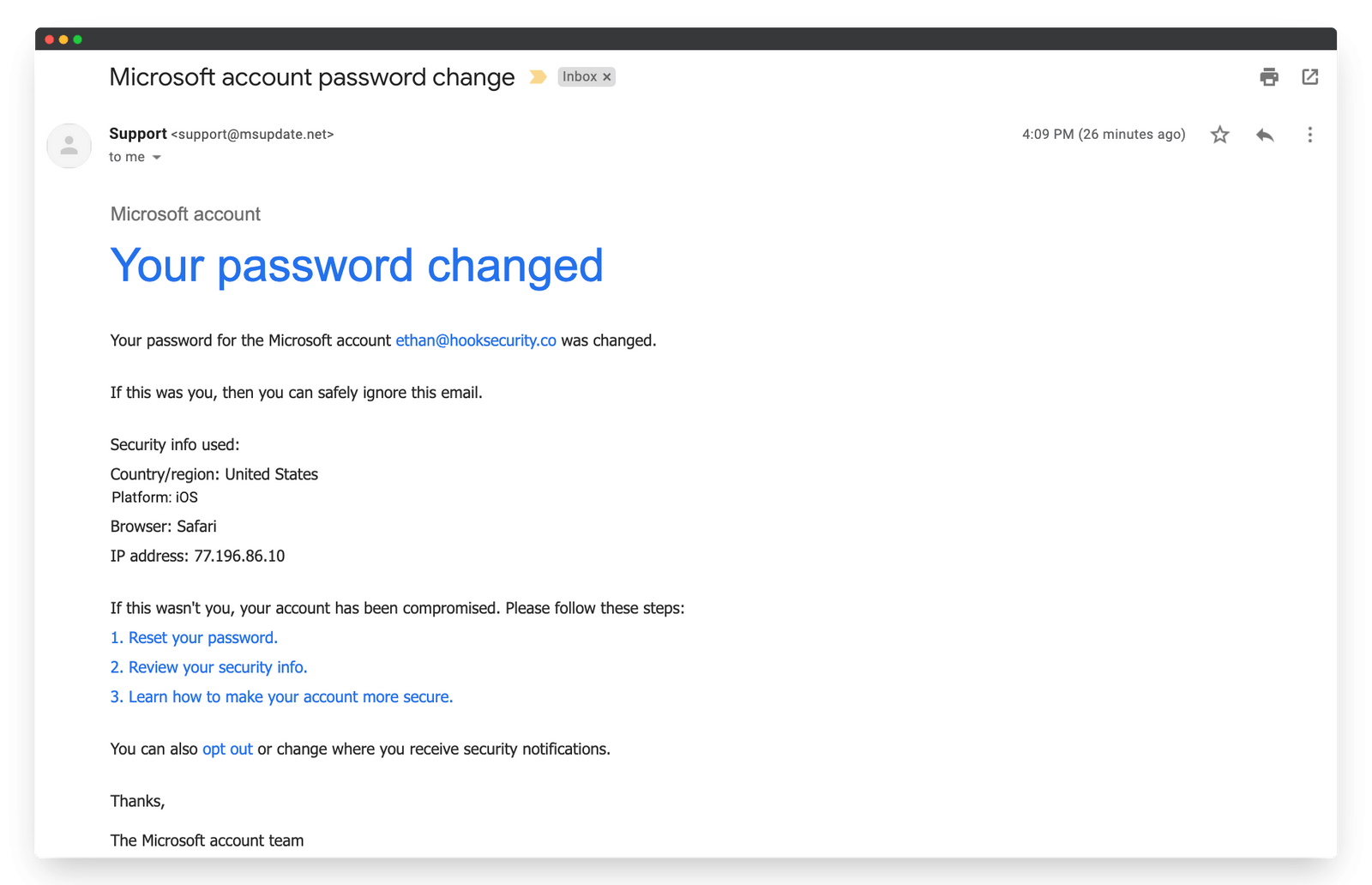
**Phishing Email Analysis Report**

**1. Sample Evidence**

**Attached Screenshot:**



**2. Summary of the Email**

The email claims to be from the **Microsoft account team** and notifies the user that their password has been changed. It provides links for resetting the password, reviewing security info, and securing the account. The message attempts to create urgency and trick the user into clicking malicious links.

**3. Phishing Indicators Found**

**a) Suspicious Sender Address**

* The sender email is **support@msupdate.net**, which is **not an official Microsoft domain**.
* Legitimate Microsoft emails would typically come from addresses like @microsoft.com or @account.microsoft.com.

**b) Urgent / Threatening Language**

* The email creates urgency by suggesting that if this was not you, your account has been compromised.
* Users are urged to take immediate action (reset password, review info).

**c) Suspicious Links**

* The clickable links (Reset your password, Review your security info, etc.) are highly suspicious.
* Hovering over such links (in a real email) often reveals **mismatched or malicious URLs** not belonging to Microsoft.

**d) Generic Greeting**

* The email does not address the user by full name.
* Instead, it uses a generic structure, which is common in phishing attempts.

**e) Visual Spoofing**

* The design mimics Microsoft’s legitimate style (logo, fonts, formatting) to **appear trustworthy**.

**4. Header Analysis (Limitations)**

* **Note:** Since this sample was provided as a **PNG screenshot**, raw email headers were not available for full analysis.
* In a real-world scenario, email headers would be extracted and analyzed using tools such as:
  + Google Admin Toolbox Header Analyzer
  + MxToolbox Email Header Analyzer
* A proper header check could reveal:
  + **Origin IP address** (likely not Microsoft).
  + **SPF/DKIM/DMARC failures**.
  + **Routing anomalies**.

**5. Conclusions**

This email is a **phishing attempt** that uses brand impersonation (Microsoft), urgency, and fake security alerts to trick the user into clicking malicious links.  
The combination of a spoofed sender domain, urgent wording, and suspicious hyperlinks strongly indicates that this is not a legitimate communication from Microsoft.