CONSUMER ALERT

Wisconsin Department of Agriculture, Trade and Consumer Protection

datcp.wi.gov

'Tis the Season for Fake Shipping Emails

Release Date: **November 14, 2017**

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

MADISON – More and more consumers are shopping for the holidays online and are accustomed to the influx of purchase and delivery confirmation emails. This added email traffic creates a scenario where scammers can sneak malware-laden spam emails into consumers' accounts 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.

"Scammers will use any opportunity to flood inboxes with malicious spam emails, and they know that they may be able to slip a well-designed message past an unsuspecting consumer if it is in the mix of legitimate shipping updates," said Michelle Reinen, Director of the Bureau of Consumer Protection. "Remember that scammers are not picky about who they send their spam messages to, so even consumers who don't shop online and are not expecting a shipment could receive these fake shipping emails."

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.wisconsin.gov, call the Consumer Protection Hotline at 800-422-7128 or send an e-mail to datcphotline@wisconsin.gov.

Connect with us on Facebook at www.facebook.com/wiconsumer or Twitter: @wiconsumer.

###

(MORE)

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