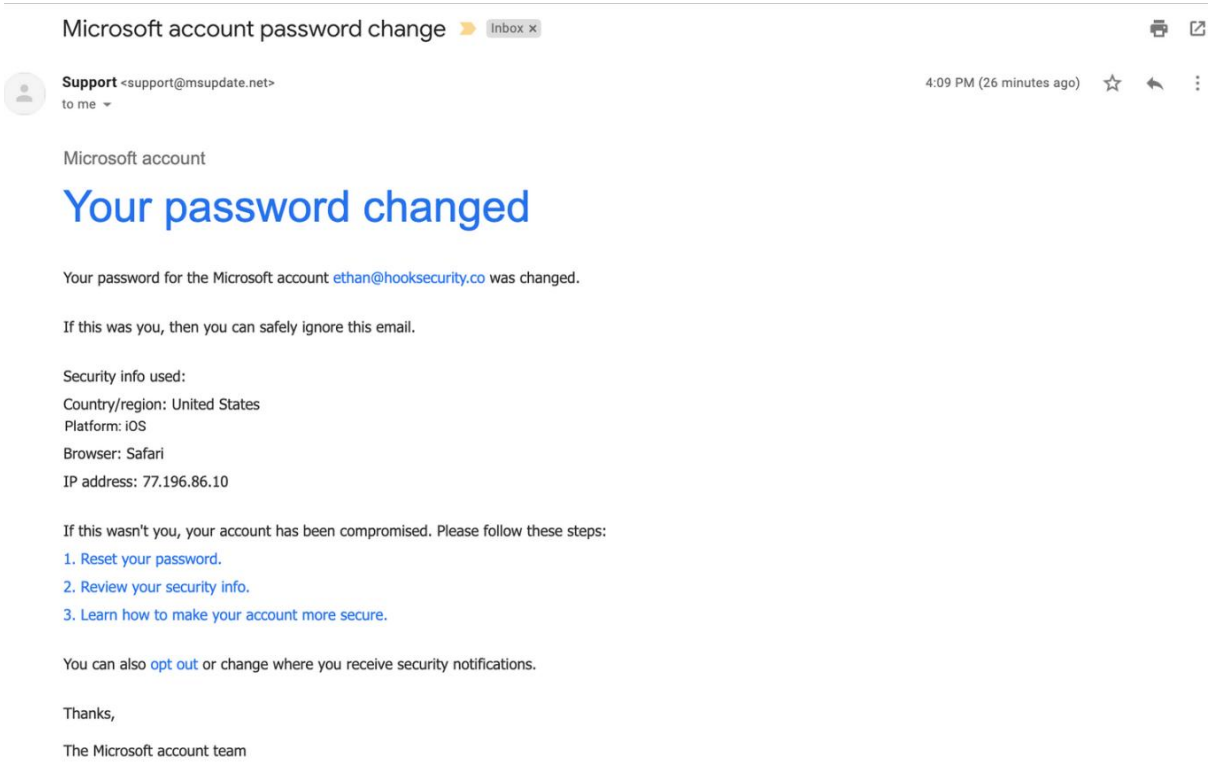
Task 2: Analyze a Phishing Email Sample.

Phishing:- Phishing is a type of cyberattack where attackers pretend to be a trusted person or organization (like a bank, email provider, or government agency) to trick people into giving away sensitive information, such as:

- Passwords
- Credit card numbers
- OTPs or PINs
- Personal details (like date of birth, address, etc.)

A Sample Phishing Email



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

Here the sender's address is support@msupdate.net

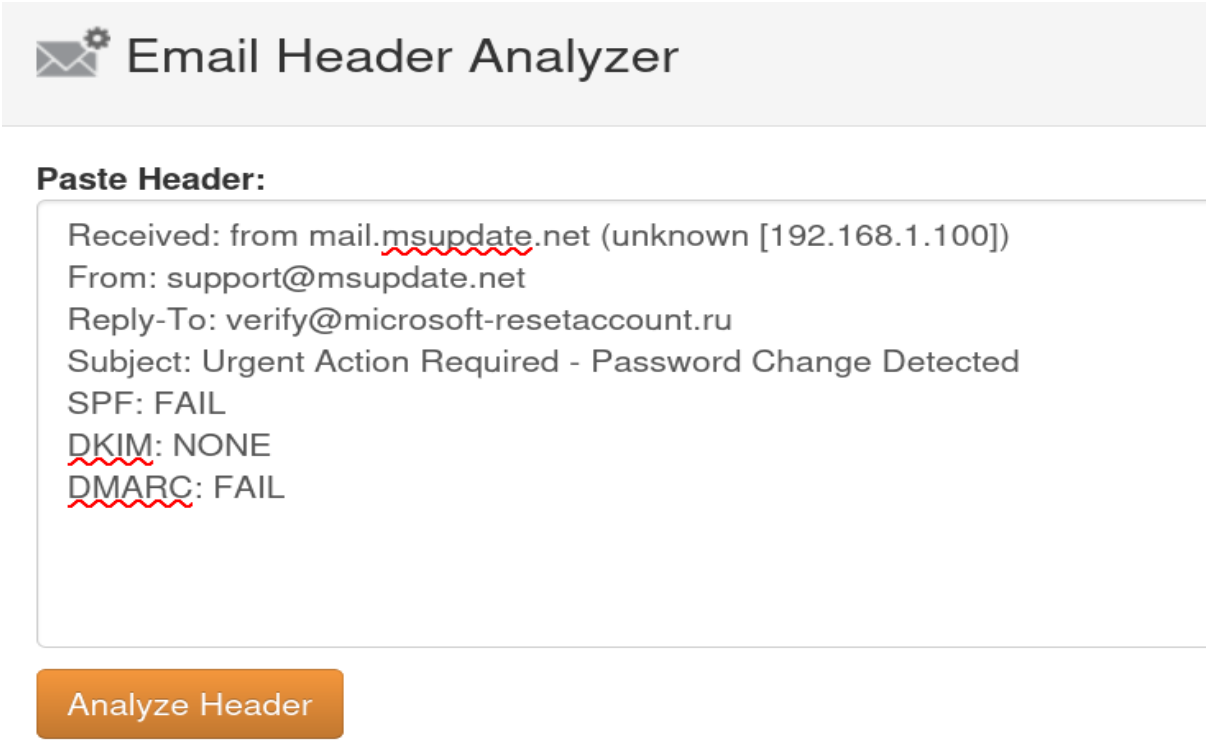
This email address is a spoofed or fake sender address.

It pretends to be from Microsoft, a well-known global technology company. The attacker wants the user to trust the email and click on the malicious links inside it.

The domain is: “msupdate.net”. It mimics Microsoft branding by using the abbreviation “ms” commonly used for Microsoft and the word “update” to sound technical and trustworthy. However, this is not an official Microsoft domain (Microsoft uses microsoft.com, outlook.com, etc.). This is a common phishing trick known as domain spoofing or lookalike domain attack, where attackers use similar-looking domains to fool users into believing the message is genuine.

Email Header Analysis

I used MXToolbox to analyze the email header of a suspicious message with the subject “Urgent Action Required – Password Change Detected.”



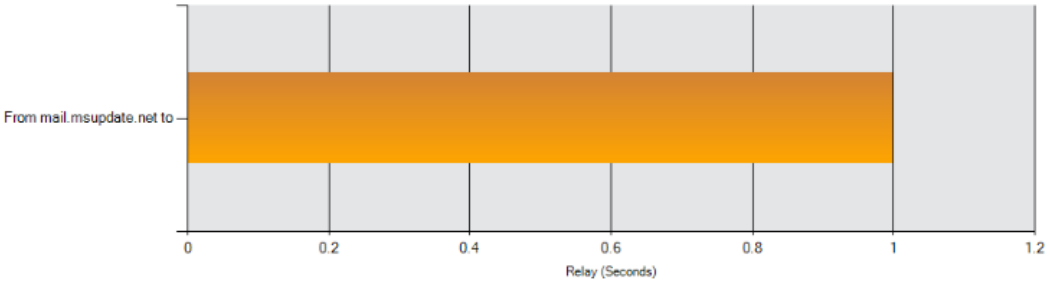
Header Analyzed

Email Subject: Urgent Action Required - Password Change Detected

Delivery Information

Relay Information

Received Delay: 0 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mail.msupdate.net 192.168.1.100			[]	

SPF and DKIM Information

Headers Found

Header Name	Header Value
From	support@msupdate.net
Reply-To	verify@microsoft-resetaccount.ru
Subject	Urgent Action Required - Password Change Detected
SPF	FAIL
DKIM	NONE
DMARC	FAIL

Received Header

```
Received: from mail.msupdate.net (unknown [192.168.1.100])
From: support@msupdate.net
Reply-To: verify@microsoft-resetaccount.ru
Subject: Urgent Action Required - Password Change Detected
SPF: FAIL
DKIM: NONE
DMARC: FAIL
```

Permanently forget this email header

The analysis revealed multiple red flags indicating a phishing attempt:

- The “From” address was support@msupdate.net, but the “Reply-To” was set to a suspicious domain verify@microsoft-resetaccount.ru, which impersonates Microsoft using a Russian (.ru) domain.
- The email failed SPF and DMARC checks, and DKIM was not configured (NONE), indicating that the sender was not authorized to send emails on behalf of the stated domain.
- The mail was received from a private IP address (192.168.1.100), which is not valid for legitimate public email servers.

These findings strongly suggest that the email is spoofed and likely a phishing attempt, designed to deceive the recipient into clicking malicious links or providing sensitive information.

Suspicious Links or Attachments

- The email contains three clickable blue hyperlinks:
    - 1. Reset your password
    - 2. Review your security info
    - 3. Learn how to make your account more secure
- These could be phishing links designed to steal user credentials.

Urgent or Threatening Language

- "If this wasn't you, your account has been compromised." This is a threatening, high-pressure statement designed to scare the recipient into clicking quickly.

Mismatched URLs

- We cannot hover over the links in the image, but in phishing emails, the visible link text may appear legitimate while the actual destination is malicious. Needs hover action in a real inbox to confirm.

Spelling or Grammar Errors

- Minor inconsistency: “opt out or change where you receive security notifications” lacks punctuation and feels off.
- Otherwise, no major spelling or grammar issues detected.

Analysis of Suspicious Email Characteristics

The email shows several key signs of phishing:

1. Fake Sender Domain: The message was sent from support@msupdate.net, which is not an official Microsoft domain, indicating domain spoofing.
2. Urgent and Threatening Language: The email claims the user's account has been compromised and urges immediate action, creating a sense of panic.
3. Suspicious Links: The email includes multiple hyperlinks (e.g., "Reset your password", "Review your security info") that could potentially lead to malicious or fake login pages.
4. Mismatched Sender and Brand: The email pretends to be from Microsoft but is not sent from a Microsoft-owned domain.

5. Minor Language Issues: Slightly unnatural phrasing like “opt out or change where you receive security notifications” adds to suspicion, though no major spelling errors are present.
6. Impersonation of a Trusted Entity: The layout and tone mimic real Microsoft notifications to build false trust.

These characteristics strongly suggest the email is a phishing attempt intended to steal user credentials or personal information.