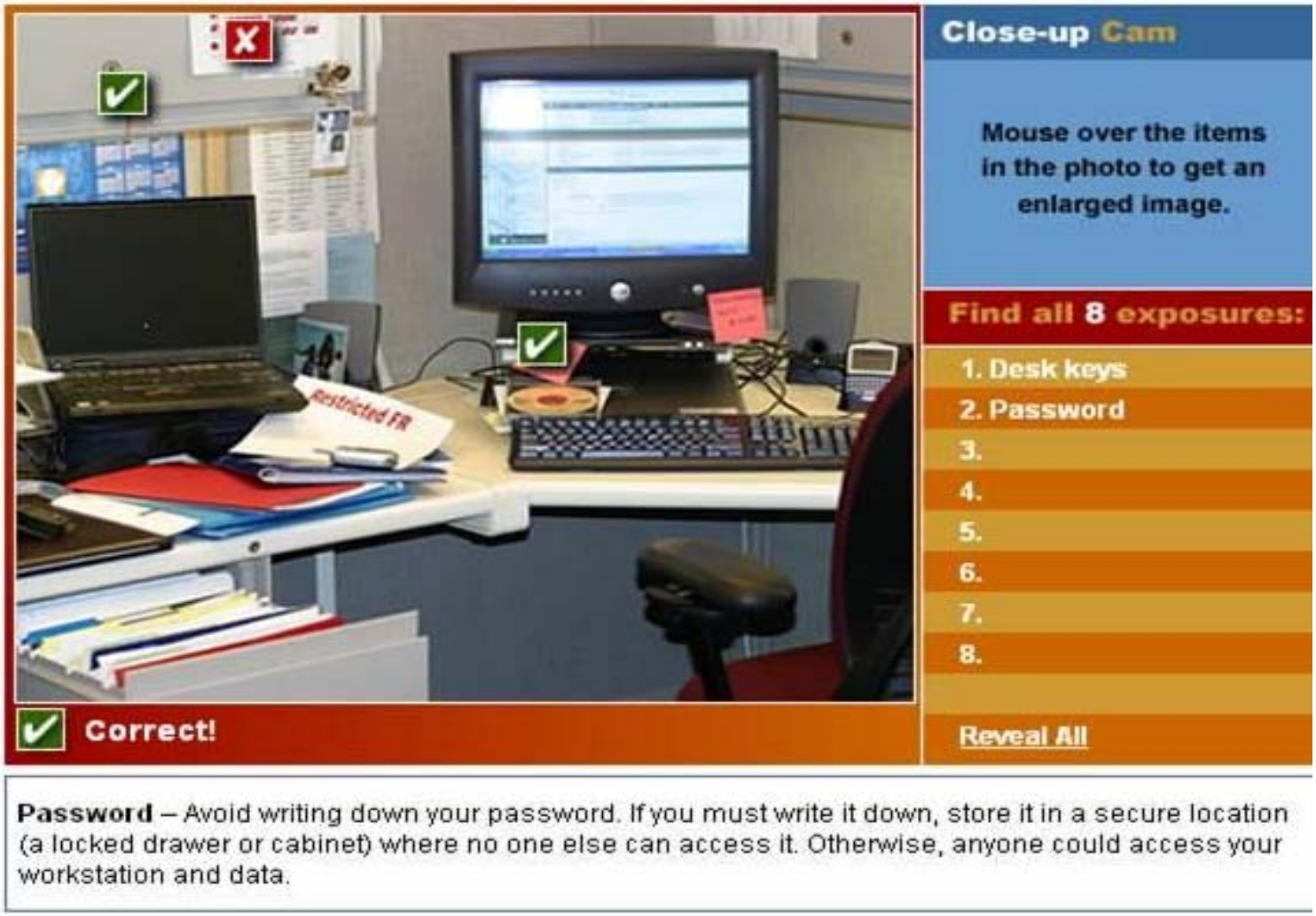
2007 FISSEA Training Exercise Winner



© Federal Reserve Bank of Richmond-2008

New Employee Training

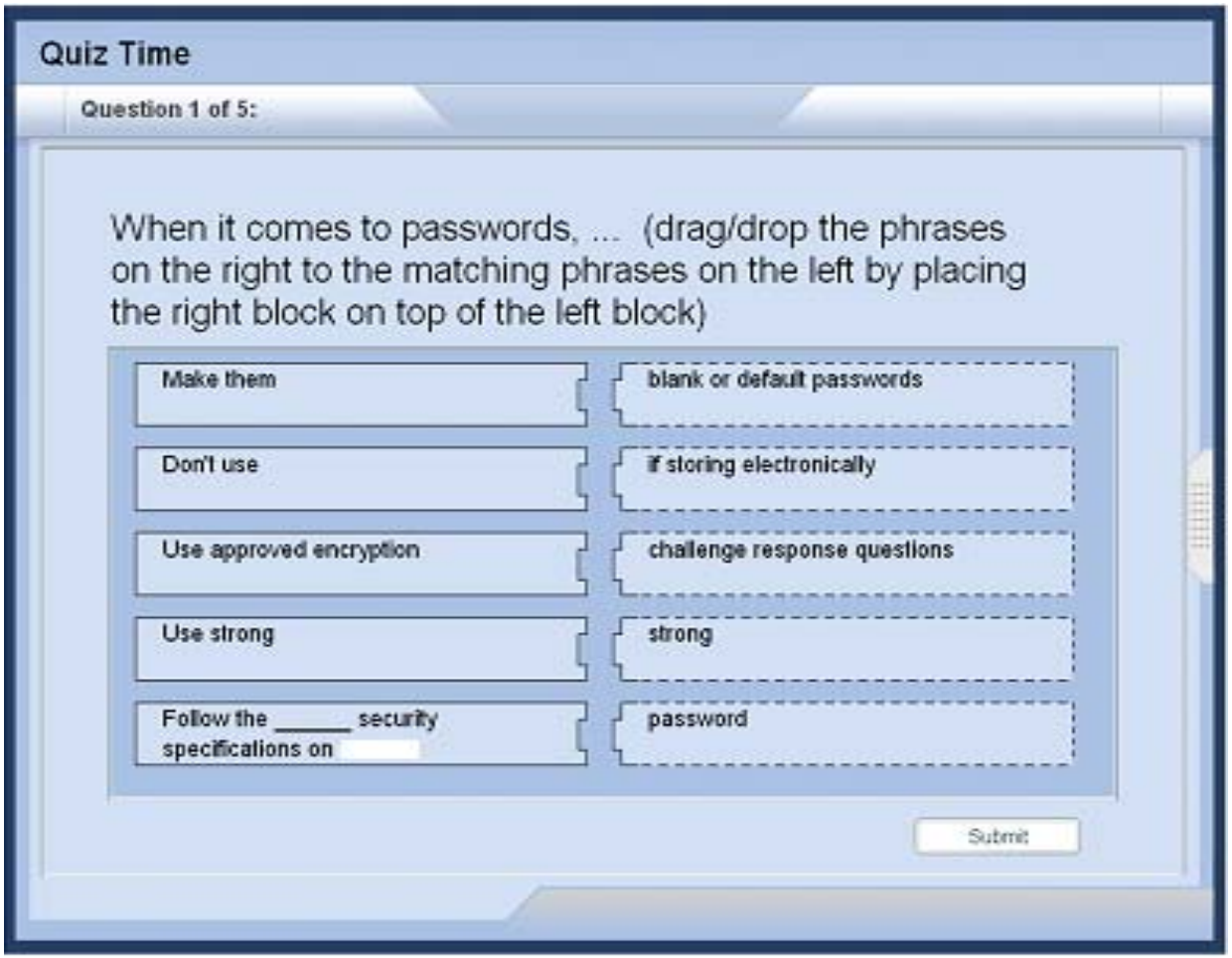
2007 FISSEA Training Exercise Winner



© Federal Reserve Bank of Richmond-2008

Targeted Training

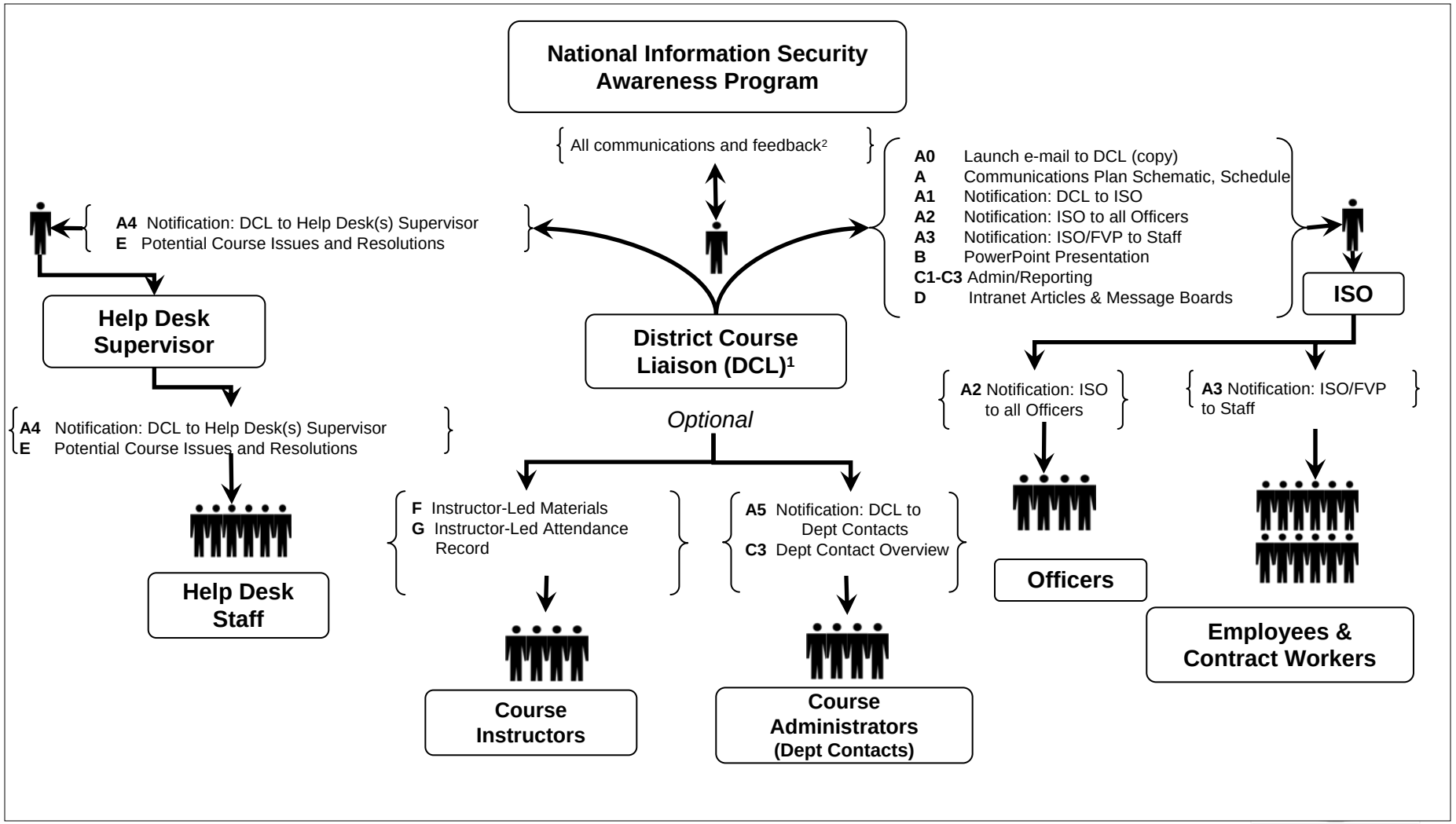
Security Awareness for Technical Staff



- For anyone in IT
- Best Practices
- OPSEC – Operational Security
- Used inexpensive, off-the shelf tool
  - PowerPoint with audio, cartoons, quizzes, links to references
  - Delivered from LMS

© Federal Reserve Bank of Richmond-2008

Communications



© Federal Reserve Bank of Richmond-2008

Training Development Lifecycle

Gather Content

Develop: Storyboards

Approvals

Design: Graphics, Interactions, Animation…

Code (Initial & Bugs)

Local Test

System Test (12x12)

Marketing, Communications, Instructions…

Editing

Reporting

Implementation

Guidance

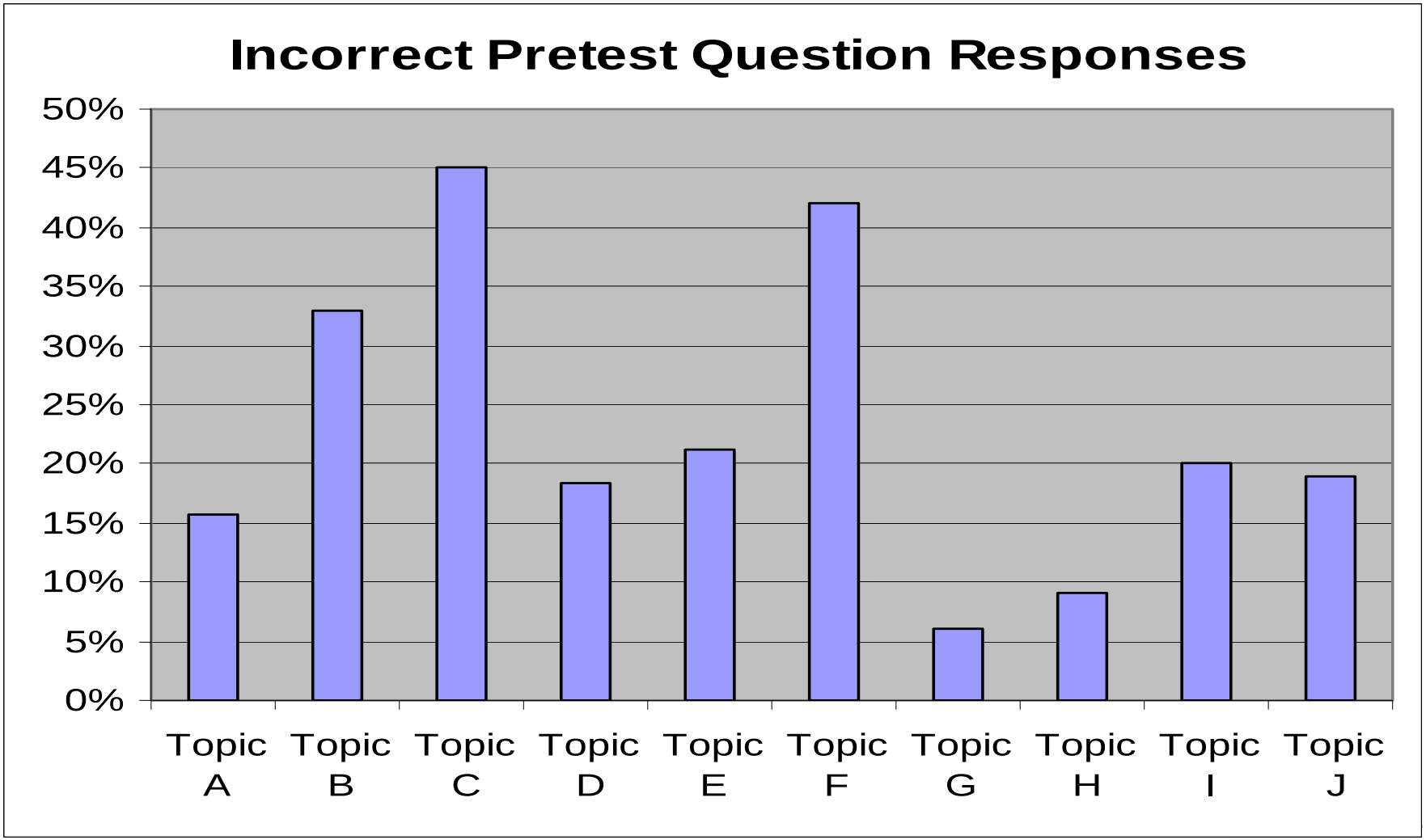
Metrics

Lessons Learned

Celebrate

© Federal Reserve Bank of Richmond-2008

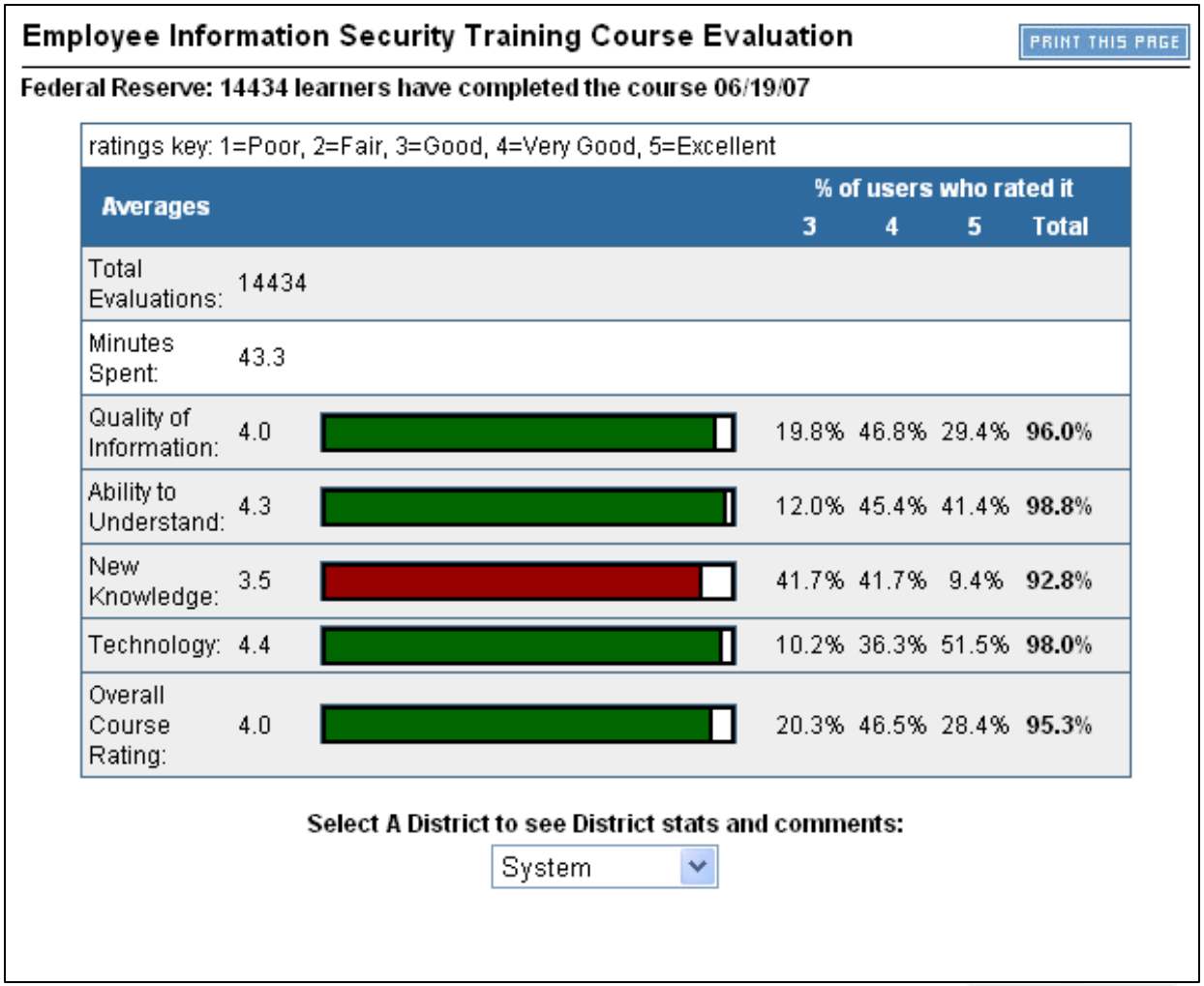
Metrics



© Federal Reserve Bank of Richmond-2008

Metrics

- Quality of course
- Ability to understand
- New knowledge
- Technology
- Overall course
- Comments
  - Liked most
  - Liked least
  - Overall



Employee Information Security Training Course Evaluation

PRINT THIS PAGE

Federal Reserve: 14434 learners have completed the course 06/19/07

ratings key: 1=Poor, 2=Fair, 3=Good, 4=Very Good, 5=Excellent

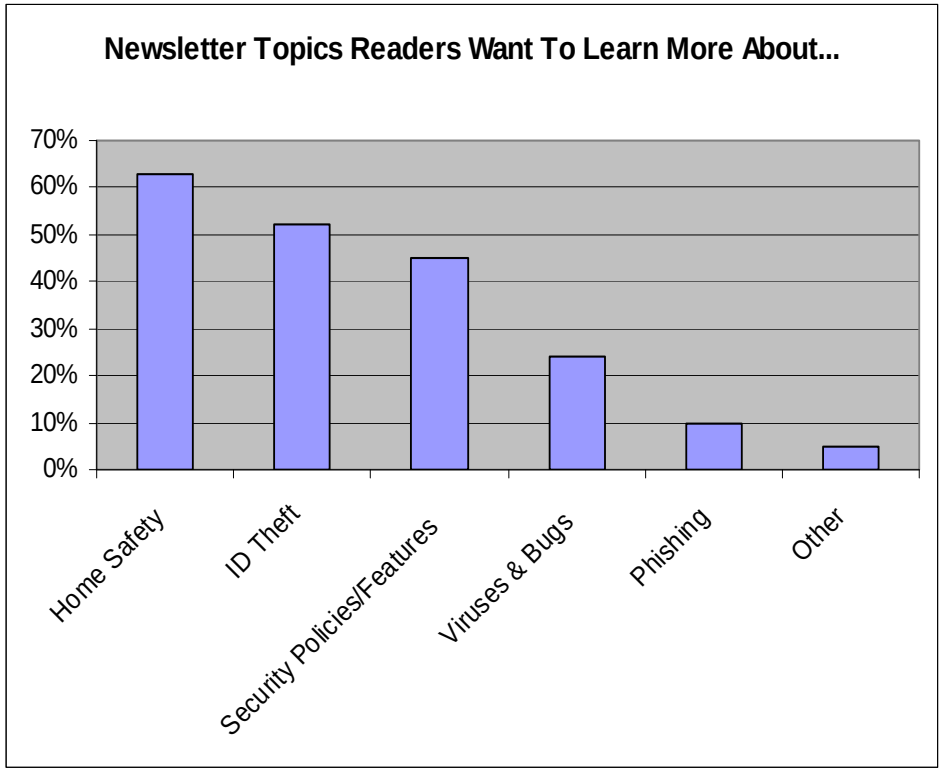
Averages			% of users who rated it 3	4	5	Total
Total Evaluations:	14434					
Minutes Spent:	43.3					
Quality of Information:	4.0		19.8%	46.8%	29.4%	**96.0%**
Ability to Understand:	4.3		12.0%	45.4%	41.4%	**98.8%**
New Knowledge:	3.5		41.7%	41.7%	9.4%	**92.8%**
Technology:	4.4		10.2%	36.3%	51.5%	**98.0%**
Overall Course Rating:	4.0		20.3%	46.5%	28.4%	**95.3%**

Select A District to see District stats and comments:

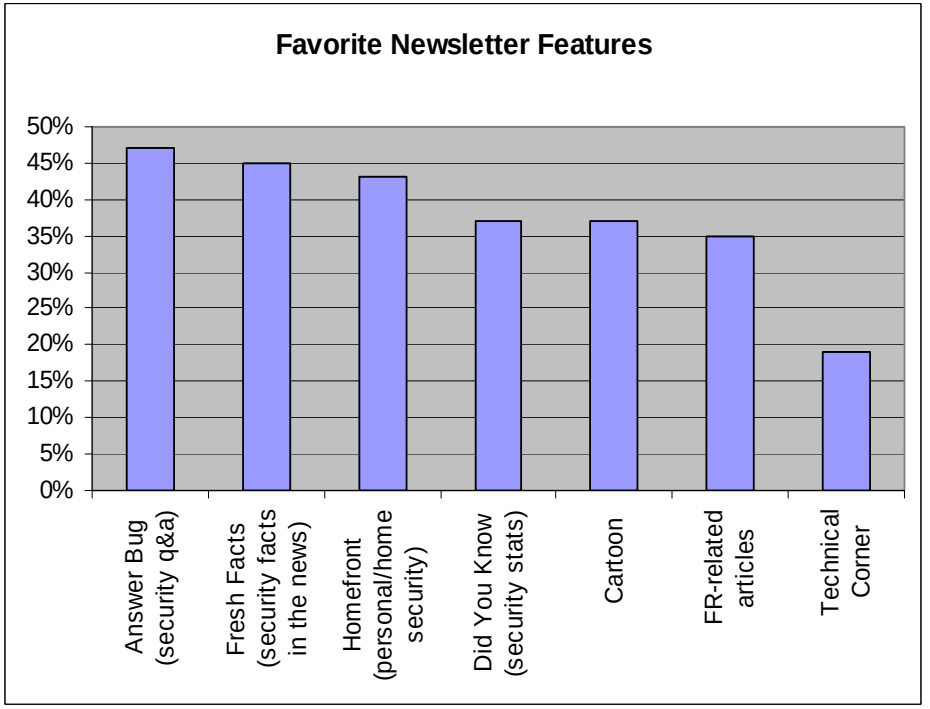
System

© Federal Reserve Bank of Richmond-2008

Metrics



- 68% prefer paper format vs. electronic



© Federal Reserve Bank of Richmond-2008

Instructor-led vs. E-learning Cost Comparison

	Instructor Led	e-learning v1	e-learning vX
Analysis	156h	80h	60h
Design	520h	200h	200h
Development	520h	200h	200h
Implementation	1,425h	1,040h	1,040h
Evaluation	260h	20h	20h
Consumption	21,850h	14,250h	14,250h
Effectiveness	60%	75%	90%
Consistency	50%	100%	100%
Cost/employee	$270.94	$104.24	$90.67

© Federal Reserve Bank of Richmond-2008

Summary

Lessons Learned

- Test, test, & test again
- Build Strong Partnerships
- Use Subject Matter Experts
- Use Security At Home
- Use Games & Freebies
  - Federal Government
  - TV Programs
- Work with Corporate Communications
- Use Well Planned, Detailed & Tested Communications
- Aim for Eighth Grade Reading Level
- Keep it Simple
- Think “Fun”

© Federal Reserve Bank of Richmond-2008

Free Resources

- US Postal Inspector General
  - www.2smrt4u.com
  - Videos (e.g., “Identity theft: How bad people get good credit”)
- www.onguardonline.gov
- www.lookstoogoodtobetrue.com
- FTC – Defend, Detect, Defer campaign
  - www.ftc.gov/bcp/edu/microsites/idtheft/index.html
  - Video & kit with speech, presentation slides, etc.
- www.getnetwise.org/
- Awareness Posters
  - www.fbi.gov/page2/july06/protect_workplace071006.htm
  - members.impulse.net/~sate/posters.html
- FISSEA – Federal Information Systems Security Educators’ Association
  - www.fissea.org
- Department of Defense Information Assurance Awareness
  - iase.disa.mil/eta/index.html

© Federal Reserve Bank of Richmond-2008

Questions

© Federal Reserve Bank of Richmond-2008