Protect Your Heart And Your Information:
Beware Of Fake Text Messages

Office of Information Technology
Division of Information Security
FEBRUARY 2026

During the Valentine's Day holiday, the evocation of love with gift-giving can cause an unfortunate rise in scams that target your emotions and aim for your wallet.

Recently, a wave of fraudulent text messages claiming to be from the United States Postal Service (USPS) has been circulating, preying on the anticipation of packages and gifts. These smishing scams (phishing attempts delivered via SMS text messaging) intend to deceive recipients into revealing sensitive information, or clicking malicious links, by pretending to resolve fake delivery issues.

The USPS is the main target for scammers due to its widespread use and trusted reputation for package deliveries. Many rely on USPS for important shipments, making fraudulent messages more believable. These fraudulent messages often claim there is an issue with a delivery, such as an incorrect address, missing payment, or a shipping delay.

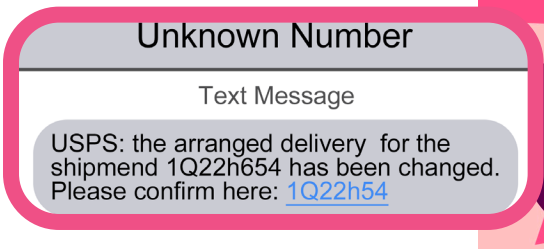
Common Fraud Messages Include:

- Your package has arrived at the warehouse and cannot be delivered due to the incomplete address information. Please confirm your address in the link.
- Final delivery attempt: Confirm your details to avoid package return.
- Pay $1.00 to schedule package delivery.

These smishing messages often use urgency, trying to make the recipient feel the need to act immediately to avoid losing a package.

How Smishing and Other Scams Work

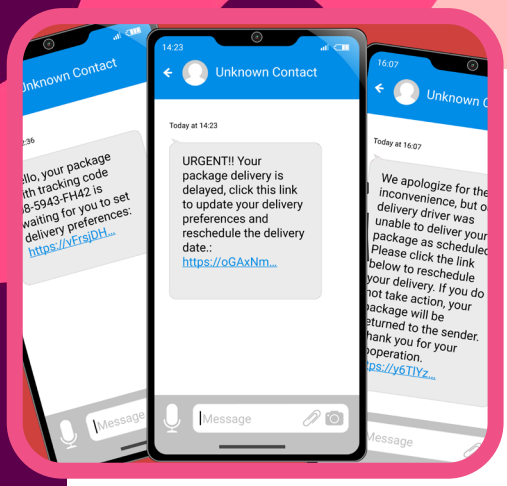
- **Fraudulent Text Notification:** The scam begins with sending a text message to the recipient claiming to be from USPS.
- **Malicious Link:** The text message contains a phishing link that redirects the recipient to a fake USPS website.
- **Theft:** A malicious website asks recipients to provide personal information, credit card numbers, or other sensitive data.
- **Fraudulent Use:** Scammers use the stolen information for identity theft, make unauthorized purchases, or other malicious activities.



Scams are particularly effective around Valentine's Day because more people expect deliveries such as flowers, chocolates, or other gifts. Also, the emotional connection tied to Valentine's Day gifts adds pressure to respond, increasing the chances of falling for a scam.

How to Spot a Fake USPS Text Message

Unfamiliar Senders/Unknown Number: USPS will not send customers text messages, or e-mails, without a customer first requesting the service with a tracking number, and it will NOT contain a link.



Spelling and Grammatical Errors: Scammers sometimes use poor grammar and misspelled words in messages.

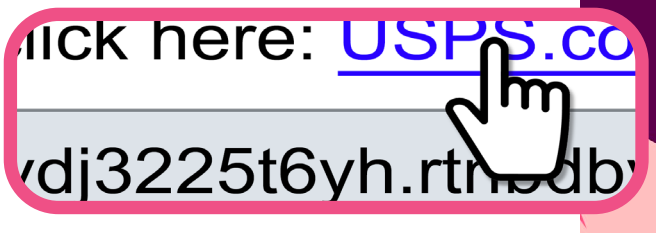
Generic Message: Pay attention to messages that don't include your name, specific tracking numbers, or accurate details about your package.

Pressure to Act Fast: Be cautious if the message urges you to act immediately to avoid missing your delivery.

Suspicious Links: Official USPS links will include "usps.com." Always hover over any link to check the URL before clicking.

A realistic USPS text message for an expected delivery may look like this:

USPS 01123456789123456789, Expected Delivery by: Friday, February 14, 2025 Reply STOP to cancel.



What to Do if You Receive a Fake USPS Text Message

- **Don't Click the Link:** Avoid clicking the link, forwarding the message, or responding to the message.
- **Contact the USPS:** Check the status of your package directly on the official USPS website or app.
- **Report the Scam:** Forward the message to 7726 (SPAM), which will assist with reporting the scam phone number. Also, email directly the United States Postal Inspection Service including a screenshot of the message, to spam@uspis.gov.
- **Report Junk:** iPhone and Android users have the option to report spam text messages directly within the app, by selecting "Report Spam/Junk" at the bottom of the message.
- **Block the Sender:** Blocking the sender will stop further scam messages.
- **Delete the Message:** Once the message has been reported delete the message to avoid any accidental clicks.

In the event, that you have accidentally clicked the link, act quickly by changing passwords, notifying all of your financial institutions, and setting monitoring alerts on all of your accounts.

USPS Official Resources

USPS Texting: If you are expecting a package, sign up for text tracking directly with USPS.

USPS Informed Delivery: By using Informed Delivery, customers will receive an email showing their mail and packages as scanned at the local USPS.

The United States Postal Inspection Service (USPIS): Learn more about the recent USPS Scams and report all known scams directly to the USPIS.

This Valentine's Day, don't let scammers play with your heart or personal information! Stay informed, be cautious, and spread the love, not the scams!

NOTE: The links in this document are for informational purposes only, and do not signify an endorsement of any products contained within the linked sites/files.

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.