



Building a Comprehensive Security Awareness Program:

If You Build It, They Will Listen

Sherri Balderson, PMP
Federal Reserve Bank of Richmond





Key Points

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



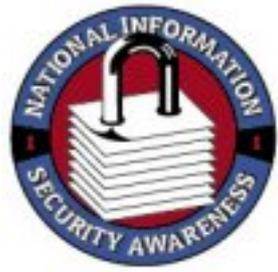


Federal Reserve Overview

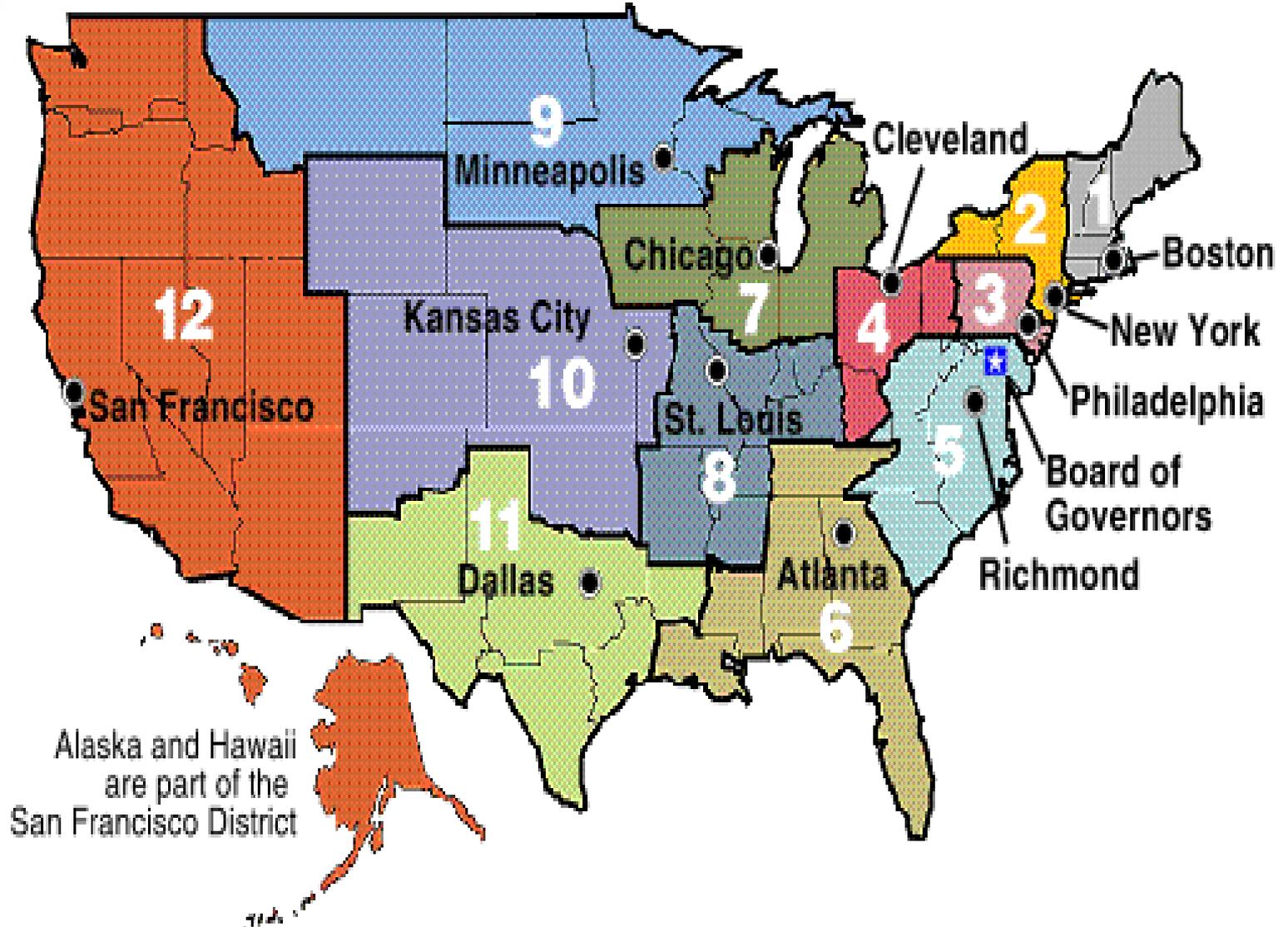
Game Show

- 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 System Structure





Decentralized Awareness Model

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





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





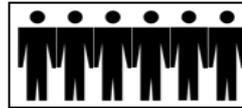
FR Awareness and Training Overview

Security Training

Specialized
(Periodic)

Training Based on Job Function and Responsibility

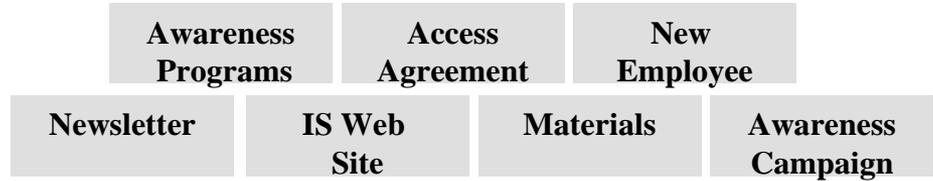
Build knowledge and skills



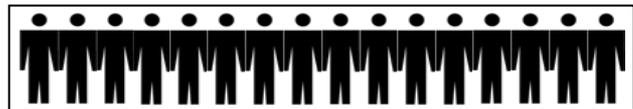
Targeted Employees and Contract Workers

Security Awareness

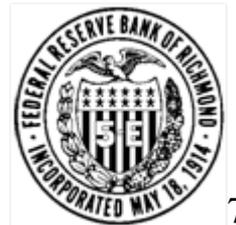
Baseline
(Ongoing)



Focus on good security practices



All Employees and Contract Workers





National Support Upper-Level Management

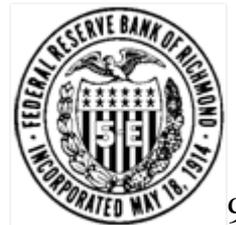
- Obtained commitment and agreement
- Led to increased funding
- Continue seeking support by constantly soliciting feedback





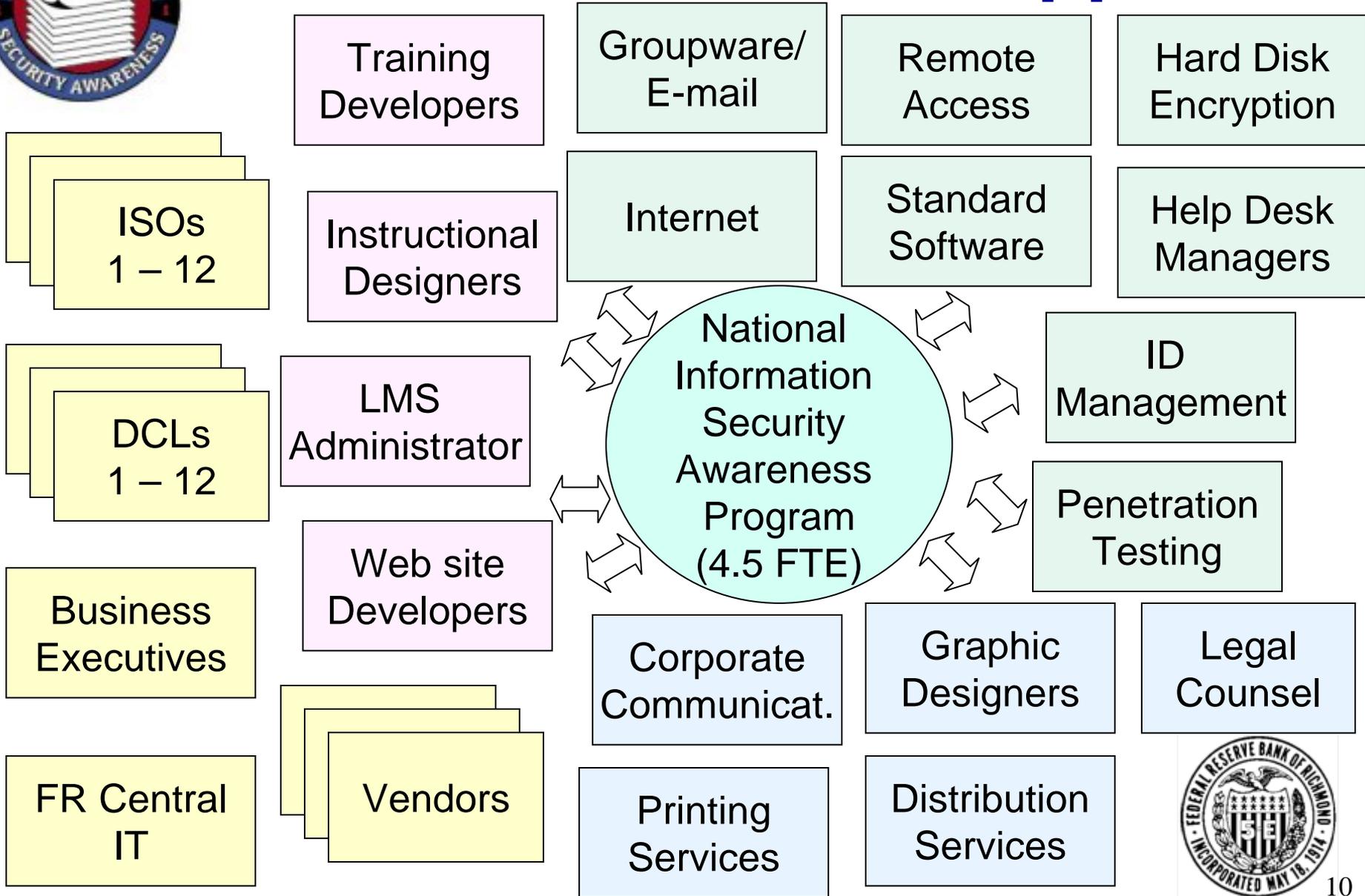
Local Support District Management

- 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





Infrastructure SMEs/Approvals





Newsletter

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

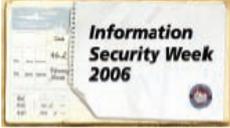
WINTER 2006

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://misap.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.ciso.com

From: payments-messages@amazon.com
Sent: Wednesday, October 15, 2006 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 inquiries 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/sec-lobos/rev-sion-intreford_it_gw_r1193-3177284-7587864?ref=oa&age=eca&sr=on-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>



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 inquiries 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/fix-pan-href=od_ri_ov_r/103-3177084-7567864/101ea0a0ae-ecce/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."



Internal Web site

2007 FISSEA Website Winner

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

The screenshot shows the website's header with the logo and the title "National Information Security Awareness" with the subtitle "News, Tips and Resources for Federal Reserve Employees". The main content area is divided into several sections:

- Home**: A vertical sidebar menu with red buttons for "Home", "About Us", "General Information", "FAQs", "News & Facts", "Training & Initiatives", and "Resources".
- What's New**: A section titled "2006/2007 Information Security Calendar" with a small image of a hand pointing to a calendar. Below it is a link to the "Security Bits & Bytes 4th Quarter Issue" and a list of articles: "Who Are You... Really? (Identity Proofing)", "Did You Know?", "Fresh Facts - Voice+Phishing=Vishing", "Cartoon", "Technical Corner - Securing Your Home Wireless Network", "What's Bugging You?", "Old Cell Phones, New Problems", and "The Better Shredder".
- Technical Staff Training**: A section with a heading "Technical Staff Training" and a paragraph: "This information security awareness training, which takes about 30 minutes to complete, is aimed at technical staff in IT and other departments throughout the Federal Reserve." Below it is a link: "Click here to access the training".
- Security Extras**: Two promotional boxes for "ID THEFT FACEOFF" and "ONLINE LINEUP", each with a "Test Your Knowledge, Click to Play!" button.
- Security Tips**: A section with a heading "Security Tips" and a box titled "Don't Take The Bait!" with a small image of a fish. Below it is a link: "Click here for an 11x17 .pdf color poster of tips for preventing phishing attacks." and a paragraph: "Spam, chain letters and hoaxes could be considered a form of 'phishing' through the use of e-mail. Don't get hooked. Don't view, open, edit or forward unexpected or questionable attachments."
- District Specific**: A section with a heading "District Specific" and two dropdown menus: "Contacts By District" and "Local IS Web Sites".



Annual Awareness Campaign

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



Ask yourself: Is this person really who he/she says?
Is this person authorized to make the request? **Also:**

- Use strong passwords, and protect them like your money or credit cards. Don't share your passwords with others.
- Follow policies when handling sensitive information. Shred highly classified documents before disposal.
- Don't share sensitive information without verifying requester and need to know.

Mind Your Own Business

or Others Just Might

Identity theft and social engineering are threats not just at home, but also in the workplace. You can beat the scam artists by asking yourself:

- Is this person really who he/she says?
- Is this person authorized to make the request?

Always remember to guard Bank and personal information, including passwords.



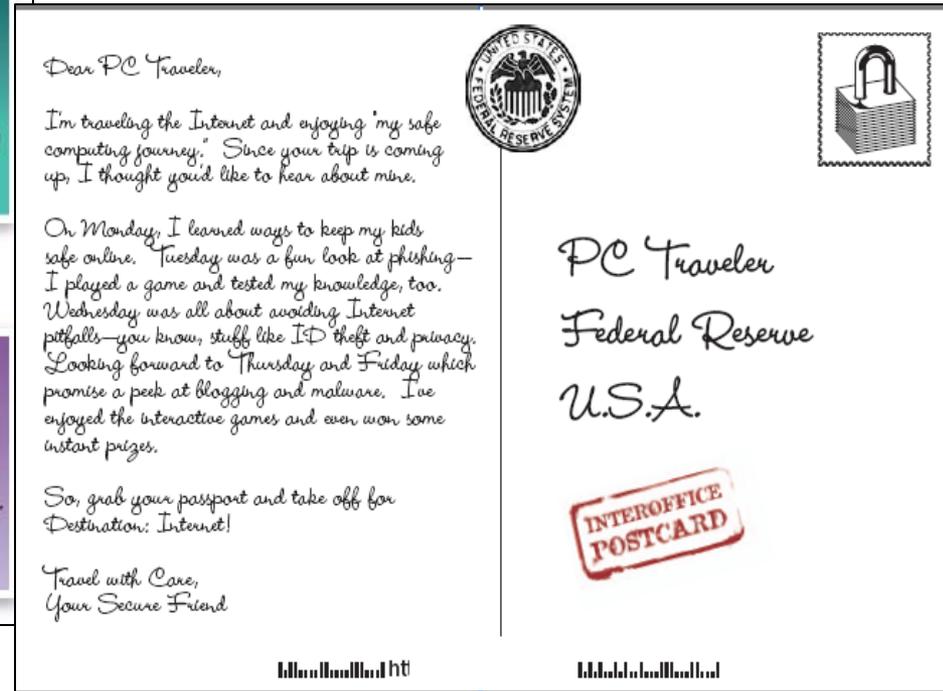
Ask yourself: Is this person really who he/she says?
Is this person authorized to make the request? **Also:**

- Guard your personal information. Don't e-mail it, and don't share it with unsolicited callers (phone, mail or e-mail).
- Shred personal papers, including bills, receipts and financial offers.
- Protect your PIN and Social Security numbers; don't use your Social Security number on your driver's license.
- Remove mail from your mailbox promptly.
- Use strong passwords, and change them often. Use current anti-virus and firewall software.
- Limit ID and credit cards you carry. Review your credit report annually.





Awareness Materials





Awareness Materials

Destination: Internet Travel with Care

Federal Reserve PC traveler, you already have your Passport to Safe Computing. Now, get ready for the rest of your journey. Visit the National Information Security Awareness web site ([http://www.frb.org/isa](#)) every day this week

Dates Label Goes Here

to learn more about safe Internet travels. Answer the question of the day for a chance to win instant prizes!

- Monday – **Kids' Internet Safety**
- Tuesday – **Phishing**
- Wednesday – **Avoiding Internet Pitfalls**
- Thursday – **Blogging**
- Friday – **Malware** (viruses, spyware and other bad stuff)

NATIONAL INFORMATION SECURITY AWARENESS STAMP OF APPROVAL

Federal Reserve INFORMATION SECURITY PASSPORT To Safe Computing

http: _____

Information Security Week 2006

FedAir PASSENGER COUPON

BOOKING ON CONFORMING TICKET

FA Home Internet 46.2

FA Work Internet February March

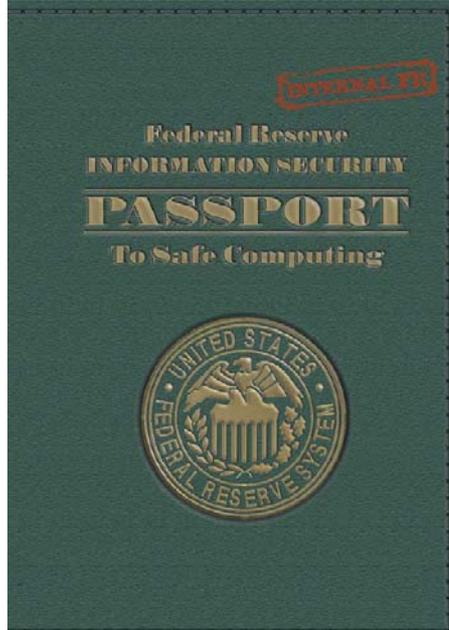
Federal Reserve Airways

PACKAGE CODE KEY	FARE	CLASS	A	REMARKS
862				
750	152	✓	---	
431	1123	✓	---	





Awareness Materials



FEDERAL RESERVE
INFORMATION SECURITY
PASSPORT
TO SAFE COMPUTING



PC TRAVELER

PC TRAVELER: YOU

DESTINATION:
Virtually Anywhere

VEHICLE:
Your Federal Reserve PC

PURPOSE:
Learn Safe Computing and Understand Your Federal Reserve Information Security Responsibilities

Federal Reserve Employee
SIGNATURE OF BEARER

7

Arrivals	Departures

Be vigilant—
Report suspected security problems immediately.
(183.1)

Don't ever jeopardize the security of FR computer systems.
Ask management if

8

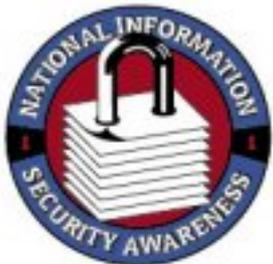
You may now access the Federal Reserve network and travel virtually anywhere. Have a safe trip!

NATIONAL INFORMATION SECURITY AWARENESS STAMP OF APPROVAL

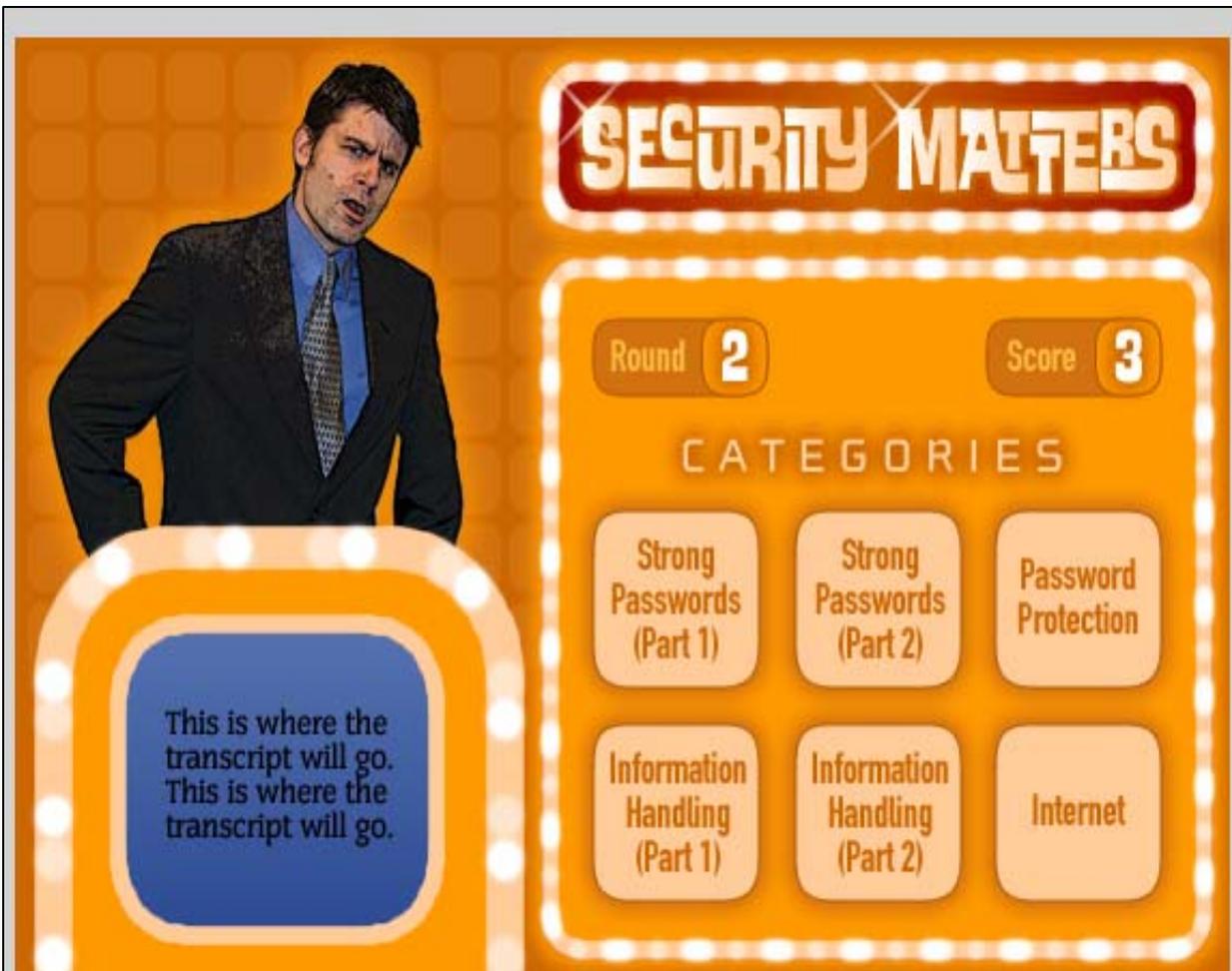


Nov 07/08





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





Required All-Employee Training “Security Matters”

INFORMATION SECURITY

SECURITY MATTERS

SYSTEM CHECK | HOW TO USE THE COURSE

- Start
- Passwords
- Information Protection**
 - Social Engineering
 - Public Forums
 - Welcome
 - Objectives
 - Sharing Information
 - Exercise
 - Public Forum Risks
 - Summary
 - Assessment**
 - Classification Categories
 - Information Handling
 - Highly Classified Documents
 - E-mail and Highly Classified Documents
 - Hidden Data in Documents
 - Fed Computing Systems
 - Home Use (Optional)
 - Responsibility Statement
 - Finish
 - SAVE & EXIT

Assessment

Following is an excerpt from a hypothetical Fed employee's personal blog. Each paragraph is a clickable item. Click **YES** or **NO** next to the paragraphs to indicate whether or not it is permissible for the employee to include this in his blog entry. Click the *Submit Answers* button when you are finished.

Joe's Blog

YES NO Just letting you know what's going on at the Fed these days. I was just named lead examiner for Alabama Commercial Bank. I finally get a real project.

YES NO We're having a food drive next week. I make sure everyone gets to donate items if they want. I bet non-Fed employees could donate if they wanted. [Click here](#) for a link to the Fed's building layout. It shows the donation drop-off location.

YES NO Our friend Kenny needs a job. I told him to check our public web site daily for new jobs.

YES NO Football season's almost here! Maybe my team will be a winner this year.

YES NO Until next time,
Joe

YES NO Fed Employee
Work E-mail: Joe.F.Employee@xxx.frb.org
Work Phone: 111.222.3333

POSTED AT 11:58 AM 4 COMMENTS

Submit Answers

→ **STOP!** After you complete the assessment, use the **Course Checklist** button at the top of this page to find the next lesson you need to complete.

If you click Next below, it will take you to the next lesson

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



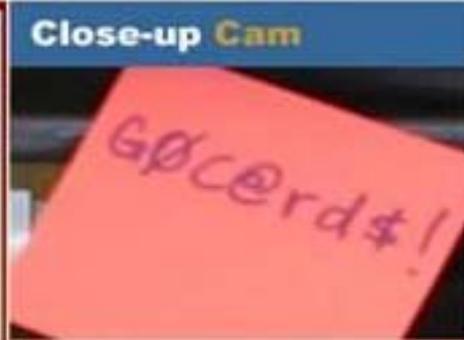


New Employee Training

2007 FISSEA Training Exercise Winner



X Incorrect!



Find all 8 exposures:

1. Desk keys
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

[Reveal All](#)

Baseball schedule – This is not a security risk. It's just a baseball schedule.





New Employee Training

2007 FISSEA Training Exercise Winner



Correct!

Close-up Cam

Mouse over the items in the photo to get an enlarged image.

Find all 8 exposures:

1. Desk keys
2. Password
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.

[Reveal All](#)

Password – Avoid writing down your password. If you must write it down, store it in a secure location (a locked drawer or cabinet) where no one else can access it. Otherwise, anyone could access your workstation and data.





Targeted Training

Security Awareness for Technical Staff

Quiz Time

Question 1 of 5:

When it comes to passwords, ... (drag/drop the phrases on the right to the matching phrases on the left by placing the right block on top of the left block)

Make them	blank or default passwords
Don't use	if storing electronically
Use approved encryption	challenge response questions
Use strong	strong
Follow the _____ security specifications on _____	password

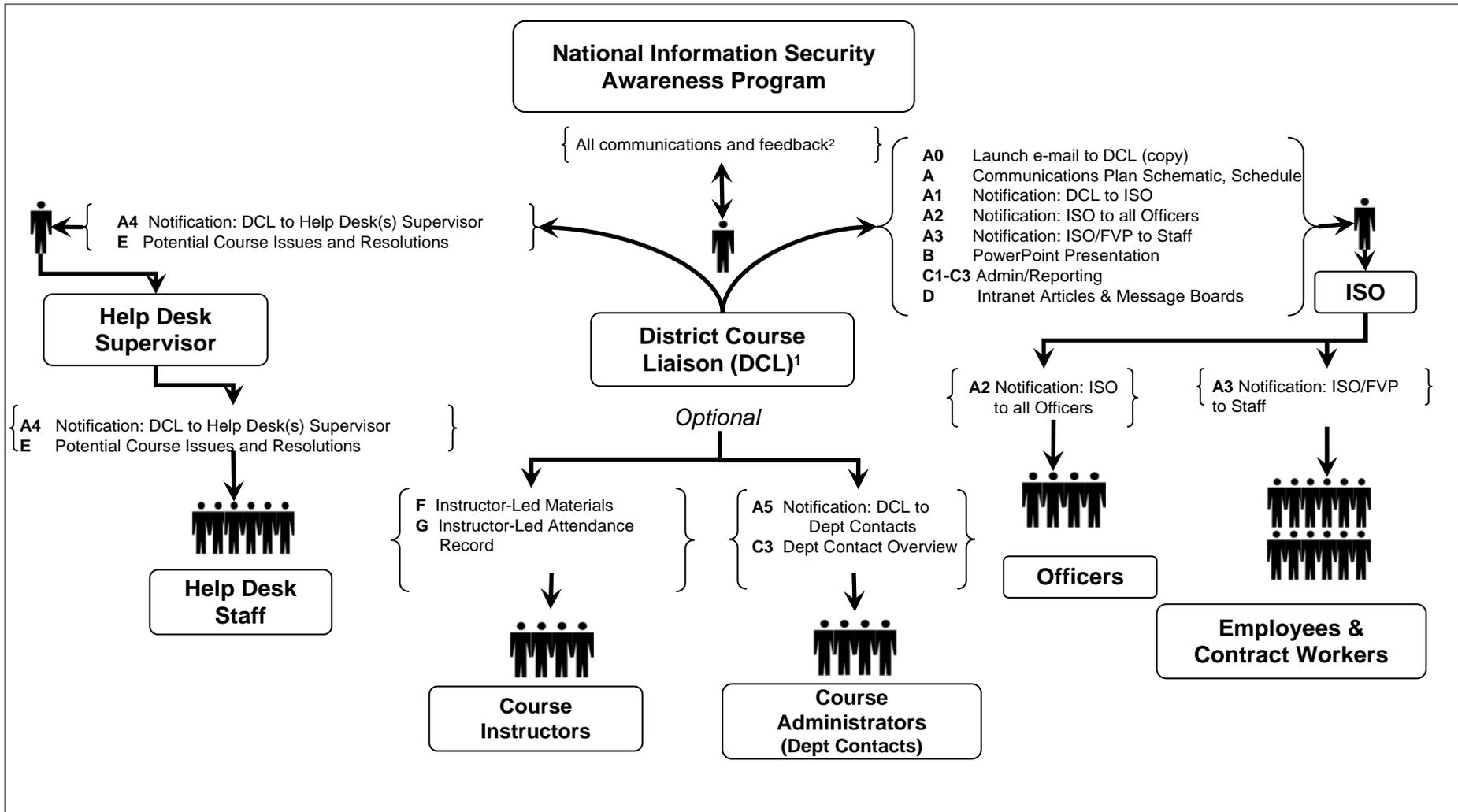
Submit

- 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



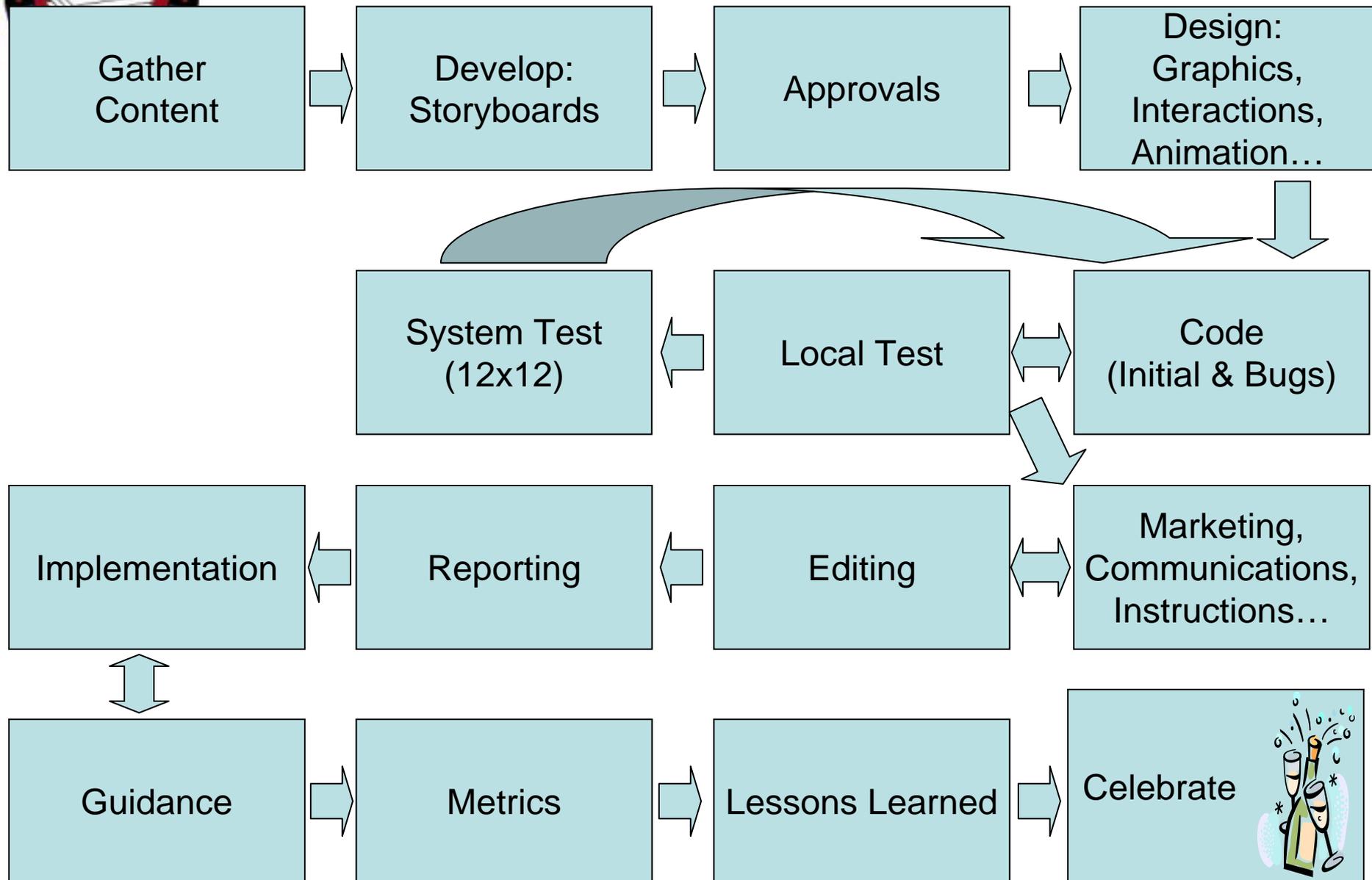


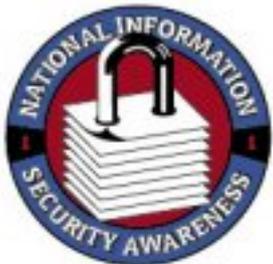
Communications





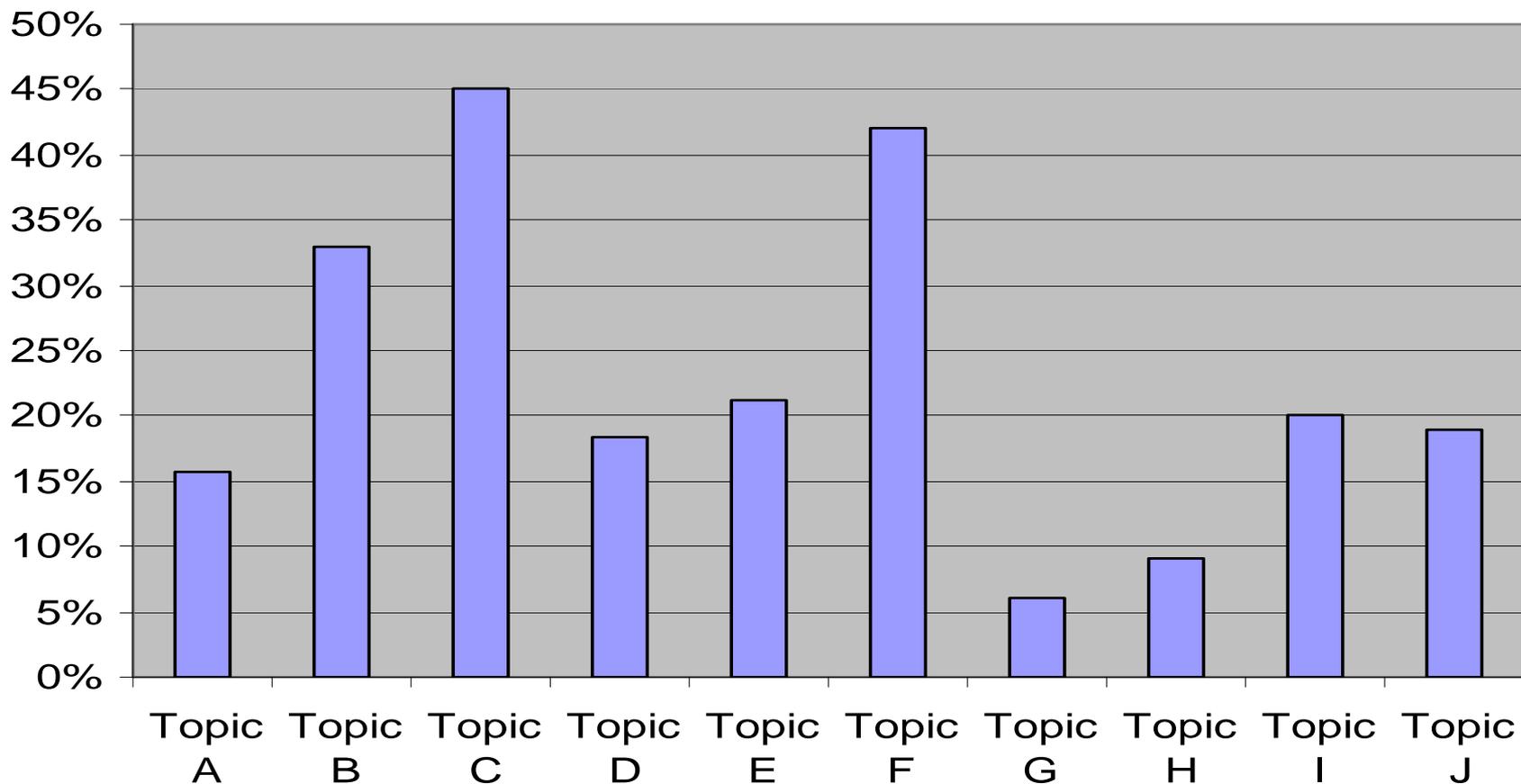
Training Development Lifecycle





Metrics

Incorrect Pretest Question Responses





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%

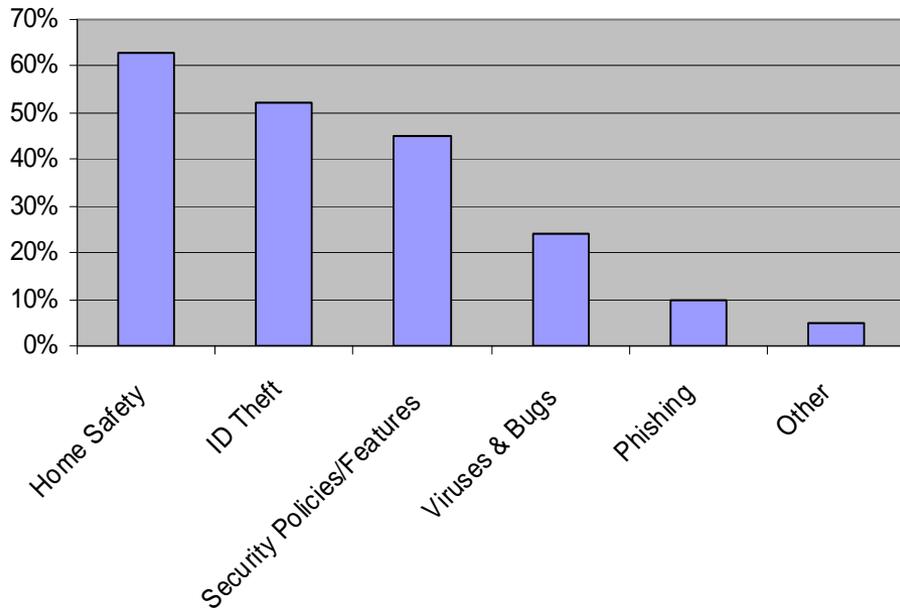
Select A District to see District stats and comments:

System



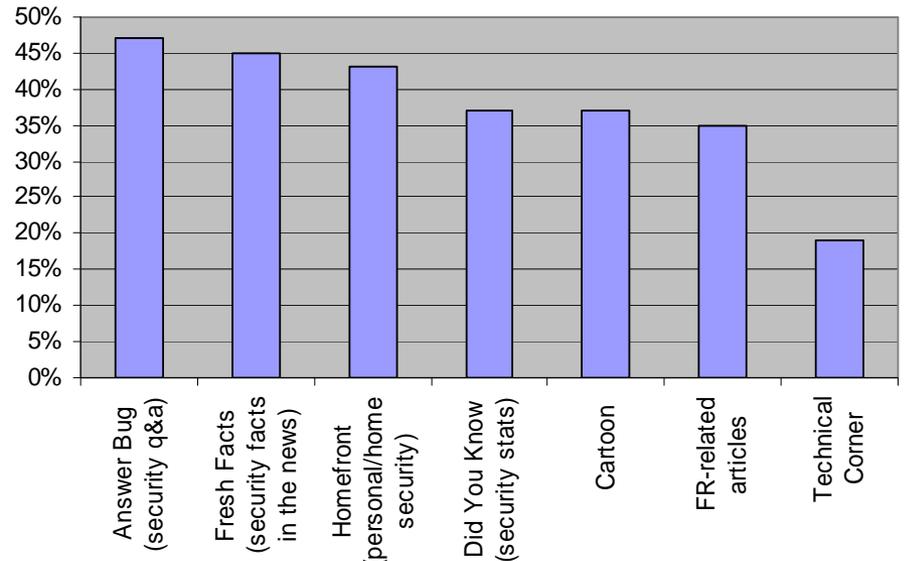
Metrics

Newsletter Topics Readers Want To Learn More About...



- 68% prefer paper format vs. electronic

Favorite Newsletter Features





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





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”





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





Questions

