

# CONSUMER ALERT

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov



## Signs of the Season: Holiday Hams and Shipping Scams

**Release Date:** November 13, 2018

**Media Contact:** Jerad Albracht, 608-224-5007  
Bill Cosh, Communications Director, 608-224-5020

MADISON – Online holiday shopping brings a flood of emails to your inbox: purchase confirmations, shipping updates, promotional offers, requests for product reviews, and more. Amongst these messages, scammers can sneak malware-laden spam emails masked as shipping or delivery alerts. The Wisconsin Department of Agriculture, Trade and Consumer Protection warns consumers to be on the lookout for phony shipping emails and to avoid clicking links or opening attachments in these messages.

“Fake shipping emails are not exclusive to the holidays, but the volume of shopping-related messages during this season opens opportunities for these scams,” said Michelle Reinen, Director of the Bureau of Consumer Protection. “Scammers send these emails randomly to as many addresses as possible, so even consumers who don’t shop online need to be on the lookout.”

Watch out for emails or texts that warn you about a problem with a delivery, that request account information for security purposes, or that ask you to open an attached “shipment label” in order to claim a package from a local office. Scammers often use the names, logos and color schemes of major shipping companies and retailers to add legitimacy to their messages, and they may also spoof the company’s web address (URL) in the sender’s email address.

In actuality, there is no product waiting for delivery, and the alarming language in these emails is intended to make recipients act quickly without considering consequences. By clicking on a link in the email, a recipient risks downloading malware or handing over personal information to the scammers. If you receive a similar email, delete it and do not click any links.

If you are expecting a shipment that may be delayed, contact the shipper directly to inquire. Some e-commerce companies offer package tracking features right on their websites.

Here are some common elements to look for in fake shipping emails:

- Poor grammar and spelling errors in emails that claim to come from major businesses. If the message is sloppy, it likely did not come from a legitimate company.
- Sender addresses that don't match the URL for the company that supposedly sent the email. For example, the "From:" line in a fake FedEx email gave an Italian email address for the sender, not a fedex.com address (see example on next page).
- Shipment emails that lack specifics about the sender or the package's supposed contents.
- Emails asking you to open an attachment in order to review an order. Never open an attachment in an unsolicited or questionable email.
- Emails containing threats that a package will be returned to the sender and that you will be charged a fee for not responding to the message.

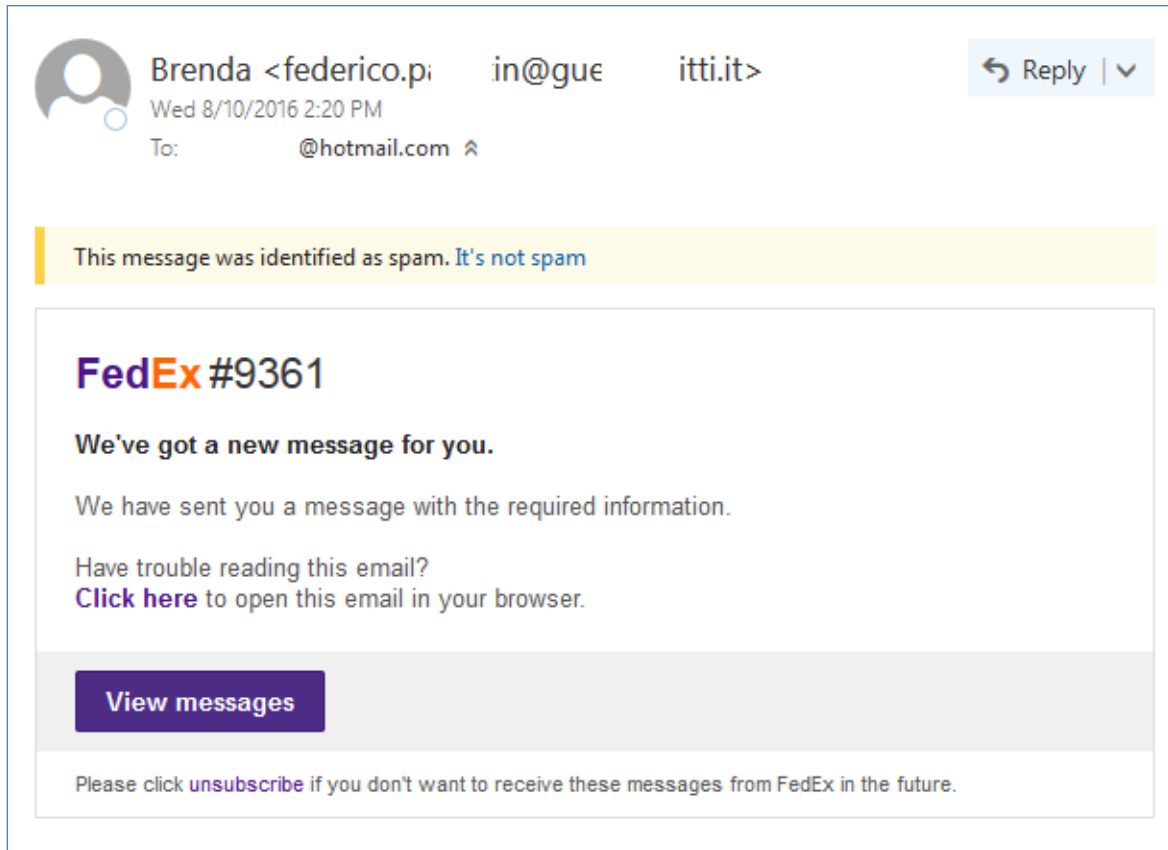
For additional information or to file a complaint, visit the Consumer Protection Bureau at [datcp.wi.gov](http://datcp.wi.gov), call the Consumer Protection Hotline at 800-422-7128 or send an e-mail to [datcphotline@wi.gov](mailto:datcphotline@wi.gov).

Connect with us on Facebook at [www.facebook.com/wiconsumer](http://www.facebook.com/wiconsumer) or Twitter: [@wiconsumer](https://twitter.com/wiconsumer).

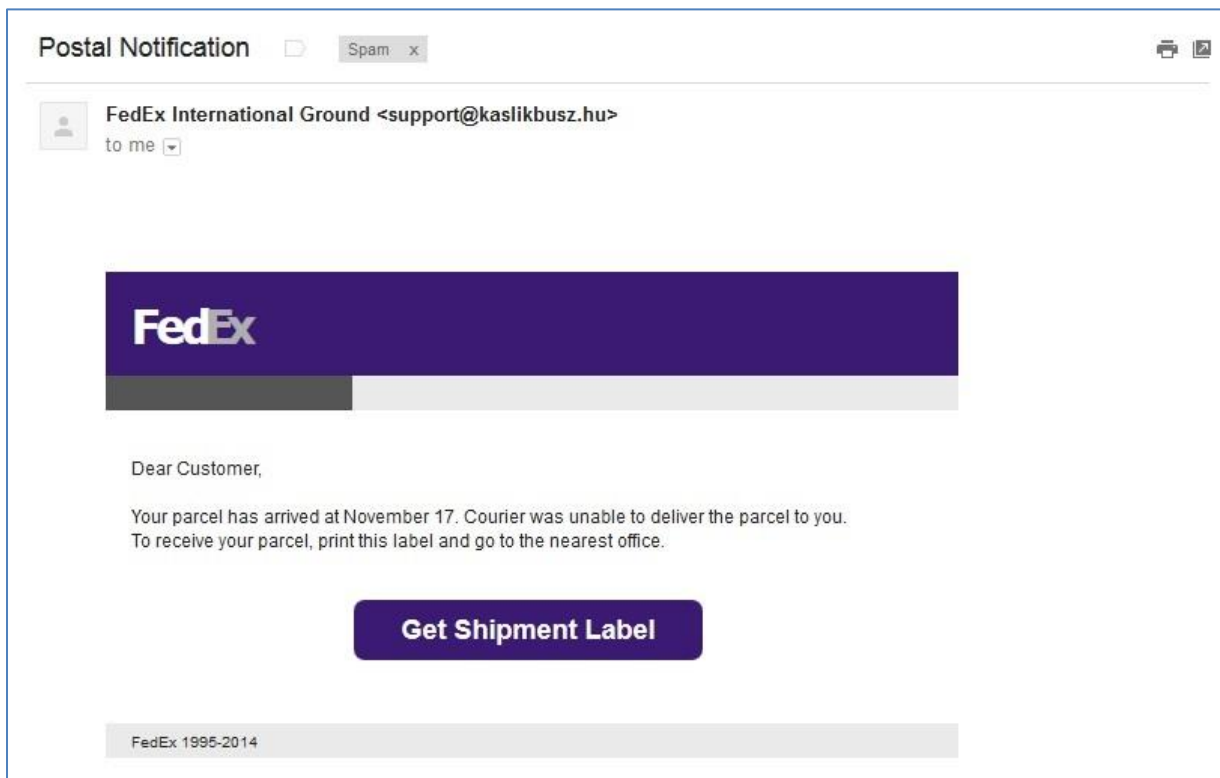
###

(MORE)

*Screenshots of fake shipping emails (included links are inactive):*



This screenshot shows an email interface. At the top left is a profile icon for 'Brenda' with the email address '<federico.p; in@gue itti.it>'. The date and time are 'Wed 8/10/2016 2:20 PM'. Below this is the recipient information 'To: @hotmail.com'. On the top right, there is a 'Reply' button with a dropdown arrow. A yellow banner below the header states 'This message was identified as spam. It's not spam'. The main body of the email features the FedEx logo followed by '#9361'. The text reads: 'We've got a new message for you. We have sent you a message with the required information. Have trouble reading this email? Click here to open this email in your browser.' At the bottom of the main content area is a dark blue button labeled 'View messages'. Below the main content area, there is a footer that says 'Please click unsubscribe if you don't want to receive these messages from FedEx in the future.'



This screenshot shows an email interface for a 'Postal Notification'. The subject is 'Postal Notification' and it is marked as 'Spam'. The sender is 'FedEx International Ground <support@kaslikbusz.hu>' and it is addressed 'to me'. The main content area features a large dark blue header with the FedEx logo. Below the header, the text reads: 'Dear Customer, Your parcel has arrived at November 17. Courier was unable to deliver the parcel to you. To receive your parcel, print this label and go to the nearest office.' At the bottom of the main content area is a dark blue button labeled 'Get Shipment Label'. At the very bottom of the email, there is a footer that says 'FedEx 1995-2014'.