

You'd Better Watch Out! More Holiday Scams And How To Avoid Them

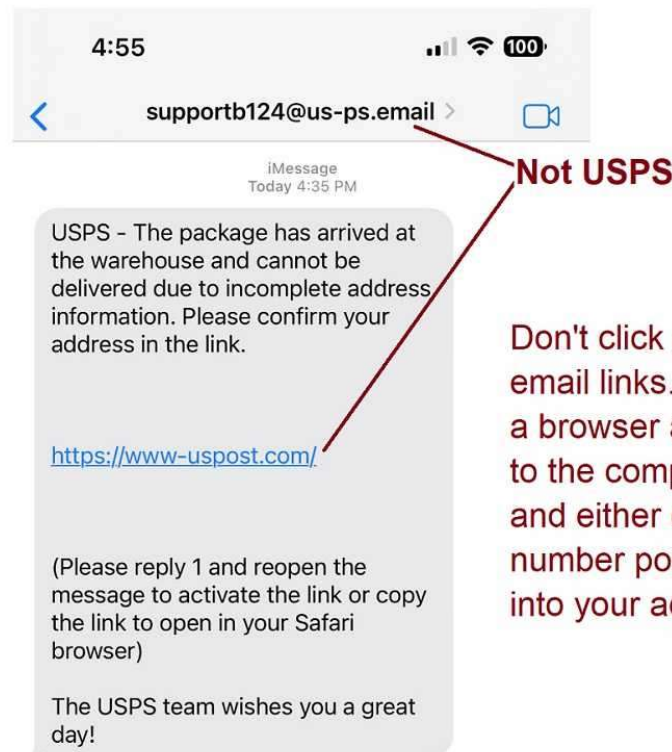
By: Jim Stickley and Tina Davis

November 12, 2024

Safely past Halloween, they're out there waiting. Right now, the scammers are looking to ruin this holiday season of gifting for their own benefit. Whether online or in person, these greedy grinchies are after what they can grab using tried and tested methods. Artificial intelligence (AI) is also helping scammers appear more legitimate. Some of the top scams are listed below to help you have a scam-free holiday season.

Phony Shipping Notices

Whether you're expecting a delivery or not, scammers will alert you via phone, email, or text there's a package on the way or you missed a delivery. They'll claim to be from FedEx, the post office, or other package delivery service sending you a link to track the fake delivery. The links lead to a spoofed website or they can download malware. Some ask for a credit card number or other PII for the bogus delivery.



Not USPS

Don't click on text or email links. Instead open a browser and navigate to the company's website and either call the number posted or log into your account.

TIPS: Don't click on any links and go to the true delivery service or merchant website to see if there's really a package delivery needing your help. Don't provide your PII or payment information when asked, it's a sign something isn't quite right.

Missing Packages

Porch Pirates are out in full force looking for package deliveries left on doorsteps and other obvious places. They love driving around neighborhoods looking for unattended deliveries. It's free stuff for

these grinch-pirates but it's a headache for you when you're not at home. Getting stolen merchandise replaced or refunded can take time you don't have for the gift-giving season.

TIPS: Instruct deliveries to a side or back door when possible or send to a friend or neighbor you know will be home. Home security cameras catch Porch Pirates in the act for law enforcement. Package tracking using the legitimate delivery service website can help with delivery days and times to be on the lookout. Use delivery options like Amazon's Key or Hub Lockers or pick up the item from the merchant when possible.

Fake Order Notices

Emails arrive about a purchase you've made from a retailer or third-party payment like PayPal, to verify your order. The purchase amount is enough to make you panic and you'll want to resolve the matter quickly. The email includes a link or phone number to dispute the order, and scammers know you'll likely follow it. The link can go to a spoofed website to steal your PII, or it will outright ask for your payment card and login information so the scammer can go a shopping spree.

The image shows a screenshot of an email titled "Confirmation.mail" from "zzerinlina55t5@gmail.com". The email body contains a confirmation of a one-time payment authorization for a Norton LifeLock subscription. Red annotations with numbers 1 through 5 point out various red flags:

- 1:** Norton nor any company would use a gmail account to contact customers. If the domain is not the company domain, it's a scam.
- 2:** If they don't even know your name, how could you be a customer?
- 3:** The logo "NORTON-LifeLock" has weird spacing in the "NORTON" part.
- 4:** The date format "Jan/05/2022" is odd.
- 5:** The phone number "1 (8 5 0) - 6 0 4 - 0 7 8 6" has odd spacing.

Other clues mentioned in the annotations include the use of a Gmail account, the weird spacing in the "NORTON" logo, the odd date format "Jan/05/2022", and the odd spacing in the phone number. The email also includes a "NORTON" logo, an "ORDER ID", "AMOUNT", and "PLAN".

Source: Microsoft

TIPS: Don't follow links or provide sensitive information. Instead, go directly to the merchant's true website and make inquiries from there. Check your payment card for unauthorized charges. If there isn't anything in either of those locations, it's likely a scam.

Keep In Mind...

Sob-sters... Appeals for donations including with GoFundMe can be bogus, so if you're giving this holiday season, stick with well-known or local charities...

Relatives needing fast financial help... Calls from a family member asking for a money wire to get out of jail, for instance, call a family member to confirm it's legit. Emails with similar scenarios, especially asking for money via gift cards, is the sign of a true scam...