**Phishing Email Identification Report**

## **Analysis and Findings**

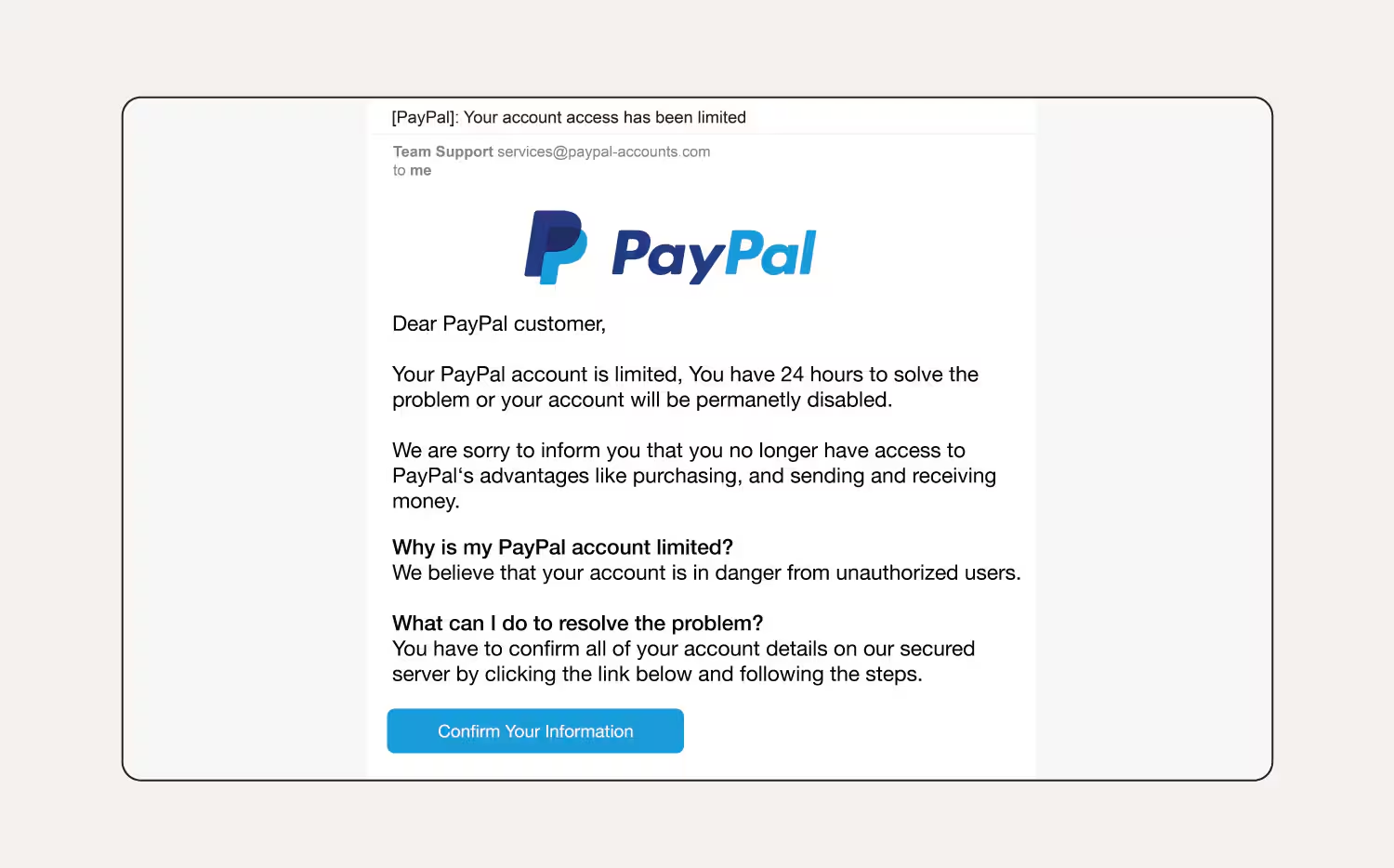
### **Example 1: Suspicious Email from PayPal**

Email Subject: "Your account access has been limited!"

📌 Sender: services@paypal-accounts.com (Spoofed address)

📌 Red Flags:

* The email is generic and does not include the user name.
* The email urges immediate action, asks the user to complete the action within 24 hours, and asks for sensitive information.

Image:  


### 

### 

### **Example 2: Suspicious Email from Apple iCloud**

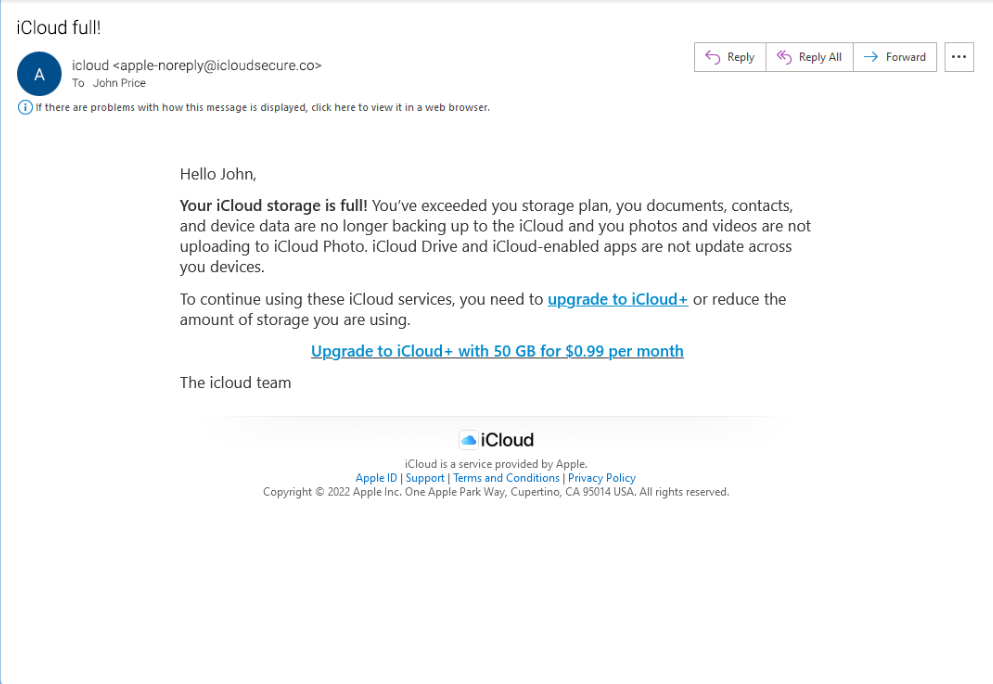
Email Subject: "iCloud full!"

📌 Sender:apple-noreply@icloudsecure.co

📌 Red Flags:

* There are lots of spelling errors.
* The email urges immediate action, or the user’s documents, files, photos, and videos will not back up to the iCloud server.

Image:



### **Example 3: Suspicious Email from PayPal**

Email Subject: "Your payment!"

📌 Sender:rajesh128674@gmail.com

📌 Red Flags:

* Asking the user to activate an account using the link, while the email is to inform the client about funds transfer.
* The sender's domain does not match the official platform website.
* The sender details indicated it is from a Gmail account (rajesh128674@gmail.com)

Image:

