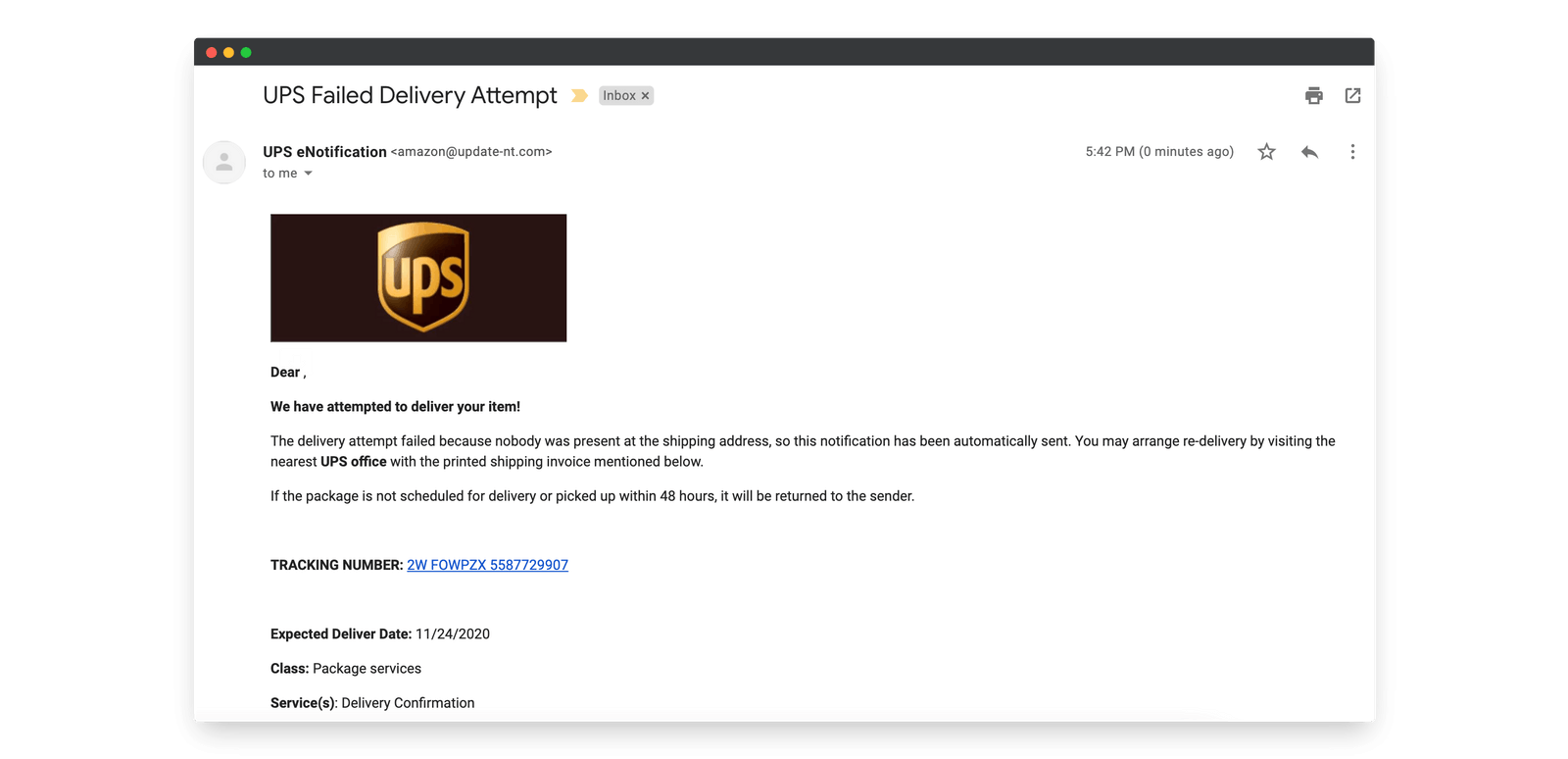
**Email Sample**



**Email Snapshot Summary**

* **Purported Source:** UPS eNotification
* **Logo:** Displays the UPS logo
* **Email Claims:** Delivery attempt failed; asks recipient to visit UPS office with printed invoice.
* **Tracking Link:** Hyperlinked tracking number (suspicious URL)
* **Expected Delivery Date:** 11/24/2020
* **Sender Display Name:** UPS eNotification

**Phishing Indicators Identified**

| **Indicator** | **Details** |
| --- | --- |
| **Suspicious Sender Address** | The email is from amazon@update-nt.com — not a legitimate UPS or Amazon domain. |
| **Brand Mismatch** | The email says it’s from UPS, but the email domain uses “amazon” – a red flag. |
| **No Personalized Greeting** | It starts with “Dear ,” — lacking your name or any personalization. |
| **Urgency Tactic** | Implies package will be returned if not acted on in 48 hours — classic phishing pressure technique. |
| **Suspicious Link** | “2W FOWPZX...” tracking link may lead to a phishing or malware page (hovering over it likely shows a non-UPS URL). |
| **Outdated Delivery Date** | Expected delivery: 11/24/2020 — implies it's a reused or spoofed old template. |
| **Grammar Issues** | Slightly awkward phrasing (e.g., “You may arrange re-delivery...”), inconsistent formatting. |
| **Unverifiable Source** | No UPS contact information, phone numbers, or official footer/signature block |

**Summary of Phishing Traits**

This email displays multiple classic phishing characteristics:

* **Spoofed sender email and mismatched brand references** (Amazon + UPS)
* **Urgency to trick recipient into clicking a link**
* **Lack of personalization**
* **Unusual domain and potential malicious links**
* **Outdated content reused from an old campaign**

**Conclusion**

**Verdict:** **Phishing Attempt Identified**

The email is highly suspicious and should **not be trusted or interacted with**. Clicking on the tracking link could compromise the system or harvest credentials.