

AttackSpotlight



FRAUDULENT SHIPPING NOTIFICATIONS ON THE RISE

Attackers Illegally Mimic Brands Like UPS, FedEx, and DHL to Trick Email Users

Scammers often send phishing emails designed to look like messages from organizations like UPS, FedEx, and DHL. People receive genuine shipping alerts on a regular basis at work and at home. Because of that, it can be harder to spot phishing emails that use this theme.

These attacks happen all year round, but they are more frequent during the holiday shopping season. Some contain dangerous links. Others contain infected attachments. All try to trick email users into acting without verifying the source of the message.

Attackers who send fraudulent shipping notifications might try to:

- Fool you into downloading dangerous software like a virus or ransomware
- Trick you into logging into a lookalike site in order to steal your password for the real site
- Steal your money or your organization’s money



Don't be fooled by familiar logos

Many phishing emails—including fraudulent shipping messages—use well-known logos and images. **Do not take emails at face value.** Most dangerous messages seem trustworthy on the surface.

WHAT SHOULD YOU LOOK FOR?

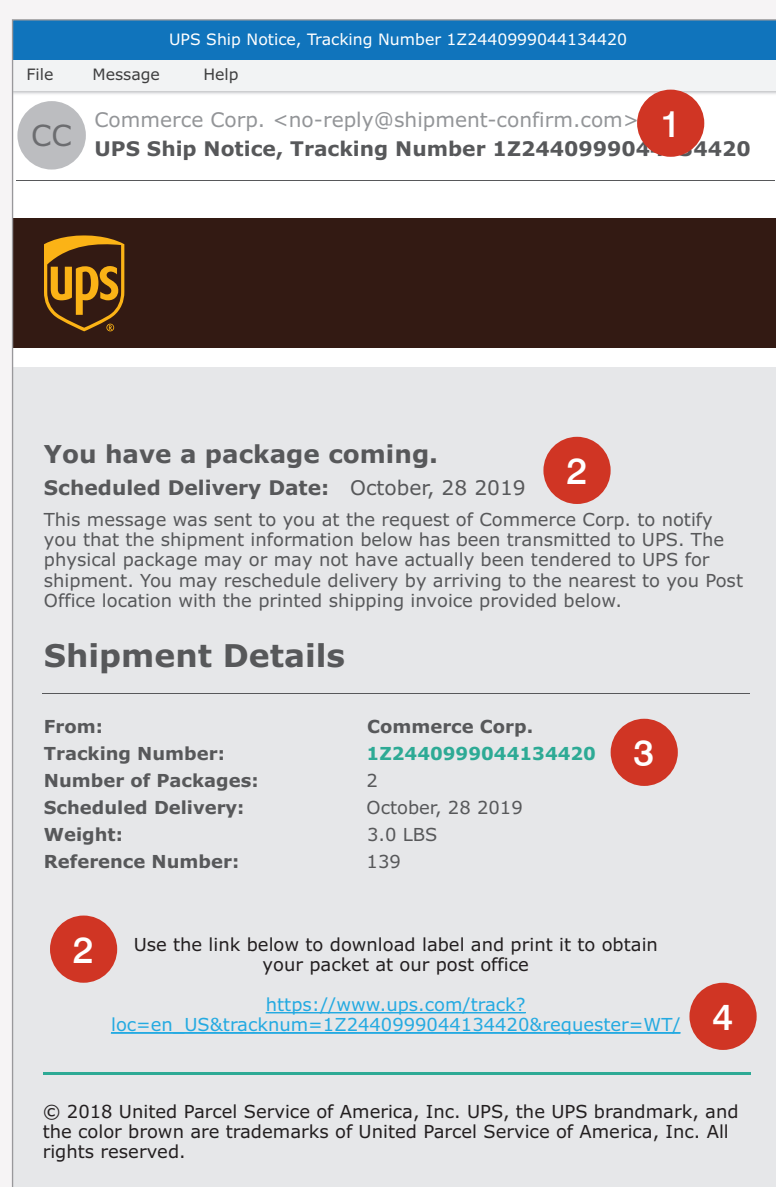
Fake shipping emails use several different tricks, including the following:

- Sending a phony tracking number
- Saying a package could not be delivered because nobody could sign for it
- Requesting additional postage in order for a package to be delivered
- Warning that a package has been held because of an invalid address
- Sending files that appear to be invoices or claim forms

These tricks all share a common goal: to trigger an emotion like curiosity, concern, excitement, or even anger. Attackers hope people will react without thinking things through.

AN EXAMPLE OF A DANGEROUS SHIPPING EMAIL

This phishing email mimics a UPS alert. We’ve changed a few details for your safety, but the danger signs we’ve highlighted are real.



- 1 Email mismatch** – There is a mismatch between the “from” name and address. The email appears to come from Commerce Corp., but the sending address doesn’t match that name.
- 2 Mistakes in the text** – The date is not punctuated correctly, and the package is called a “packet” in the email text. Global organizations like UPS rarely make these kinds of errors.
- 3 Invalid tracking number** – This tracking number is not valid when checked on the UPS website. Attackers hope users won’t bother to verify it.
- 4 Disguised links** – On the surface, this link looks valid and safe. But a malicious link is embedded in the text.

HOW TO PROTECT YOURSELF

Examine all shipping emails carefully before acting on them. These tips can help you avoid malicious messages:

- **Think before you act.** When you receive a shipping alert, look for warning signs that indicate the email could be dangerous.
- **Fight your feelings.** Be extremely cautious of any email that pushes you to act on an emotion like curiosity, excitement, or concern.
- **Check the source.** Verify tracking numbers on the shipper’s website and confirm other requests by calling a known, trusted customer service number.
- **Don’t confuse “familiar” and “genuine.”** Confirm an email is safe before you click a link, enter a password, make a payment, or download a file.

Stay on the lookout for fraudulent shipping alerts, especially during the holiday shopping season. And be sure to report suspicious emails to your security team.