OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 23, 2020

MEMORANDUM FOR: JEFFERY A. ADAMS
VICE PRESIDENT, CORPORATE COMMUNICATIONS

GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

Margaret B. McDavid

FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service and Information Technology

SUBJECT: Management Alert - Active Smishing Campaign Masquerading as the U.S. Postal Service
(Report Number 21-018-R21)

This management alert presents an Active Smishing Campaign Masquerading as the U.S. Postal Service. This issue came to our attention during our ongoing audit of the Integrity of U.S. Postal Service's Social Media Presence (Project Number 20-278). The objective of this management alert is to bring this issue to your attention with a recommendation for corrective action.

We appreciate the cooperation and courtesies provided by your staff. If you have questions or need additional information, please contact Mary Lloyd, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Introduction

During our audit of the Integrity of U.S. Postal Service's Social Media Presence (Project Number 20-278), we found a smishing campaign that may have a significant negative impact on the Postal Service's brand, reputation, and customer loyalty. The purpose of this alert is to bring this issue to your attention with a recommendation for corrective action.

Smishing is a mobile phishing[1] attack that targets victims using text messages rather than emails. These messages appear to be sent by legitimate, trusted organizations like the Postal Service. Smishing attacks attempt to trick mobile users into clicking on links that are connected to fraudulent sites that could steal credentials or propagate malware.

Conclusion

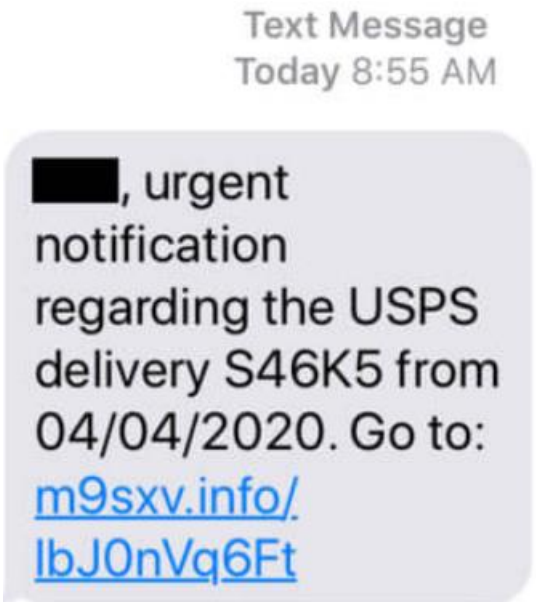
We found the Postal Service had not informed the public of an active large-scale smishing campaign that used the Postal Service as a disguise. This malicious campaign could negatively impact the Postal Service's brand, reputation, and customer loyalty.

Smishing Campaign

During our audit we identified a news article[2] dated September 16, 2020, that publicly discloses a known smishing campaign using the Postal Service as a disguise to trick mobile users. According to the article, the malicious messages claim to contain important information about a Postal Service package. The message attempts to trick recipients into clicking on a link to steal the individual's credentials or to infect their device with malware. Figure 1 is an example of a smishing message using the Postal Service as a disguise.

[1] Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in an email to distribute malicious links or attachments.
[2] New Smishing Campaign Using USPS as Its Disguise, September 16, 2020.

Figure 1. Example of a Smishing Message



Source: Twitter.

We reviewed official Postal Service social media channels and USPS.com for information warning customers of this smishing scam and found that the Postal Service has not provided any public notification of this latest campaign. However, according to another article,[3] Postal Service fraud investigators acknowledged that this was a smishing scam to get information from the recipient when they clicked on the link. The Postal Service also stated that it would not send text messages unless someone has previously signed up for such messages about a specific package delivery.

According to the Federal Trade Commission's guidance[4] on responding to situations where a business has been impersonated in a smishing scam, a business should inform its customers as soon as possible by announcing it on their social media sites and warn customers to ignore suspicious texts purporting to be from their company. The guidance further states that the important point is to remind customers that legitimate businesses would never solicit sensitive personal information through an insecure channel like text messages.

Proactive notification of attempts to defraud its customers could help protect the Postal Service's brand, reputation, and customer loyalty.

During our audit, the U.S. Postal Inspection Service took corrective action by adding smishing information to their website.

[3] Solicitor warns of scam involving text messages appearing to be from U.S. Postal Service, September 4, 2020.
[4] Has a phishing scam hooked your company's good name? March 6, 2017.

Recommendation #1: We recommend the **Chief Postal Inspector** initiate a smishing awareness campaign and the proper precautions a customer should take when encountering a smishing message.

Recommendation #2: We recommend the **Vice President, Corporate Communications**, initiate a smishing awareness campaign through its social media platforms and USPS.com on the proper precautions posted on the U.S. Postal Inspection Service website.

Management's Comments

Management generally agreed with the finding and recommendations in the report.

Regarding recommendation 1, management agreed with this recommendation and stated the Postal Inspection Service deployed a smishing awareness campaign to the public on October 28, 2020 via their website. Therefore, management requests this recommendation be closed with issuance of this audit report.

Regarding recommendation 2, management agreed with this recommendation and stated that Corporate Communications will work with the Postal Inspection Service to promote awareness of smishing campaigns across Postal Service social media channels and alert customers of these events on usps.com, to the extent possible. Management will, at least monthly, link to the Postal Inspection Service's website and online information as it becomes available. The target implementation date is February 2021.

See Appendix A for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the alert.

With regard to recommendation 1, we verified that management has implemented the corrective action they describe and agree to close this recommendation on issuance of this alert.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All Recommendation 2 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.

APPENDIX A. MANAGEMENT'S COMMENTS

UNITED STATES POSTAL SERVICE

December 22, 2020

JOSEPH WOLSKI
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Management Alert – Active Smishing Campaign Masquerading as the U.S. Postal Service (Report Number: 21-018-DRAFT)

Thank you for the opportunity to review and comment on the recommendations contained in the Management Alert, Active Smishing Campaign Masquerading as the U.S. Postal Service.

The Postal Service had previously addressed recommendation 1 on October 28, 2020 and agrees with recommendation 2. Management will address each recommendation separately below.

Recommendation #1: We recommend the Chief Postal Inspector, initiate a smishing awareness campaign and the proper preçautions a customer should take when encountering a smishing message.

Management Response/Action Plan: The U.S. Postal Inspections Service already deployed a smishing awareness campaign prior to this management alert being issued. Therefore, we request this recommendation be closed with issuance of this audit report. The U.S. Postal Inspection Service is dedicated to bringing awareness to the crimes being perpetrated against postal customers and businesses. We have various ongoing crime prevention campaigns throughout the year and provide specific awareness when issues arise, such as smishing. We began developing smishing awareness material in September of 2020 and deployed this information to the general public on October 28, 2020 through our website (https://www.uspis.gov/news/scam-article/smishing/).

Recommendation #2: We recommend the Vice President, Corporate Communications, initiate a smishing awareness campaign through its social media platforms and USPS.com on the proper precautions posted on the U.S. Postal Inspection Service website.

Management Response/Action Plan: Management agrees with the recommendation with respect to the Corporate Communications role.

As such, Corporate Communications, once it becomes aware of a legitimate smishing campaign, and working in concert with the U.S. Postal Inspection Service, will promote awareness across USPS social media channels alerting customers to the event. Additionally, we will also use USPS.com to the degree possible to alert customers to these events. The USPS will at least monthly link to the developed websites and/or online information developed by the U.S. Postal Inspection Service as it becomes available.

Target Implementation Date: February 2021

Responsible Official:
Director, Digital Communications

Jeffery A. Adams
Vice President, Corporate Communications

Gary R. Barksdale
Chief Postal Inspector

cc: *Manager, Corporate Audit Response Management*