

**Sender Address**

Real PayPal emails come from @paypal.com not @paypal-accounts.com

**Generic Greeting**

Usually, an important email will address you specifically by name. Not *Customer*

**Urgency & Threats**

Scammers love using time pressure to cause you to act without thinking

**Phishing Link Button**

Always hover over links, they usually reveal a suspicious URL that isn’t the official site (PayPal.com)

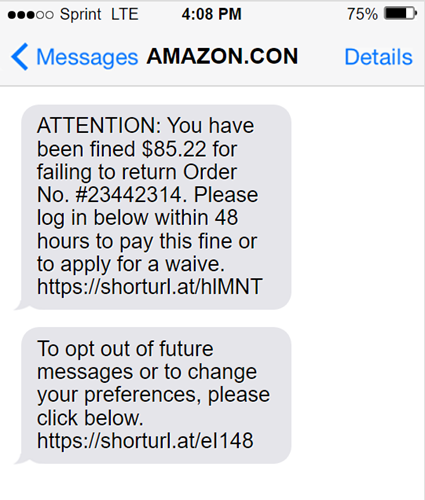
**Suspicious Instructions**

Instructed to confrim all account details through a link provided in the email

**Grammar & Punctuation Errors**

Random capitalization and punctuation.

Awkward phrasing: “Purchasing, and, sending and receiving money”



**Unusual Opt-Out Message**

Real opt-out texts will ask you to Reply YES or NO to opt out of future texts

**Suspicious Links**

Uses shortened URLs, commonly used to hide suspicious links. Normally would link somewhere in amazon.com

**Order Number Trap**

Scammers throw in numbers to make the message look official, but they rarely match real orders

**Urgency & Threats**

A fine wouldn’t be issued to you through text or email. The “*48-hour* deadline” is designed to scare you into clicking

**Strange Wording**

Apply for a “waive” is strangely worded. Larger companies like Amazon would have caught mistakes like this while proof-reading

**Fake Name**

Name appears as “Amazon.con”, sometimes done intentionally to avoid legality issues.