



FISSEA Security Awareness, Training, & Education Contest

Entry Form

Please review rules before completing entry form including the due date. No late entries will be accepted. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Ahmed Hussein

Organization: Federal Aviation Administration

Type of Entry:

Awareness: there are four categories in this area: Poster, Motivational Item (aka: trinkets - pens, stress relief items, t-shirts. etc.), Website, Newsletter

Training & Education: there is one category for this area: Interactive scenario/exercise

Awareness

Title of Entry: Awareness Newsletter - FAA Monthly “Cyber Security Awareness Bulletin”

Description of Entry:

The Office of Information Systems Security, at the Federal Aviation Administration hosts a variety of awareness and training events throughout the year to increase general users’ awareness of cyber security threats within the day-to-day activities, both on-line and physical threats. One of the tools used to increase that awareness is through monthly Cyber Security Awareness Bulletin. The newsletter is published monthly with a mass mail distribution sent to our federal employees as well as contractors. It provides an array of safety computing tips and practices for the general user not only while at the workplace, but at home place as well.

Name of Submitter: Ahmed Hussein

Organization: Federal Aviation Administration

Type of Entry: Newsletter

FAA Monthly “Cyber Security Awareness Bulletin”

Description of Entry:

The Office of Information Systems Security, at the Federal Aviation Administration hosts a variety of awareness and training events throughout the year to increase general users’ awareness of cyber security threats within the day-to-day activities, both on-line and physical threats. One of the tools used to increase that awareness is through monthly Cyber Security Awareness Bulletin. The newsletter is published monthly with a mass mail distribution sent to our federal employees as well as contractors. It provides an array of safety computing tips and practices for the general user not only while at the workplace, but at home place as well.



http://www.Cyber Security Awareness Bulletin

November 2009
Issue 25

The Awareness, Training, Compliance and Evaluations Division, AIS-200, is responsible for informing FAA employees about the latest issues, products and services in the IT/ISS industry. The Cyber Security Awareness Bulletin is a monthly newsletter for FAA's ISS community. The bulletin contains helpful and informative articles designed to improve the dialogue with the ISS community and keep them abreast of new ISS related developments in the FAA and in the ISS industry.



INSIDE THIS ISSUE

- 1 Federal P2P Ban Weighed
- 2 Tips for Safe Online Holiday Shopping
- 3 Software Assurance E-Learning Curriculum
- 4 Fake Airline Ticket Spam Taking Off
- 5 Software Assurance Policy
- 6 Continuation of Software Assurance Policy
- 7 In the News

Federal P2P Ban Weighed

New legislation introduced in the U.S. House would restrict the use of peer-to-peer (P2P) file sharing software across the federal government. The Secure Federal File Sharing Act, introduced by U.S. Rep. Edolphus Towns, D-N.Y., chairman of the House Oversight and Government Reform Committee, comes after numerous sensitive government documents were found on P2P networks, including blueprints for President Obama's helicopter, *Marine One*.

Although this legislation is not yet in effect, the Department of Transportation currently has a P2P policy in effect; the DOT Information Technology and Information Assurance (IT/IA) Policy Number 2006-17: *Peer-to-Peer (P2P) File Sharing Software*, dated March 11, 2006. This policy prohibits the use of P2P software unless approved in writing by the DOT Office of the Chief Information Officer (OCIO). All waiver requests within the FAA must be initiated by the information systems security manager (ISSM) and cosigned by the authorizing official. The request must be reviewed and approved by the FAA CIO before it is forwarded to the DOT OCIO for final approval.

The FAA has approved ONLY one P2P application for use today; it is Lotus Notes SameTime. It is authorized for IM and to facilitate net meetings. Departmental policy requires that authorized P2P technologies must be configured so shared desktop and other file sharing features are disabled. Departmental policy also states that P2P technologies must never be used on information systems that access, process, or store sensitive information, including personally identifiable information. If the use of unauthorized P2P software is identified, the FAA Cyber Security Management Center (CSMC) will notify the affected LOB/SO information systems security manager (ISSM). The LOB/SO ISSM will then notify the employee's supervisor or manager. Sanctions for violations of this policy will be dealt with under current agency disciplinary procedures and may include temporary or permanent loss of access to FAA computer and network resources.

Tips for Safe Online Holiday Shopping



Online holiday shopping offers a myriad of conveniences over dealing with traffic, snow, lack of parking, and crowds. From the comfort of your own home you can shop for gifts anywhere in the world.

Even with the convenience, online shopping can have a few pitfalls as there are always con artists out there, which is why you need to be on your guard.

Here are a few tips to help make your online holiday shopping go more smoothly:

- **Evaluate the seller.** Is the seller well-known? If you're planning to purchase from a large online retailer like Amazon.com, you don't have to worry about being ripped off. You will, however, want to make sure you understand their policies. If you're going to buy from a smaller retailer or one you're not familiar with, it's in your best interests to find out if they're worth doing business with. That also goes for auctioneers with items you may be considering bidding on through eBay, for example.
- **Understand the sales, return, and privacy policies.** It's very important that you know what the seller's policies are with regards to sales, returns, and privacy. This information should be available on all reputable sellers' Web sites, usually under the "Policies," "About Us," "Shipping," "Customer Support," or "Help" sections of the site.
- **Make sure that the Web site uses encryption technology** before you provide your personal information. Encryption scrambles the information you send, such as your credit card number, in order to prevent computer hackers from obtaining it en route. You can tell when you are on a secure web page several ways:
 - If you look at the top of your screen in the address bar where the Web site address is displayed, you should see https://. The "s" that is displayed after "http" indicates that web site is secure. You may not see the "s" until you are actually on the order page on the Web site.
 - Another way to determine if a Web page is secure is to look for a closed padlock displayed at the bottom of your screen. If that lock is open, you should assume it is not a secure site.
 - Finally, if you use the Firefox browser, the entire address bar will turn yellow if you are on an encrypted page. In Internet Explorer 7, the address bar will turn green if the page is encrypted.
- **Shop on the Internet with a credit card.** In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. When it has been determined that your credit was used without authorization, you are only responsible for the first \$50 in charges. You are rarely asked to pay this charge. We recommend that you obtain one credit card that you use only for online payments to make it easier to detect wrongful credit charges. Make sure your credit card is a *true* credit card and not a debit or check card. A debit or check card exposes your bank account to thieves. Your checking account could be wiped out in minutes. Further, debit and check cards are not protected by federal law to the extent that credit cards are.

Software Assurance E-Learning Curriculum

Are you responsible for designing, developing, or testing software for your line of business or staff office? If so, do you want to improve your awareness of best practices and guidelines, methods, and technique for Software Assurance (SwA)? Or are you interested in taking SwA training courses and obtaining continuing professional education (CPE) credits towards CISSP certification?

The Office of Information Systems Security (AIO) contracted with Strategic Systems International and Veracode to purchase the Veracode SecurityReview® eLearning Curriculum that allows us to improve software assurance awareness and provide training for software developers and security personnel on how to build secure software applications.

The Veracode SecurityReview® e-Learning Service integrates web-based secure programming training modules and a knowledgebase for developers and security personnel to meet SwA awareness and training requirements. The e-Learning service consists of three parts: Self-paced Security Assessment, Web-based Software Assurance courses and exams, and Knowledge Base on Secure Software Development.

The eLearning Security Assessment allows you to determine your knowledge of Application Security by taking an Application Security Fundamentals assessment quiz. Based on the results of the quiz, you can better determine the types of courses, which would benefit you, as a software designer or developer within your organization.

The Web-based Software Assurance courses and exams are integrated with a Learning Management System that allows you to track progress through the courses and print a transcript containing list of completed courses. The web-based courses cover a wide range of topics targeted for general, information assurance, program managers, and software developer audiences. Topics include: Software Assurance Awareness (General), application security fundamentals (all), and technical courses, such as secure Java and secure .NET development, how to break software security, and cryptography. The duration for general courses is 60 minutes; whereas technical courses range from 120 to 740 minutes.

The Knowledge Base on Secure Software Development contains thousands of security assets, including guidelines, checklists, techniques, and vulnerability descriptions. The Knowledge Base contains basic and advanced search and filter capabilities. For example, you can narrow the search criteria to specific software language or operating platform, in order to find out how to eliminate cross-scripting in Java-based applications.

For more information about the FAA Software Code Vulnerability Service or how to access the Veracode Software Assurance eLearning Curriculum, contact Mary Horn, AIS-200 at (202) 385-6899 or mary.horn@faa.gov.

You are also encouraged to visit the FAA Software Code Vulnerability Scanning Service Web Site that is located at:
https://intranet.faa.gov/faaemployees/org/staffoffices/aio/programs/iss/software_code_vulner_scan_serv/.

Fake Airline Ticket Spam Taking Off

Excerpted from Symantec Security Blogs
Written By: Samir Patil November 23, 2009



Is your wish to spend the upcoming holidays in Hawaii or the Bahamas? With the recent increase in the volume of airline ticket spam, spammers have made it seem easy to grab cheap (or even free) airline tickets to your favorite destinations. During the holiday season many people travel to visit family and friends. In the current economic environment, cheap deals on airfare will attract users' attention and spammers take full advantage of this fact.

Symantec researchers are observing an increase in spam that is offering cheap airline tickets or gift vouchers to use towards a purchase of airline tickets. Spam messages are originating with spoofed email addresses, such as "AirlineTickets@spam-domain" and "Free.Airline.Tickets@spam-domain." The link provided in the message redirects the user to an online form where the user's personal information and credit card details are requested.

The top 20 headlines used in airline ticket spam are as follows:

Subject: RE: 2 [airline name removed] Airline Tickets
Subject: Fly the skies with cheap airfares.
Subject: Fly Anywhere in the U.S.
Subject: 2 Round Trip Airline tickets. Fly anywhere in the US
Subject: Airfare on us - with this [airline name removed] Airlines Reward Card
Subject: Airline ticket bookings made easier.
Subject: Airline tickets. The quickest way to anywhere.
Subject: Airline tickets to any place in the world.
Subject: Amazing deals across all airlines.
Subject: Book cheap airline tickets now!
Subject: Cheap airfares. Save more, fly more!
Subject: Have some place to go We'll pay for your Airfare!
Subject: It's not too late to receive a companion airline ticket voucher on us.
Subject: Need to Fly for the Holidays?
Subject: Someone sent you [airline name removed] Airline tickets
Subject: [airline name removed] ticket voucher for xxxx - please review today
Subject: You have been chosen to receive 2 free Airline Tickets
Subject: Special airfares that will have you in the air!
Subject: Second chance to receive a companion airline ticket voucher on us.
Subject: Save on Holiday Travel Costs

Since there are many fake products associated with such unsolicited offers, users can never be assured that the cheap airline ticket is genuine (if it is actually ever supplied). Users can avoid compromising their data by simply typing legitimate URLs directly into the browser address bar when ordering their supplies, and by not letting curiosity get the best of them when unsolicited offers are sent. Users should also have anti-spam and antivirus solutions installed and up to date to prevent compromising personal information.

Software Assurance Policy

FAA Order 1370.109 - Signed October 23, 2009

This article provides an overview of the new FAA Order 1370.109, Software Assurance Policy, signed on October 23, 2009. This Order establishes a Security Software Assurance policy for the Federal Aviation Administration (FAA) to protect the confidentiality, integrity, and availability of FAA information systems.

Software Assurance Definition:

Software Assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner.

What is the Purpose of the Order?

- Establishes a methodology for ensuring software assurance security for software in development, operation, and maintenance phases.
- Determines if software code designs are securely written, implemented, and operating as intended while protecting information systems and their components.
- Utilizes approved tools purchased for Agency-wide use, to verify and validate the software contained within an information system is compliant with accepted security practices to reduce patch management activities.
- Assigns accountability to software developers to provide secure quality deliverable products that perform as expected.

Policy Tenets:

The following policy statements must be adhered to for all FAA organizations:

- Software assurance security assessments must have the ability to conduct static and dynamic analysis when possible on the binary executables of software code or can be manually tested at the discretion of the LOB/SO.
- Software assurance security assessments must comply with the standards from the NIST National Vulnerability Database (NVD) located at URL: <http://nvd.nist.gov/>
- Software assurance assessments must categorize identified vulnerabilities using the Common Vulnerability Scoring System (CVSS) and adhere to the Common Weakness Enumeration (CWE) dictionary for software weakness types. Information about these standards can be found at <http://nvd.nist.gov/cvss.cfm> and <http://nvd.nist.gov/cwe.cfm>.
- Vendor technologies used to perform software assurance assessments are referenced in the NIST Software Assurance Metrics and Tool Evaluation (SAMATE) list.
- Security test planning and/or execution must be performed during specific key phases of the software development life cycle.

Continued on Page 6

Software Assurance Policy from Page 5

Who does this Order apply to?

This Order applies to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), Information System Owners (ISO), software developers, and Federal Acquisition Executive (FAE), who are responsible for developing or maintaining software. This policy assigns responsibility and accountability to each FAA line of business to determine their critical applications or systems that are to be assessed including frequency of testing and review of code for compliance with this order.

What is the Scope of this Order?

This Order sets the criteria for evaluating testing tools that identify software deficiencies so that defects are uncovered and remediated. The scope of this policy includes examination of software as well as execution of that software code in various environments and conditions.

Where can a copy of the FAA Order 1370.105 be obtained?

FAA Order 1370.109 is available on the intranet at:

https://employees.faa.gov/tools_resources/orders_notices, and on the AIO Intranet web site at:

<https://intranet.faa.gov/faaemployees/org/staffoffices/aio/library/>

For further information, contact Mitchell Estep, AIS-500 at 202-385-6906, Mitchell.Estep@faa.gov or Greg Brisco, AIS-500 at 202-385-6907, Greg.Brisco@faa.gov.

In the News

Climatologists Hot Over E-mail Hack

<http://www.securityfocus.com/brief/1039>

Workers Stealing Data for Competitive Edge

<http://www.net-security.org/secworld.php?id=8534>

Spam 'Godfather' Gets 51 Months In Prison

http://voices.washingtonpost.com/securityfix/2009/11/spam_godfather_alan_ralsky_get.html

Cyberattacks Against the U.S. "Rising Sharply"

<http://www.scmagazineus.com/report-cyberattacks-against-the-us-rising-sharply/article/158236/>

Experts: Smart Grid Poses Privacy Risks

http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_privacy.html

New Verizon Wireless-Themed Zeus Campaign Hits

<http://www.scmagazineus.com/new-verizon-wireless-themed-zeus-campaign-hits/article/157848/>

FAA Information Systems Security
Awareness, Training, Compliance and Evaluations Division (AIS-200)

950 L'Enfant Plaza North, S.W.
4th Floor, Room 441
Washington, DC 20024

If you have any comments or suggestions on topics you'd like to see covered, please contact:
9-AWA-AIO-ISS-Community@FAA