FISSEA Contest
Entry Form

Name of submitter: Rian Campbell

Organization: Federal Reserve Bank of Richmond

Email: Rian.Campbell@rich.frb.org

Type of entry: Website

Title of Entry: National Information Security Awareness Internal Website

Description of Entry: We maintain this internal web site for all 21,000 Federal Reserve employees around the country. Our home page is kept up to date with current information security news and internal events/initiatives, and we provide informational pages, links, games, contact information, etc., on the site to serve as a "one stop shop" for information security awareness in the Federal Reserve.

National Information Security Awareness

News, Tips and Resources for Federal Reserve Employees

Navigation

- Home
- About Us
  - General Information
  - FAQs
- News & Facts
  - Current *Security Bits & Bytes*
  - 2006/2007 Calendar
  - Newsletter Archives
  - Shannon's Story: from *Bits & Bytes*
  - Lori Lee-Savage (ID Theft)
  - Security Cartoon
- Training & Initiatives
  - Technical Staff Training
  - IS Week 2006
  - Responsibility Statement
  - All-Employee Training 2005
  - New Employee Training
- Resources
  - Virus Hoax Site
  - Info Security Officers
  - Handling Classified Information
  - *Passport to Safe Computing*
  - Password Strength Tester

What's New

2006/2007 Information Security Calendar

Access your monthly information security calendar, complete with all Federal Reserve holidays and paydays, and a security reminder for every month!

Security Bits & Bytes 4th Quarter Issue

Click here to read the latest Information Security Awareness newsletter for Federal Reserve Employees. In this issue:

- 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
- The Better Shredder

Technical Staff Training

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.

Be on the lookout for more information on the rollout of this course in your district!

Click here to access the training

Security Extras

Test Your Knowledge, Click to Play!

ID THEFT FACEOFF

ONLINE LINEUP

Test Your Knowledge, Click to Play!

Security Tips

Don't Take The Bait!

(Click here for an 11x17 .pdf color poster of tips for preventing phishing attacks.)

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

Contacts By District

Local IS Web Sites

This is our home page. Our IS Week 2006 awareness campaign concentrated on Internet topics including: kids' safety, phishing, blogging, malware, and other Internet pitfalls. The following pages show that content which includes interactive games.

Keep Kids Safe Online

Did You Know?
11 years old - average age of a child when he or she is first exposed to pornography on the Internet

Links:
- SafeKids.com
- Protect Your Family
- Safe Surfing
- Be Safe Online
- Kids' Safety Tips

Security Bits & Bytes Articles
(these .pdf files take a bit longer to load; you'll need to scroll to the article):
- Print Shannon's Story
- Kids' Pledge

Test Your Kid Safety Know How with these Quizzes:
- Child Safety (ages 2-12)
- Child Safety (ages 13-17)

Get Your Web License!

Shannon's Story - an Important Safety Message

Shannon could hear the footsteps behind her as she walked home. The thought of being followed made her heart beat faster. "You're being silly," she told herself, "no one is following you." To be safe, she began to walk faster. But the footsteps kept up with her pace. She was afraid to look back, and she was glad she was almost home.

Shannon said a quick prayer, "God, please get me home safe." She saw the porch light burning and ran the rest of the way to her house.

Don't Become Phish Bait

Did You Know?
5.7 Billion - number of phishing e-mails sent each month. (APWG)

Links:
- Onguard Online - Phishing
- Anti-Phishing Workgroup
- phishinginfo.org
- Field Guide to Phishing

Security Bits & Bytes Articles
(these .pdf files take a bit longer to load; you'll need to scroll to the article):
- Phishing Hits Home
- New Phishing Hook
- Phishing Scams Grow

Test Your Phishing IQ
- Phishing Quiz 1
- Phishing Quiz 2

Phishing eCard

Outsmart Phishers!

- Visit only reputable web sites (ones belonging to large organizations or individuals you know and trust).
- Don't click on links in suspicious e-mails.
- Check sender information: Be suspicious of messages in your in-box that appear to have been sent by an employee but are addressed in Internet style (ex. "JohnSmith@rich.frb.org" instead of "John Smith").
- If in doubt about any message received on a work PC, contact your local help desk.

Blogging Boom

Did You Know?
11 Million - number of American adults who say they have created a blog

Links:
- Blogging Statistics
- Blogging=Danger?
- Be a Safe Blogger
- Blog Safety
- Blogging Tips
- Blogging Tips for Teens

Security Bits & Bytes Articles
(these .pdf files take a bit longer to load; you'll need to scroll to the article):
- Think Before You Talk
- Blog Q&A from Answer Bug

Dooced!

Following is a list of people who have been "dooced," or fired from their jobs due to information posted in their personal blogs:

Matthew Brown (Starbucks)

Daniel P. Finney
(St. Louis Post-Dispatch)

Michael Hanscom (Microsoft)

Blogging Best Practices

All employees and contract workers must use caution when communicating in online public forums (blogs, mailing lists, newsgroups, chat rooms, e-mail, etc.).
In particular:

1. Avoid sharing any FR-related information online, even if that information is not classified. Examples of information that should not be shared include:
   - References to the Bank
   - References to your employment at the Bank
   - Information about your job responsibilities
   - Information about our computing environment
   - Your Bank e-mail account (e.g., firstname.lastname@xxx.frb.org) or phone number
2. Remember, none of your online activities are anonymous. Your Bank e-mail account, as well as your private e-mail account activity if performed from your Bank PC, can be traced back to the Bank.

Malware & More

Did You Know?
80% - of all cybercrime goes unreported

Links:
- Viruses & Worms
- Signs of Spyware
- Spyware Quick Facts

Security Bits & Bytes Articles
(these .pdf files take a bit longer to load; you'll need to scroll to the article):
- You're Being Watched
- Zombies Attack

How Secure Are You?
- Viruses (Quiz 1)
- Viruses (Quiz 2)
- Spyware (Quiz 1)
- Spyware (Quiz 2)

Test Your Knowledge, Click to Play!
BEWARE OF **SPYWARE**
Learn the clues!

Defining Malware

Malware is software designed to infiltrate or damage a computer system, without the owner's consent. Malware typically includes computer viruses, worms, Trojan horses, and spyware.

Virus: a program that can sneak onto your computer - often through an e-mail attachment - and then make copies of itself, quickly using up all available memory.

Worm: a program that reproduces itself over a network and can use up your computer's resources and possibly shut your system down.

Trojans: programs that, when installed on your computer, enable unauthorized people to access it and sometimes to send spam from it. Trojans could even record keystrokes and send that information to hackers.

National Information Security Awareness

Avoid Internet Pitfalls!

Did You Know?
12 months - the average victim of identity theft is unaware of the problem for one year

Links:
- Online Shopping Facts
- Better Business Bureau
- Free Annual Credit Report
- ID Theft Quick Facts
- Online Shopping Quick Facts
- Too Good to be True
- ID Theft

Security Bits & Bytes Articles
(these .pdf files take a bit longer to load; you'll need to scroll to the article):
- ID Theft True Story
- Security Nightmares
- $hopping $ense

Are You at Risk?
- A Quiz for Consumers
- Buying Online
- ID Theft IQ Test

The Three-Point Security Check

Before submitting any personal information online, especially financial information such as credit card numbers, be sure the web page is secure. Trusted web sites will secure your personal information by encrypting or scrambling the data. You can check the page's security by following this three-point security check:

- Look for "https" in the web site address, rather than "http." The "s" stands for "secure" and indicates the information you send is encrypted or scrambled. This means it can't be read during transmission.