☑Phishing Email Analysis Report

Task: Analyze a Phishing Email Sample
Objective: Identify phishing characteristics in a suspicious email
Tools Used: Email client screenshot, manual analysis

□ Email Snapshot Summary

Field	Value
From	`support@msupdate.net`
Subject	Microsoft account password change
Recipient	ethan@hooksecurity.co
IP Address	77.196.86.10
Platform	iOS
Browser	Safari
Links in email	Password reset, review security, security tips, opt-out

---

□ Phishing Indicators Found

#	Indicator	Details
1	**Suspicious Sender Domain**	The email is from `@msupdate.net` — this is **not an official Microsoft domain** (should be `@microsoft.com`).
2	**Generic Content**	The email refers to "ethan@hooksecurity.co" but doesn't use a full name or personalized greeting.
3	**Fear-based Language**	Warnings like *"your account has been compromised"* push urgency.
4	**Multiple Links**	Includes links with text like "Reset password", "Review your security info", which may redirect to phishing sites.
5	**No Digital Signature**	There's no DKIM, SPF, or verification info shown — raises doubts about authenticity.
6	**Unknown IP Mention**	The IP `77.196.86.10` could be used to confuse or scare the recipient into acting.

✖Why This Email is Suspicious

- **Microsoft will never send account alerts from an unverified domain** like `msupdate.net`.
- Phishing emails often **mimic security alerts** to scare users into clicking fake password reset links.
- URLs should be hovered and verified before clicking — here, link destinations are unknown and unverified.

- Legitimate emails will have **DKIM/SPF pass, correct branding, and digital signatures**.

☑Conclusion

This email is a **probable phishing attempt**.
It contains **spoofed sender address**, **fear-inducing language**, and **suspicious links** to trick the user into resetting a password on a fake site. Such emails should be **reported and deleted immediately**.