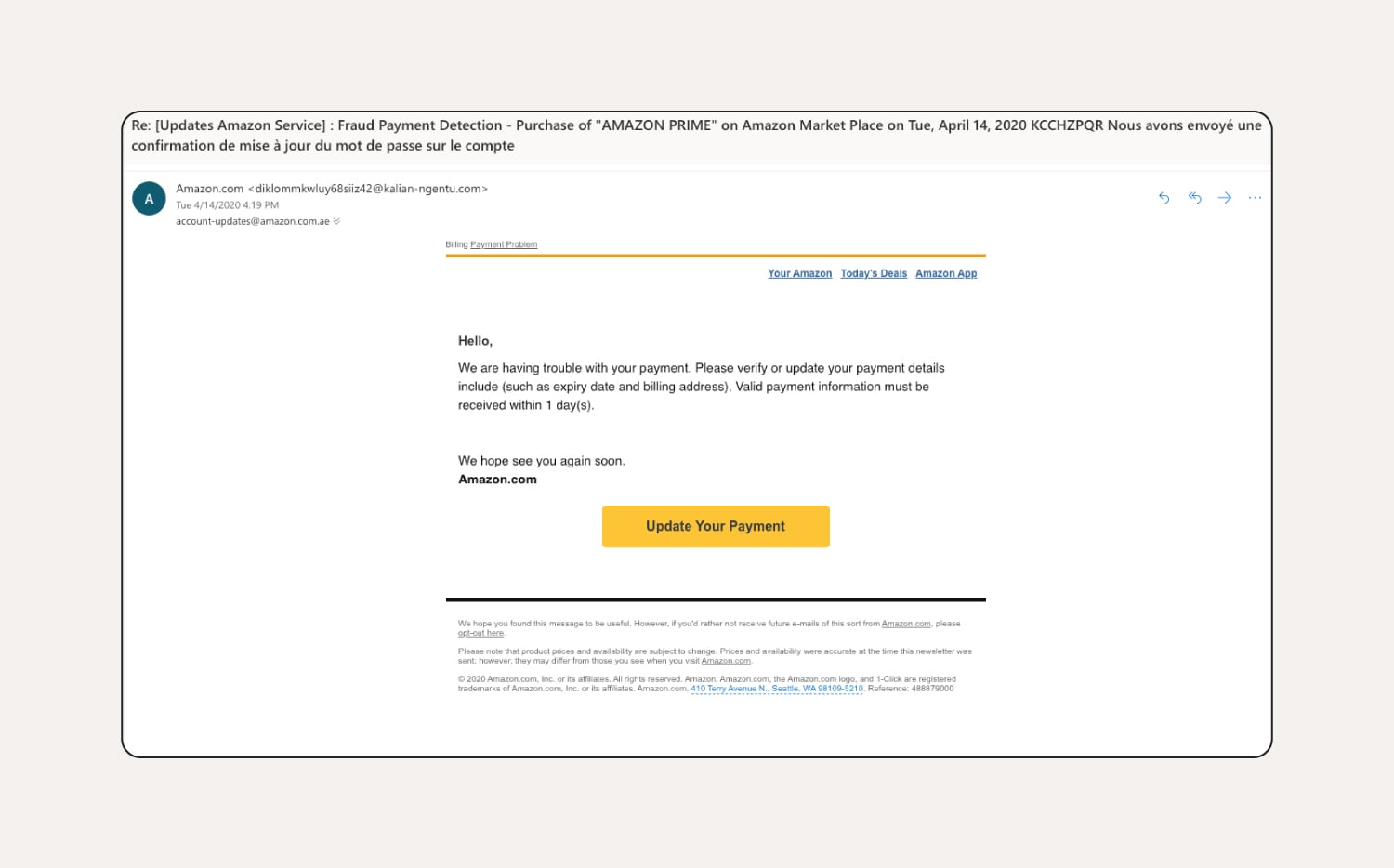


SOURCE: NORTON

**“PayPal Account Limited”**

**⚠️ Phishing Indicators:**

| **Category** | **Observation** | **Reason It’s Suspicious** |
| --- | --- | --- |
| **Sender Email** | services@paypal-accounts.com | Legitimate domain is paypal.com. This one is spoofed to trick users. |
| **Subject Line** | “[PayPal]: Your account access has been limited” | Creates panic to trigger emotional response. |
| **Urgency/Threat** | “You have 24 hours… or your account will be permanently disabled” | Classic phishing urgency tactic. |
| **Generic Greeting** | “Dear PayPal customer” | Real PayPal emails use your full name. |
| **Link/Button** | “Confirm Your Information” | Usually leads to a fake login page to steal credentials. |
| **Spelling/Grammar** | “You have to confirm all of your account details...” | Slightly unnatural sentence structure. |



SOURCE : NORTON

**“Amazon Payment Trouble”**

**⚠️ Phishing Indicators:**

| **Category** | **Observation** | **Reason It’s Suspicious** |
| --- | --- | --- |
| **Sender Email** | idikomkmwkluy68isil42@kalian-ngentu.com | Not a legitimate Amazon domain. Amazon uses domains like amazon.com or amazon.in. |
| **Subject Line** | “Fraud Payment Detection – Purchase of AMAZON PRIME...” | Uses fear to provoke immediate action – a common phishing tactic. |
| **Urgency** | “Valid payment information must be received within 1 day(s)” | Tries to pressure the user with a deadline. |
| **Link/Button** | “Update Your Payment” (actual link unknown but likely spoofed) | Link likely does not go to amazon.com. Hovering over it would likely show a fake domain. |
| **Grammar** | “We hope see you again soon.” | Grammar errors suggest non-professional origin. |
| **Brand Imitation** | Imitates Amazon formatting | Phishers mimic brands to gain trust. |