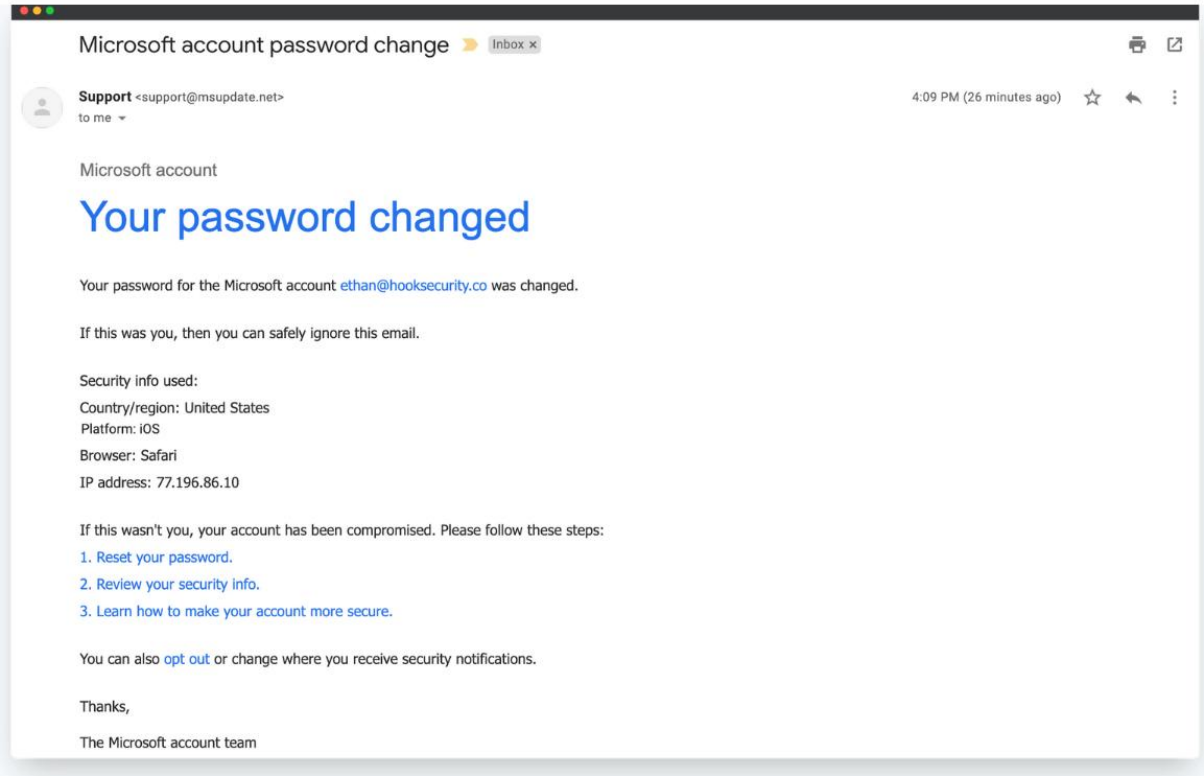
Phishing Email Analysis Report

Sampled Email:



Email Summary:

- **Subject:** Microsoft account password change
- **Sender:** support@msupdate.net
- **Claim:** Your Microsoft account password has been changed
- **Call to Action:** Reset password and review security info via embedded links

---

Phishing Indicators Found:

1. Suspicious Sender Address

- support@msupdate.net is **not an official Microsoft domain**.
- Legitimate Microsoft emails usually come from @accountprotection.microsoft.com, @microsoft.com, or @secure.microsoftonline.com.

2. Urgency & Fear Tactics

- The message says *"If this wasn't you, your account has been compromised."*
- Fear is a classic phishing trigger to rush the user into clicking.

3. Fake Links (Possible Spoofing)

- Phrases like:
    - Reset your password.
    - Review your security info.
    - Learn how to make your account more secure.
      These are all **hyperlinked** but the real destination URL isn't visible in the screenshot.

These are commonly used to redirect victims to fake Microsoft login pages to steal credentials.

4. Impersonation of Microsoft Branding

- Uses Microsoft styling, logos, and common phrasing like:
    - "The Microsoft account team"
- Despite visual similarity, branding alone does not prove authenticity.

5. Grammar and Structure (Neutral)

- The grammar and structure appear professional — this makes it more convincing.
- However, **lack of personalization** ("Hello [Name]" or account number) is suspicious.

6. IP Address Used for Login

- Shows IP: 77.196.86.10 — meant to give a false sense of legitimacy.
- This is a social engineering trick to add realism.

✅ Conclusion:

This is a phishing email.
It impersonates Microsoft to steal login credentials using fake urgency, a spoofed domain, and fake login links.