Task 2

**Objective:** Identify phishing characteristics in a suspicious email sample.

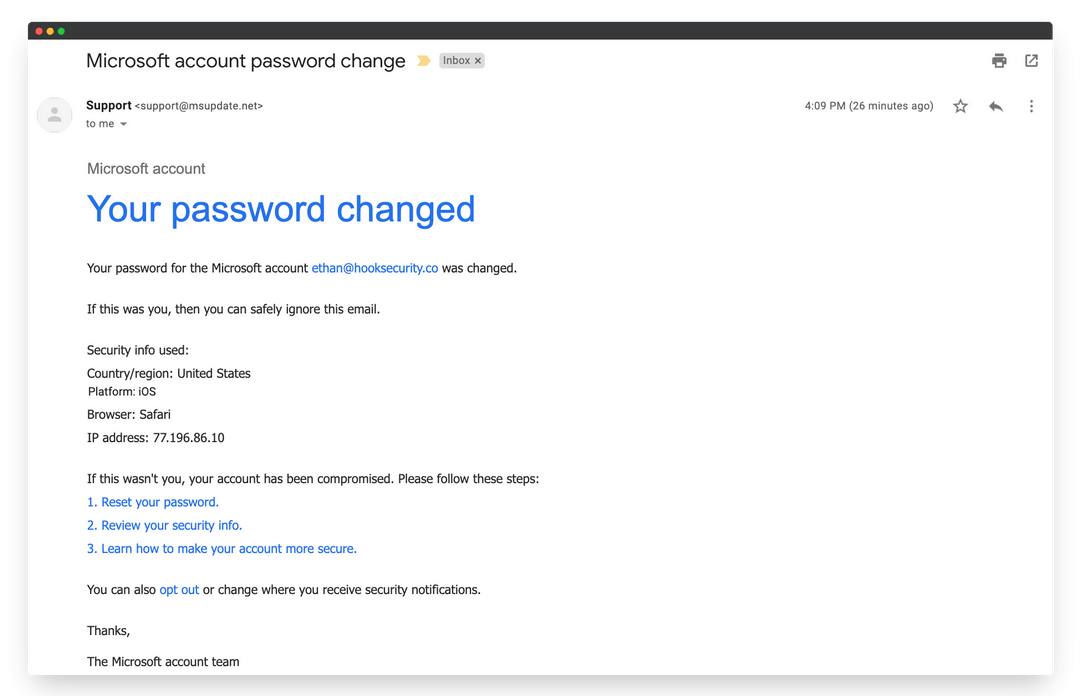
**Tools:** Email client or saved email file (text), free online header analyzer.

**Deliverables:** A report listing phishing indicators found.

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

Sample Email Source

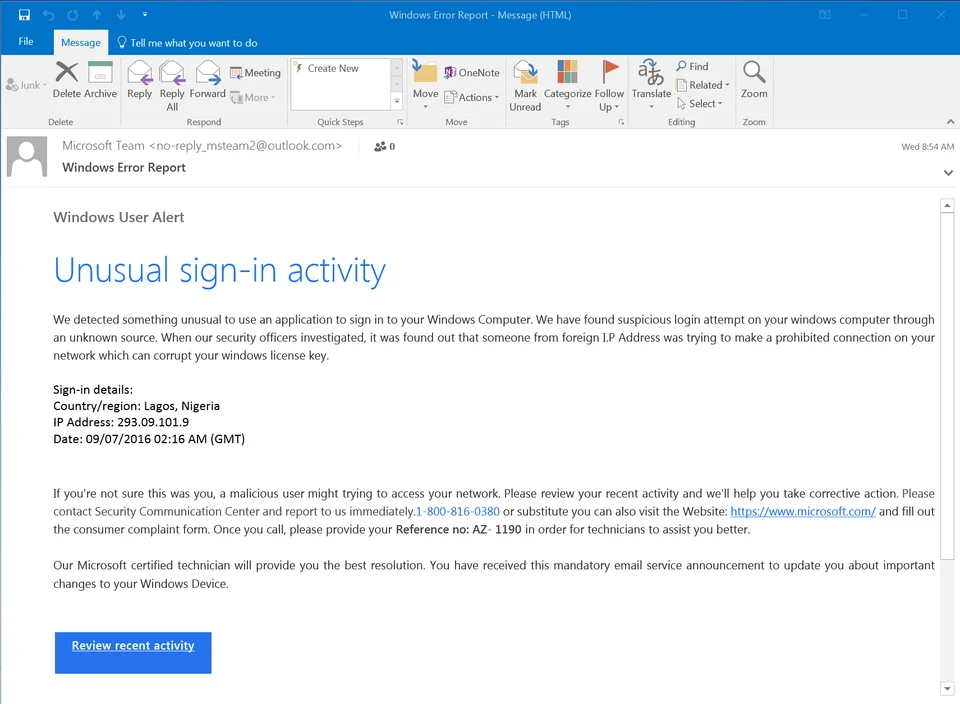
1. Sample1 - Password change alert



(*Fig. 1*)

Reasons of Suspicion:

1. Suspicious sender domain (msupdate.net, not microsoft.com).
2. Classic sense-of-urgency tactics (“If this wasn’t you, your account has been compromised”).
3. Prominent password-reset links.
4. Generic language and closing.
5. Mimicking a legitimate Microsoft alert.
6. Sample 2 – Unusual activity alert



(*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.

1. 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:

1. Point out that the critical link (*https://blog1seguimentmydomaine2bra.me/*) is not a legitimate domain and likely malicious.
2. 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:

* 1. **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.

* 1. **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.
  2. Avoid Clicking on Links or Downloading Attachments from Unknown Sources
  3. **Keep Software and Security Tools Updated - Regularly** update your

operating system, browsers, email clients, and antivirus software to protect against exploitation of known vulnerabilities.

* 1. Use Multi-Factor Authentication (MFA)