# Task2 Report

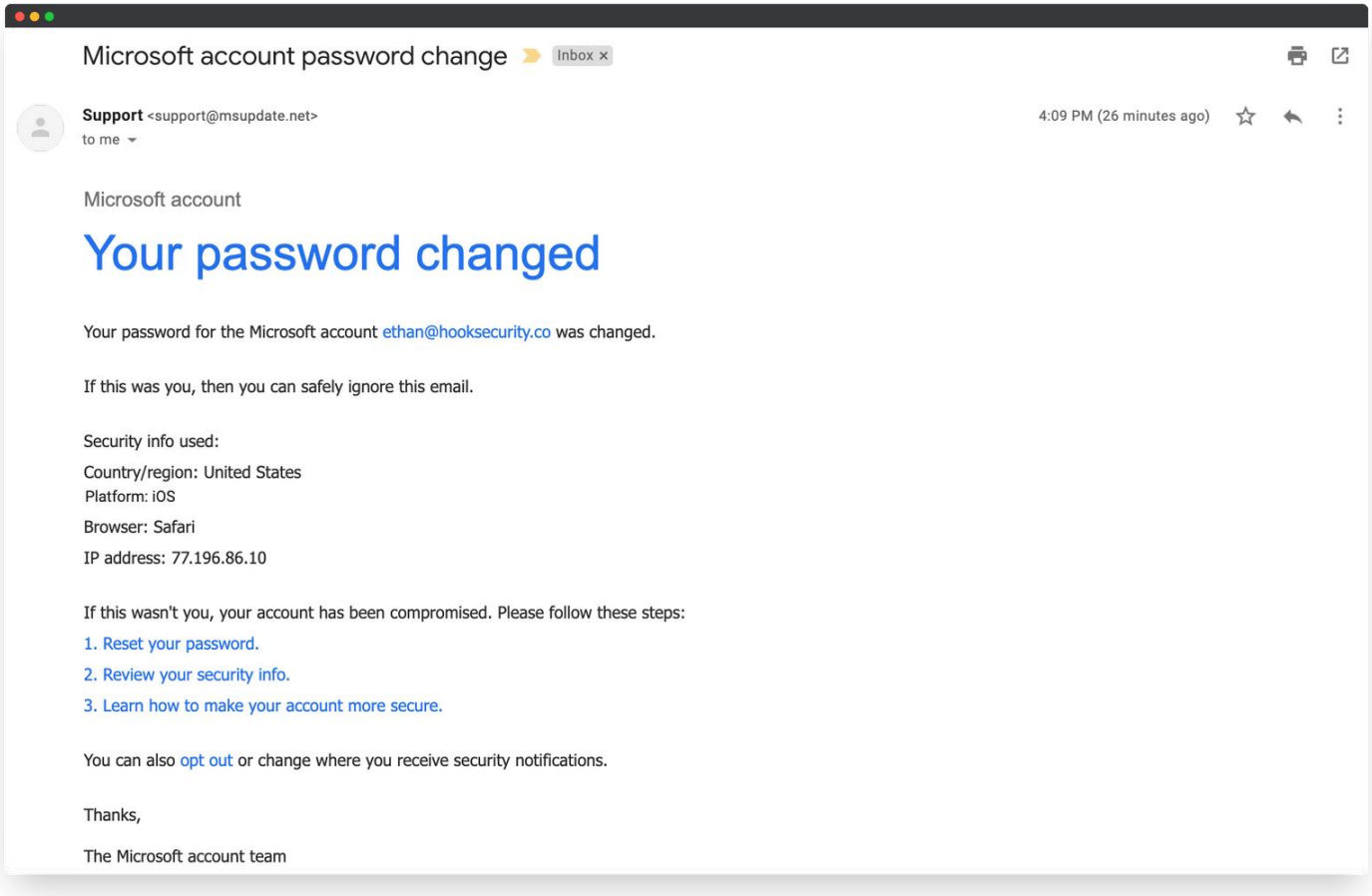
Overall Status: **Status**

Project Name: **Analyze a Phishing Email Sample**

Date: 27/05/25

**Objective: Identify phishing characteristics in a suspicious email sample.**
**Tools: Email client or saved email file (text), free online header analyzer.**

Example taken from: https://www.hooksecurity.co/phishing-examples/microsoft-phishing-example



Microsoft account password change Inbox ×

**Support** <support@msupdate.net>
to me

4:09 PM (26 minutes ago)

Microsoft account

## Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,

The Microsoft account team

Points in this email which clearly shows this is phishing email:

| Indicator | Explanation |
|---|---|
| **1. Sender Address**: support@msupdate.net | ✕ **Fake domain** — not a legitimate Microsoft domain (should be something like @microsoft.com or @account.microsoft.com). |
| **2. Generic Branding** | ✕ No official Microsoft logo or header design — Microsoft emails usually have professional branding. |
| **3. Poor Email Formatting** | ✕ Minimal formatting, plain text, no visual consistency — unusual for Microsoft, which uses branded templates. |
| **4. Sense of Urgency** | ✕ The message warns of a potential compromise, urging immediate action — a common phishing tactic. |
| **5. Hyperlinks (e.g., "Reset your password")** | ⚠ The actual URLs behind these links are not shown. Hovering over them (in a real scenario) would likely reveal suspicious, non-Microsoft URLs. |
| **6. IP Address Displayed** | ⚠ While not inherently suspicious, **legitimate services rarely show your IP address** like this in a password change notification. It's often used in phishing to make the email appear more technical and authentic. |
| **7. "opt out" link** | ✕ Reputable services typically don't offer an "opt out" of security notifications — this is often a trick to phish more data or verify active email addresses. |
| **8. To/From Field** | ✕ The "To" field shows **"to me"** with no personalization (e.g., name) — Microsoft typically uses your name or account alias. |
| **9. Unusual Language** | ⚠ Slightly off or robotic phrasing like "If this wasn't you, your account has been compromised." — legit providers usually use clearer, more natural phrasing. |
| **10. No Account Recovery Verification** | ✕ Microsoft usually includes extra verification steps (e.g., last 2 digits of phone number) in real recovery emails — this email lacks that. |