OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Information Security Awareness Training and Phishing

Audit Report

Report Number
IT-AR-16-001

October 5, 2015

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

The Postal Service's information security awareness training related to phishing was not effective.

Background

Information security awareness training is a formal process for educating employees about corporate information technology policies and procedures. Implementing information technology training helps reduce security threat risks. The U.S. Postal Service's security awareness training program consists of specified topics such as password protection, transmission of sensitive information, and phishing.

Phishing is a security threat used to deceive an email recipient by posing as a legitimate entity. About 156 million phishing emails are sent globally every day. In 2014, phishing email attacks caused about 18 percent of cyber intrusions.

With one of the largest corporate email systems, the Postal Service handles more than 3.5 million emails a day delivered to more than 200,000 email accounts. In November 2014, the Postal Service announced a significant cyber intrusion that appeared to be caused by a phishing email attack. Providing security awareness training that emphasizes security threats, combined with testing employees' understanding, are key to avoiding or minimizing the impact of phishing emails.

Our objective was to evaluate the effectiveness of the Postal Service's information security awareness training related to phishing and to determine how employees respond to phishing emails.

What the OIG Found

When we began our review, the Postal Service's information security awareness training related to phishing was not effective because it did not completely explain how to identify and report phishing emails. However, during our audit, management added instructions for identifying and reporting phishing emails. Therefore, we are not making a recommendation in this area.

In addition, current policy does not require all employees with network access to complete the annual information security awareness training. Although this training is available to all employees with network access, only Chief Information Office employees and new hires are required by policy to complete the annual training.

We performed a limited phishing assessment by sending emails containing false links to 3,125 Postal Service employees. Of the 3,125 employees who received the phishing email, 2,916 (93 percent) did not report the email as required by policy.

The results of our test identified 789 of the 3,125 employees (25 percent) clicked on the link in the phishing email. Of these 789 employees, we determined 710 (90 percent) did not report that they clicked on a phishing email to the Postal Service's Computer Incident Response Team as required by policy.

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Of 3,125 employees in our sample, 2,986 (96 percent) did not complete the annual information security awareness training, based on training records for FY 2014. In addition, 750 of 789 employees in our sample who clicked on the link in the phishing email (95 percent) did not complete the training.

When management does not require all employees with network access to take annual information security awareness training, users are less likely to appropriately respond to threats.

A recent study revealed that user awareness training effectively changes behavior and reduces security-related risks by up to 70 percent.

What the OIG Recommended

We recommended the Postal Service modify policy to require all employees with network access to take annual information security awareness training.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

October 5, 2015

MEMORANDUM FOR: GREGORY S. CRABB
ACTING CHIEF INFORMATION SECURITY OFFICER
AND DIGITAL SOLUTIONS VICE PRESIDENT

E-Signed by Michael Thompson
VERIFY authenticity with eSign Desktop

FROM: Michael L. Thompson
Acting Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – Information Security Awareness Training and Phishing (Report Number IT-AR-16-001)

This report presents the results of our audit of the U.S. Postal Service information Security Awareness Training and Phishing (Project Number 15TG020IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Aron Alexander, director, Information Technology, or me at 703-248-2389.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

The Postal Service's information security awareness training did not explain how to identify and report phishing emails.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's information security awareness training and phishing (Project Number 15TG020IT000). Our objective was to evaluate the effectiveness of the Postal Service's information security awareness training related to phishing and to determine how employees respond to phishing emails. See Appendix A for additional information about this audit.

An effective information security awareness and training program explains proper rules of behavior for using agency information technology (IT) systems and information. Users[1] are the largest audience in any organization and, therefore, the most important group of individuals in terms of helping reduce accidental errors and IT vulnerabilities.

Users need to understand and comply with agency security policies and procedures and be trained in how to use the systems and applications to which they have access. Furthermore, users must be aware of actions they can take to better protect their agency's information, including, but not limited to, reporting suspected incidents or violations of security policy and following rules established to avoid social engineering attacks.

Social engineering is a non-technical intrusion method that attackers[2] use to gain unauthorized access to computer networks. It relies heavily on user interaction, such as phishing emails that guide users into clicking on a link that infects their computer. Phishing is the most common form of social engineering. About 156 million phishing emails are sent globally every day and 16 million reach the recipient bypassing security controls. Of these 16 million emails, about half are opened and 10 percent of recipients click the link contained in the email, resulting in a compromised network.

With one of the largest corporate email systems, the Postal Service handles more than 3.5 million emails a day delivered to more than 200,000 email accounts. In November 2014, the Postal Service announced a significant cyber intrusion that appeared to be caused by a phishing email attack; therefore, providing security awareness training that emphasizes security threats combined with testing employees' understanding are key to avoiding or minimizing the impact of phishing emails.

Summary

When we began our review, the Postal Service's information security awareness training[3] related to phishing was not effective because it did not explain how to identify and report phishing emails. During our audit, management added instructions for identifying and reporting phishing emails to the training course;[4] therefore, we consider this matter closed.

In addition, current policy does not require all employees with network access to complete the annual information security awareness training. Although this training is included in the fiscal year (FY) 2015 Strategic Training Initiatives (STI),[5] available to all employees with network access, the policy only identified employees from the Chief Information Office (CIO) and new hires as employees required to complete the annual training.

---

1 Includes employees, contractors, and other collaborators or associates requiring access.
2 A party who acts with malicious intent to compromise an information system.
3 Our Shared Responsibility, Learning Management Systems (LMS) Course #10021144.
4 CyberSafe 101: Passwords and Phishing, LMS Course #10024251.
5 The STI identifies an employee's required training for the year. The annual information security awareness training was included in the STI for FY 2015 and the target audience included Postal Career Executive Service, Executive Administrative Service, Inspection Service, and Field Craft employees.

Postal Service policy does not require all employees with network access to complete the annual information security awareness training.

As a result of our limited phishing test, we found that employees did not respond to the phishing email according to policy.[6] When management does not require all employees with network access to take information security awareness training that includes how to respond to security threats, users are less likely to appropriately respond to threats.

Information Security Awareness Training Program

Phishing Awareness Training

When we initiated our review, the Postal Service's information security awareness training[7] related to phishing did not effectively train employees on how to respond to phishing emails according to policy.[8] This issue occurred because the Corporate Information Security Office (CISO)[9] decided to emphasize other matters in their security awareness training, such as encryption and password protection. Specifically, the training[10] did not completely explain how to identify and report phishing emails. For example, the training displayed a video which showed how users should right-click and delete a phishing email; however, it did not show how to identify phishing emails or how to immediately report phishing attempts to the Computer Incident Response Team (CIRT).[11]

Recommended practice[12] is that information security awareness training include information on known threats, the organization's security requirements, and who to contact for further security advice or for reporting incidents. In addition, Postal Service policy[13] requires users to report all information security incidents to the CIRT immediately.

During our audit, the CISO introduced a new online training course that addressed this issue. The training now instructs employees on how to identify and report phishing emails; therefore, we consider this matter closed.

Training Policy

While the annual information security awareness training is included in the FY 2015 STI, Postal Service policy[14] does not require all employees with network access to complete this training annually. This issue occurred because management used a risk-based approach and only required employees from the CIO and newly hired employees to complete training. The recommended practice[15] is to make information security awareness training mandatory for all users (including contractors) with access to IT systems. See Appendix B for a listing of the job functional groups required to complete the training outlined in the policy.

Without mandated annual information security awareness training outlined in a policy for everyone with network access, all users may not be aware of how to appropriately respond to and report phishing emails, which increases the risk of a cyber intrusion. According to a recent study,[16] information security awareness training could reduce security-related risks by up to 70 percent.

---

6 Handbook AS-805, *Information Security*, Section 13-3.1, Incident Prevention, and Section 13-3.2, Incident Reporting, dated May 2015.
7 Outlines the security requirements that users and managers need to implement to protect the Postal Service's sensitive and critical information resources. This program incorporates Postal Service training, awareness, and policies related to security.
8 Handbook AS-805, Section 13-3.1, Incident Prevention, and Section 13-3.2, Incident Reporting.
9 The office responsible for setting the overall strategic and operational direction of the Postal Service information security program and its implementation strategies.
10 Our Shared Responsibility, LMS Course #10021144.
11 The CIRT is responsible for monitoring incidents to ensure appropriate response and immediate resolution of security incidents.
12 *The State of Oregon Information Security Resource Center*, *18 Best Practices in Security Awareness Training*, dated 2006.
13 Handbook AS-805, Section 13-1, Security Incident Management.
14 Handbook AS-805, Section 6-5.3, Training Requirements, Exhibit 6-5.3. The policy states that, based on requirements defined by the CISO at the beginning of the fiscal year, designated personnel with access to Postal Service information resources must participate in information security training and data protection requirement training. Information security training is recommended for all other non-bargaining personnel.
15 *The State of Oregon Information Security Resource Center, 18 Best Practices in Security Awareness Training*, dated 2006.
16 Aberdeen and Wombat's *The Last Mile in IT Security: Changing User Behaviors*, dated January 2015.

Of the 3,125 employees we sampled, 789 (25 percent) clicked on the link in the phishing email, and 710 of these employees (90 percent) did not report the email to the CIRT.

Phishing Assessment

We performed a limited phishing assessment by sending emails containing false links to 3,125 judgmentally[17] selected recipients to determine if they would click on the link and report the phishing attempt as required by Postal Service policy.[18] In preparation for the test, we requested the CISO to prevent normal defense mechanisms[19] so we could measure employees' abilities to recognize and report phishing emails. We did not release the names and email addresses of employees that were part of the assessment to Postal Service management. Specifically, we found:

- Of the 3,125[20] employees we sampled, 789 (25 percent) clicked on the link in the email, and 710 of these employees (90 percent) did not report the email to the CIRT. According to industry statistics,[21] similar phishing assessments have reported that 11 percent of recipients clicked on the links in phishing emails. Table 1 shows the distribution of these employees by job function.

Table 1. Phishing Test Results by Job Function

Job Function	Sample Selection	Clicked Phishing Link		Clicked and Didn't Report	
Administration	349	134	38.4%	117	87.3%
Operations	348	131	37.6%	120	91.6%
Postmaster	346	116	33.5%	111	95.7%
Management	348	101	29.1%	95	94.1%
Finance/Human Resources	346	87	25.1%	73	83.9%
Contractor	344	67	19.5%	50	74.6%
Information Technology	348	59	17.0%	54	91.5%
Sales	349	51	14.6%	50	98.0%
Mail Services	347	43	12.4%	40	93.0%
Total	**3,125**	**789**	**25.2%**	**710**	**90.0%**

Source: OIG phishing email assessment results.

- Of 3,125 employees who received the phishing email, 2,916 (93 percent) did not report the incident to the Postal Service CIRT team, as required by policy.[22] However, 83 employees not included in our phishing assessment, such as managers and peers of the employees who received the phishing email, reported the email to the CIRT.
- Of 3,125 employees in our sample, 2,986 (96 percent) did not complete the annual information security awareness training, based on training records for FY 2014. In addition, 750 of 789 employees in our sample who clicked on the link in the phishing email (95 percent) did not complete the training, based on training records for FY 2014.

17 Selected job functional groups that routinely had access to email.
18 Handbook AS-805, Section 13-3.1, Incident Prevention, and Section 13-3.2, Incident Reporting.
19 This was done to allow the OIG to send over 3,000 emails at one time. We believe Postal Service defenses would have blocked a mass distribution of 3,000 emails, but would not have blocked these emails if they were sent individually at various times. The purpose of the campaign was to test users' awareness of phishing emails and not the Postal Service's defense mechanisms.
20 We distributed phishing emails to 3,131 employees, six of which were returned as invalid, leaving 3,125 employees who received the test email.
21 The *Verizon 2015 Data Breach Investigations* report.
22 Handbook AS-805, Section 13-3.2, Incident Reporting.

Recommendation

We recommend management modify Handbook AS-805, Information Security, Section 6-5.3, Training Requirements, to require all employees with Postal Service network access to take annual information security awareness training.

We recommend the acting chief information security officer and Digital Solutions vice president:

1. Modify Handbook AS-805, *Information Security*, Section 6-5.3, Training Requirements, to require all employees with Postal Service network access to take annual information security awareness training.

Management's Comments

Management agreed with the findings and the recommendation; however, they disagreed with the OIG's analysis and conclusions concerning the policy for annual information security awareness training. In addition, they disagreed with the portrayal of the reporting in the audit as a 93 percent failure. They noted that even with 7 percent of employees reporting, the Postal Service received over 100 reports of the phishing email within the first hour.

Management agreed with the intent of the recommendation and will research the implications and review the proposed policy change with all stakeholders. The target implementation date is March 30, 2016.

See Appendix C for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendation in the report and the corrective actions should resolve the issue identified.

The updated Information Security Training Matrix and STI are not policy. Handbook AS-805 is the Postal Service's information security policy and it does not currently require all employees with Postal Service network access to take annual information security awareness training. Therefore, we recommended that management modify Handbook AS-805 to require all employees with Postal Service network access to take annual information security training.

Regarding management's comment on our portrayal of the reporting in the audit as a 93 percent failure, the OIG found that 93 percent of employees who received the phishing email did not report the incident to the Postal Service CIRT. The OIG did not measure who reported within the first hour; however, we measured the total number of employees that reported the incident.

The OIG considers the recommendation significant and, therefore, requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. This recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information

Background

Information security training and awareness programs are a vehicle for disseminating security requirements to employees to protect the network from threats such as viruses,[23] spyware,[24] and phishing. Awareness creates sensitivity to the threats and vulnerabilities of computer systems and recognition of the need to protect the information, systems processing, and transmission of the information.

Phishing emails can cause damage ranging from denial of access to substantial financial loss. These emails often attempt to get users to click on a link that will install a Trojan[25] on their computer. The attacker can then use the Trojan to collect information from the infected computer or compromise the network.

A method for combating phishing email attacks is to train users to recognize and report phishing attempts. Reporting incidents[26] enables the responsible group to review security controls and procedures, establish additional corrective measures, and reduce the likelihood of recurrence.

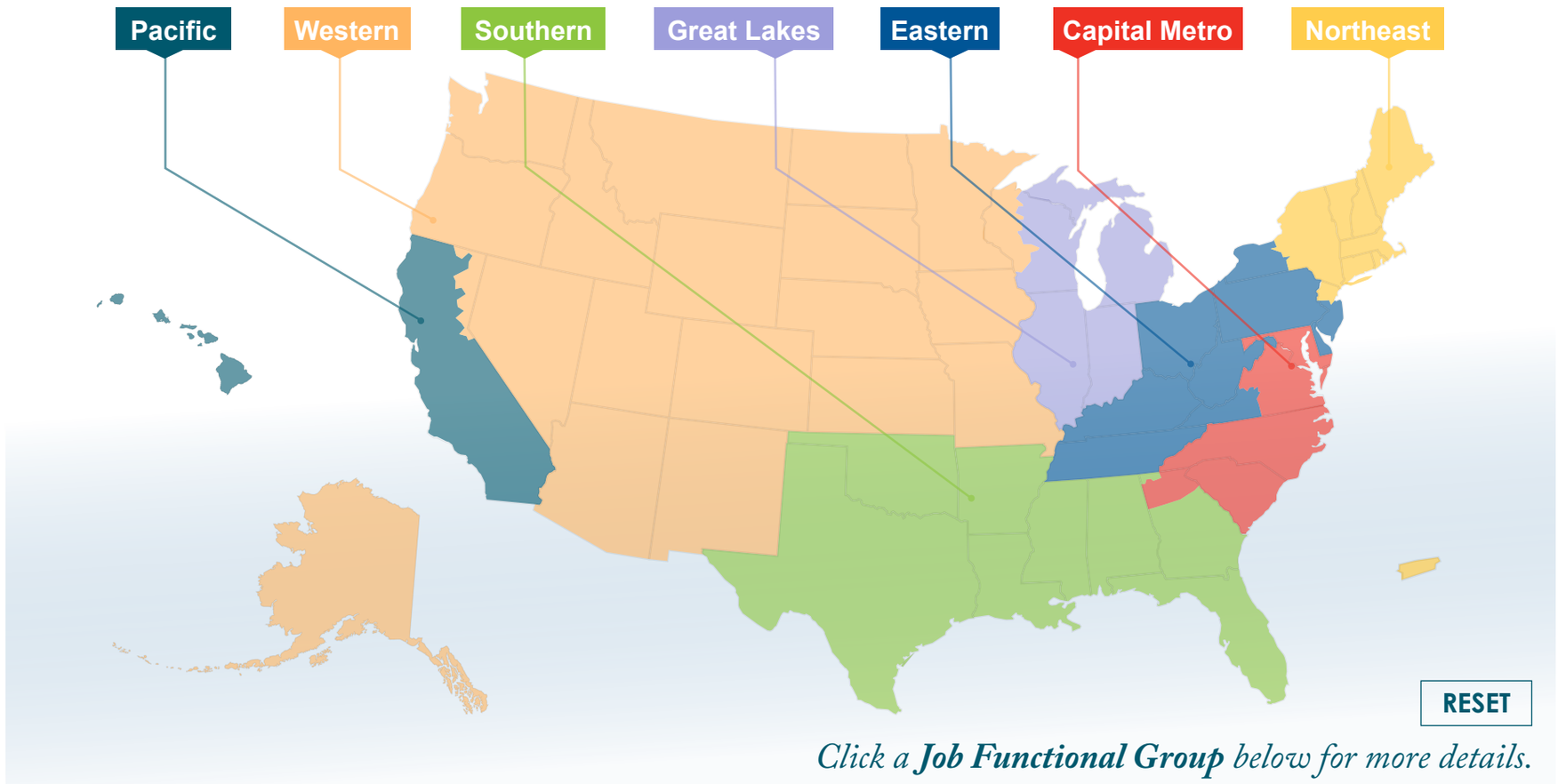
Objective, Scope, and Methodology

Our objective was to evaluate the effectiveness of the Postal Service's information security awareness training related to phishing and to determine how employees respond to phishing emails. To accomplish our objective, we identified Postal Service employees with email accounts. We judgmentally selected job functional groups that routinely had access to email, which included Sales, administration, Finance/Human Resources, IT, mail services, management, operations, and postmasters.[27] As a result, our universe totaled 110,590 such Postal Service employees. We limited the scope of this audit to phishing emails and did not employ any additional social engineering techniques.

From our universe, we developed a statistical sample within the Postal Service's seven geographical areas and job functions. See Table 2 for a stratified sample of the employees nationwide.

23 A program written to alter the way a computer operates without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to the computer in the process.
24 Any program that monitors online activities or installs programs without consent for profit or to capture personal information.
25 Software programs that appear to be harmless but contain hidden code designed to exploit or damage a system. Hackers can transmit them through email messages or use them to modify or destroy data or obtain confidential information.
26 Events, whether suspected or proven, deliberate or inadvertent, that threaten the integrity, availability, or confidentiality of the network.
27 We excluded some groups that may not access their emails frequently, such as custodians, mechanics, and rural and area mail carriers.

Table 2. Stratified Sample of Postal Service Employees Nationwide



	GEOGRAPHICAL AREAS							
Job Functional Groups	**Cap Metro**	**Eastern**	**Great Lakes**	**Northeast**	**Pacific**	**Southern**	**Western**	**Total**
Sales	24	52	46	57	28	70	72	**349**
Administration	72	45	34	50	30	60	58	**349**
Finance/Human Resources	43	18	73	48	41	22	102	**347**
Information Technology	33	44	47	61	39	59	65	**348**
Mail Services	27	44	52	56	43	62	63	**347**
Management	33	43	44	66	38	69	55	**348**
Operations	39	47	42	58	34	67	61	**348**
Postmaster	19	59	43	52	15	64	96	**348**
Contractor	200	29	22	18	10	29	39	**347**
								3,131

Source: OIG statistician's stratified sample.

We performed a phishing email assessment to determine whether Postal Service employees could recognize and appropriately respond to phishing email attempts. In preparation for the test, we requested the CISO to prevent normal defense mechanisms and keep notifications of the audit to a minimum so we could measure employees' ability to recognize and report phishing emails. We also requested CISO to report the names and email addresses of anyone who reported phishing emails. Additionally, we agreed to keep the list of employees that were part of the phishing assessment anonymous. We distributed phishing emails to 3,131 employees at one time, and counted employee responses from May 27 through June 4, 2015. During the assessment, six emails were returned as invalid, leaving 3,125 employees who received the test email.

We reviewed employee training records to identify who completed the annual information security awareness training in FY 2014. In addition, we interviewed key officials and evaluated the information security awareness program to include related training topics, awareness communications, policies, and practices.

We conducted this performance audit from March 2015 through October 2015, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusion based on our audit objective. We believe the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective. We discussed our observations and conclusions with management on August 28, 2015, and included their comments where appropriate.

We assessed the reliability of computer-generated data by performing automated testing. We assessed the results of the email phishing test by reviewing the number of clicked, did not click, reported, and did not report phishing emails. We determined the data obtained were reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
U.S. Postal Service Cybersecurity Functions	IT-AR-15-008	7/17/2015	None
South Florida District Vulnerability Assessment	IT-AR-14-001	10/22/2013	None

Appendix B: Training Matrix

Table 3 summarizes the Postal Service employee job function groups that are required or recommended to complete the annual information security awareness training.

Table 3. CISO Annual Training Matrix for 2014

Groups	Our Shared Responsibility Video
Existing ACE Users	Recommended
New Hire ACE User	Required***
All CIO	Required
Retail Associates/Window Clerks, Postmasters, and Postmaster Relief	Not Specified[30]
Back Office Personnel	Not Specified
Network, System, and Database Administrators	Not Specified
Developers	Not Specified
Information Systems Security Officers, Information Systems Security Representative, Project/Program Managers, and Relationship Managers	Not Specified
Inspection Service	Recommended
OIG (may use equivalent training but completion must be tracked)	Recommended
Suppliers, Contractors, Vendors, Businesses, and Partners	*****

***New hire ACE users are also given a copy of Handbook AS-805-C.

*****Handbook AS-805 equivalent training in terms of content and frequency to be provided by the supplier, contractor, vendor, or business partner.

Source: Postal Service CISO.

28 The CISO has not required or recommended these groups to complete the annual security awareness training.

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

September 18, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Report – Information Security Awareness Training and Phishing
(Report Number IT-AR-15-DRAFT, project number 15TG020IT000)

Thank you for the opportunity to review and comment on the subject draft audit report. We agree that annual security awareness training, which includes phishing awareness training, is critically important for the organization.

To this point, in FY2015 USPS launched the CyberSafe at USPS™ cybersecurity awareness and training initiative to educate employees, suppliers and customers on critical cybersecurity topics for the organization and the postal industry. We have focused the FY2015 efforts on employees and employees of contractors who have active access to USPS networks.

CyberSafe at USPS™ includes information such as:

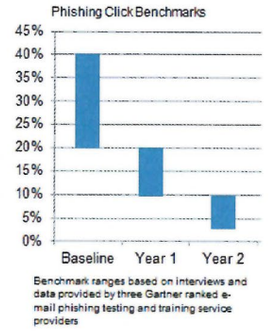
- Introductory video emphasizing the individuals role in helping to protect USPS information and systems
- Information on USPS connection with the Department of Homeland Security's National Cybersecurity Awareness Campaign—Stop.Think.Connect.™
- Information on when and how to report suspicious activity or computer incidents
- Cybersecurity tips such as:
  - Development and use of strong, unique yet easy to remember passwords
  - Defining, identifying and avoiding phishing traps
  - Protecting sensitive data
  - Securing workstations
- Formally tracked training such as CyberSafe 101 web based training course (WBT) and multiple PCI related courses

As part of the CyberSafe at USPS ™ initiative, USPS is requiring employees with active ACE account access to the USPS network to complete the new CyberSafe 101 WBT course by 9/30/2015. This course focuses on individual's role and responsibility to help protect the USPS information and systems, strong passwords and how to identify and report phishing traps. As of September 18, 2015, over 120,000 USPS employees and over 3,000 supplier employees have completed the course.

In regards to USPS policy for annual information security awareness training, we disagree with the OIG analysis and conclusions in the Highlights section of this report which states: "current policy does not require all employees with network access to complete the annual information security

awareness training." USPS is requiring employees with active ACE account access to the USPS network to complete the new CyberSafe 101 WBT course by 9/30/2015 as part of the strategic training initiative program for FY15. We have also updated the Information Security Training Matrix on the CISO website to reflect this requirement as required in policy via Handbook AS-805, Information Security, Section 6-5.3, Training Requirements.

The USPS considered the OIG phishing test that was conducted as part of this audit to be a baseline test of where USPS employees were with respect to identifying and reporting phishing tests. The OIG test was done right at the beginning of the launch of the CyberSafe at USPS™ initiative, and the 25% click rate for the test was in line with industry benchmarks for similar companies just launching their phishing awareness and training programs.



Since the OIG test, we have conducted two follow-up phishing tests in June, 2015 and September, 2015 and have already seen a drop in phishing click rates to 18% and 11% respectively. We will continue to conduct frequent phishing tests to measure the effectiveness of the awareness and training initiative and make adjustments to the program to continue to improve organizations defenses.

With respect to the reporting of phishing traps to the USPS Computer Incident Response team, USPS agrees that user reporting is an important part of the overall network defenses. We are emphasizing the need to report then delete suspicious e-mails via the CyberSafe at USPS™ initiative. However, we have to disagree with the OIG portrayal of the reporting within this audit as a 93% failure. Even with 7% of the employees reporting, USPS received over 100 reports of the phishing trap within the first hour. These reports would have been sufficient for us to execute our phishing defenses to protect the network. It also must be noted that the OIG specifically requested USPS not execute such defenses and to specifically allow the phishing test to pass through our e-mail server defenses.

In summary, USPS is executing a multiple phase cybersecurity improvement strategy to meet its security objectives and address security needs across the enterprise. This includes on-going awareness and training via the CyberSafe at USPS™ initiative. Protecting the privacy of customer, employee, supplier and the Postal Service information has been and always will be a priority for the Postal Service.

Recommendation 1:
We recommend the acting chief information security officer and digital solutions vice president:

> Modify Handbook AS-805, Information Security, Section 6-5.3, Training Requirements, to require all employees with Postal Service network access to take annual information security awareness training.

Management Response:
Management agrees with the intent of this recommendation and the importance of annual information security training and we will research the implications of the proposed policy change with all stakeholders. The requested policy change must be vetted by all internal stakeholders.

As outlined above, USPS is requiring employees with active ACE account access to the USPS network to complete the new CyberSafe 101 WBT course by 9/30/2015 as part of the strategic

training initiative program for FY15. We have also updated the Information Security Training Matrix on the CISO website to reflect this requirement as required in policy via Handbook AS-805, Information Security, Section 6-5.3, Training Requirements. USPS will also require cybersecurity training in FY16 as we continue to add new content to the CyberSafe 10* series of web based training courses and these will be reflected in the Information Security Training Matrix as part of policy.

The current policy under AS-805, Information Security, Section 6-5.3, Training Requirements states:
Based on requirements defined by the CISO at the beginning of the fiscal year (see the Information Security Training Matrix on the CISO Website), designated personnel with access to Postal Service information resources must participate in information security training and data protection requirement training.

The policy was written this way to be flexible to the annual business and training needs of the Postal Service and thus any required training that was documented in the Information Security Training Matrix on the CISO Website was policy for the specified period of time.

The OIG is requesting AS-805, Information Security, Section 6-5.3, Training Requirements be changed to:
Based on requirements defined by the CISO at the beginning of the fiscal year (see the Information Security Training Matrix on the CISO Website), designated personnel with access to Postal Service information resources must participate in data protection requirement training; and all personnel with network access to Postal Service information resources must complete the information security training.

We will review the proposed policy change with required stakeholders during the next AS-805 policy update period which starts this fall.

Target Implementation Date: Stakeholder comments on the proposed policy change will be completed by 3/30/2016.

Responsible Management Officials:
Acting Chief Information Security Officer and Digital Solutions Vice President

Responsible Management Officials:

Greg Crabb
(a) Chief Information Security Office and
Digital Solutions Vice President

Attachments:

cc: Manager, Corporate Audit Response Management

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100