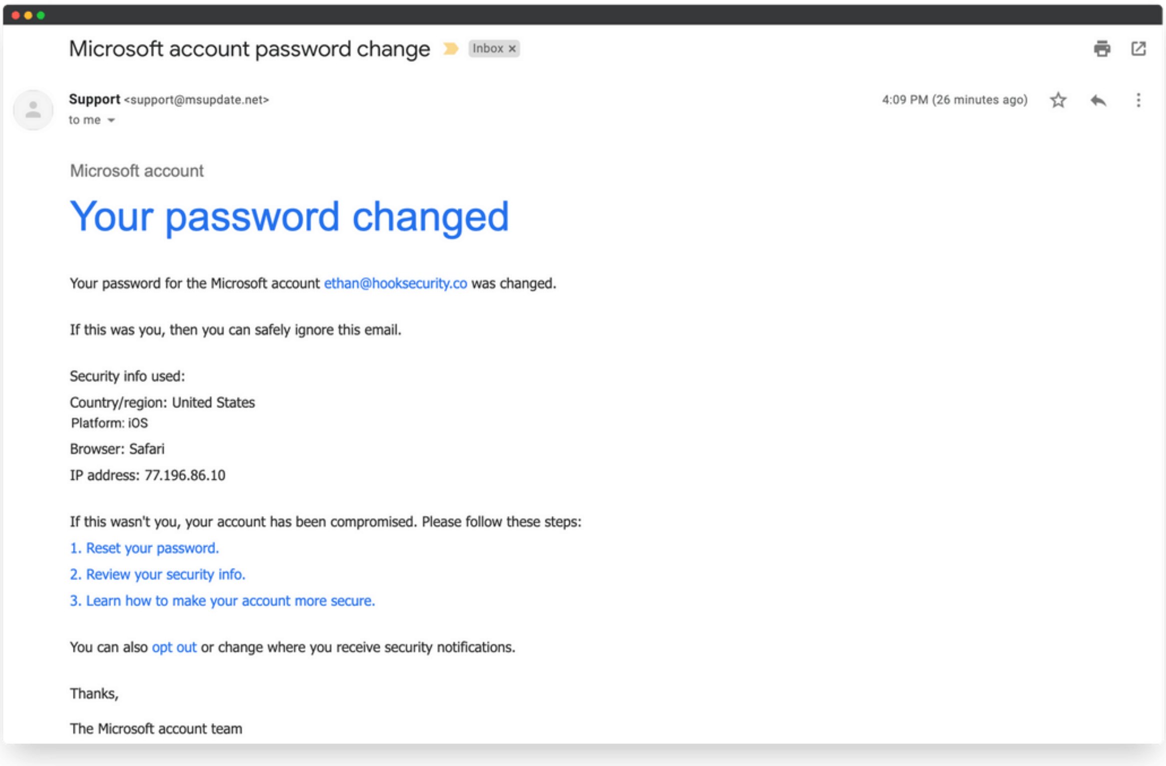
Task 2

Objective: Identify phishing characteristics in a suspicious email sample.
Tools: Email client or saved email file (text), free online header analyzer.
Deliverables: A report listing phishing indicators found.

Note: In this report I have used 3 sample for phishing analysis.

Sample Email Source

1. Sample1 - Password change alert



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,

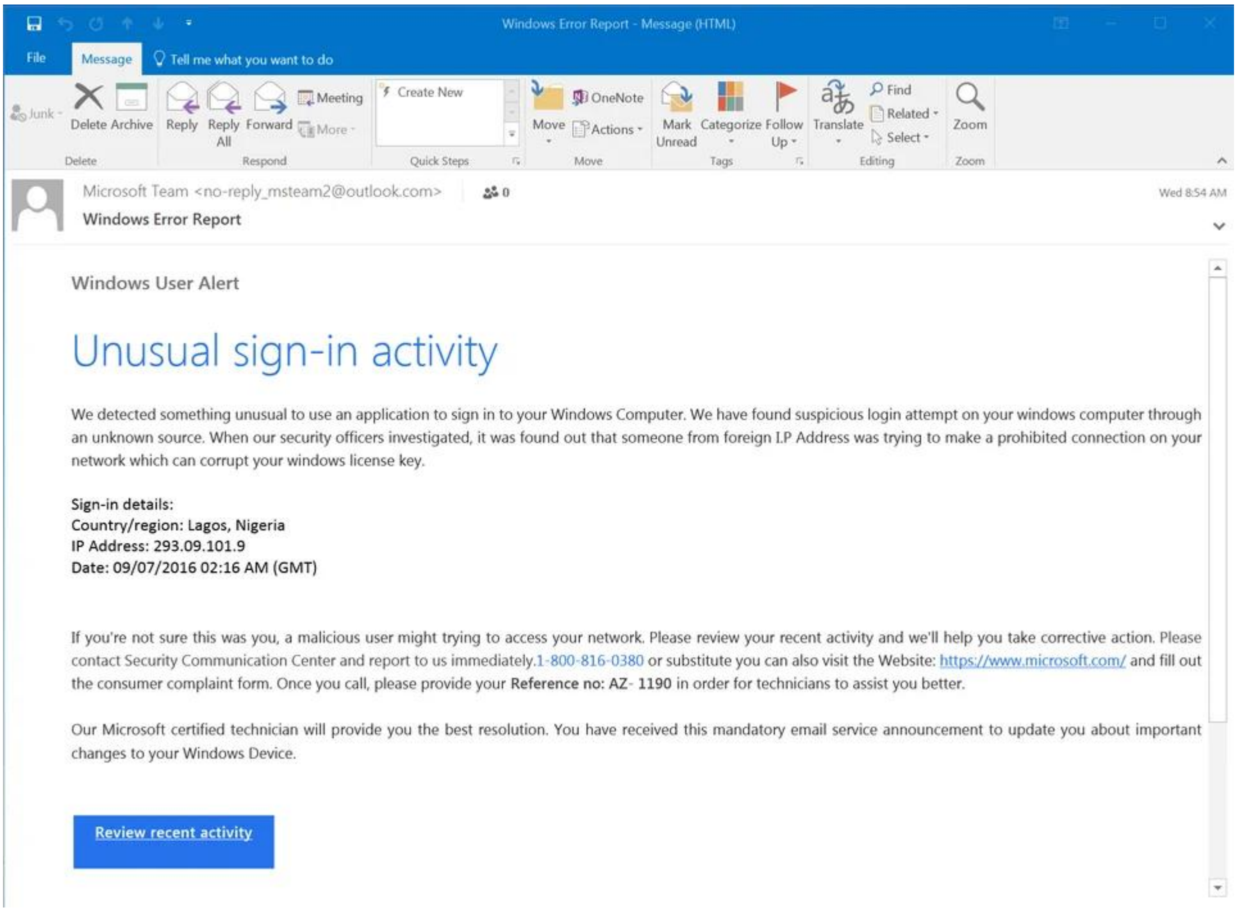
The Microsoft account team

(Fig. 1)

Reasons of Suspicion:

a. Suspicious sender domain (msupdate.net, not microsoft.com).
b. Classic sense-of-urgency tactics ("If this wasn't you, your account has been compromised").
c. Prominent password-reset links.
d. Generic language and closing.
e. Mimicking a legitimate Microsoft alert.

2. Sample 2 – Unusual activity alert



Microsoft Team <no-reply_msteam2@outlook.com>
Windows Error Report
Wed 8:54 AM

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

(Fig. 2)

Reasons of Suspicion:

- The sender's domain is unofficial and untrustworthy.
- The message relies on urgency, fear, and requests personal interaction (phone call or clicking a button).
- Invalid IP and grammar errors.
    - "windows computer" / "windows license key" – 'W' must be capital.
    - "through an unknown source" – "from an unknown source".
    - "foreign I.P Address" – No periods in IP & 'a' must be lowercase.
    - Overuse of passive voice.
- Legitimate Microsoft security alerts are far more specific, have proper branding, and come from trusted domains.

3. Sample 3 – Email analysis
   This is a sample of the complete email header.

```
Received: from SA3PR19MB7370.namprd19.prod.outlook.com (::1) by
 MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 19 Sep 2023 18:36:46
 +0000
Received: from BN0PR03CA0023.namprd03.prod.outlook.com (2603:10b6:408:e6::28)
 by SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.27; Tue, 19 Sep
 2023 18:36:45 +0000
Received: from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com
 (2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com
 (2603:10b6:408:e6::28) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.28 via Frontend
 Transport; Tue, 19 Sep 2023 18:36:45 +0000
Authentication-Results: spf=temperror (sender IP is 137.184.34.4)
 smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not
 signed) header.d=none;dmarc=temperror action=none
 header.from=atendimento.com.br;compauth=fail reason=001
Received-SPF: TempError (protection.outlook.com: error in processing during
 lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout)
Received: from ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4) by
 BN8NAM11FT066.mail.protection.outlook.com (10.13.177.138) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.6813.19 via Frontend Transport; Tue, 19 Sep 2023 18:36:44 +0000
```

Reasons of suspicion:

a. Point out that the critical link (*https://blog1seguimentmydomaine2bra.me/*) is not a legitimate domain and likely malicious.
b. Authentication failed for domain '*atendimento.com.br'*, indicating the email may be spoofed or forged. - the sending infrastructure doesn't match the claimed sender's domain and authentication fails.

Precaution measure:

a. **Verify the Sender's Email Address Carefully:** - Always check the sender's email domain. Official emails come from trusted, verified. Be suspicious of misspelled or unfamiliar domains.
b. **Hover Over Links Before Clicking:** Hover your mouse pointer over links to see the actual URL destination. Do not click if the URL looks suspicious or doesn't match the claimed institution.
c. Avoid Clicking on Links or Downloading Attachments from Unknown Sources
d. **Keep Software and Security Tools Updated - Regularly** update your operating system, browsers, email clients, and antivirus software to protect against exploitation of known vulnerabilities.
e. Use Multi-Factor Authentication (MFA)