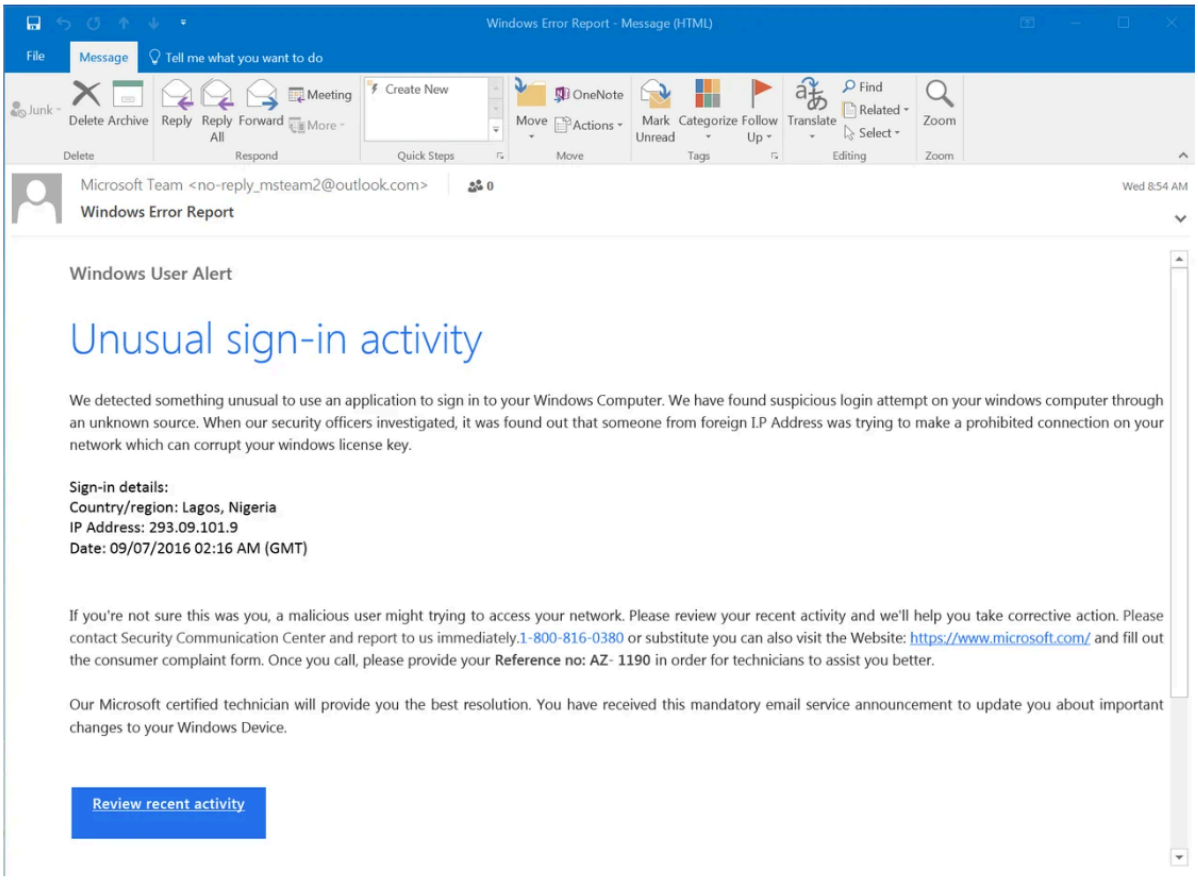

Phishing Email Analysis Report
Subject: Windows Error Report - Unusual sign-in activity

Sender: Microsoft Team no-reply_msteam2@outlook.com

Date/Time: Wed 8:54 AM (date not fully visible)

Email Client: Microsoft Outlook (HTML message)

1. Sender Analysis
The sender address is no-reply_msteam2@outlook.com.
Legitimate Microsoft emails typically come from official Microsoft domains such as @microsoft.com or @windows.com.
The use of a generic Outlook.com address is suspicious and a common tactic in phishing.
2. Subject and Header
The subject "Windows Error Report" and "Unusual sign-in activity" are designed to create urgency and fear.
The email claims to be from "Microsoft Team," which is vague and not an official Microsoft team name.

3. Content and Language
The email uses formal language but contains multiple grammatical and stylistic errors, such as:
"We detected something unusual to use an application to sign in to your Windows Computer." (awkward phrasing)
"We have found suspicious login attempt" (missing plural "attempts")
"unknown source" is misspelled as "unkonwn source" (typo)
"foreign I.P Address" (unusual capitalization and spacing)
"corrupt your windows license key" (Windows should be capitalized)
These errors are typical in phishing emails.
4. Technical Details Provided
The email provides sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9 (Invalid IP address; IP octets range from 0-255)
Date: 09/07/2016 02:16 AM (GMT) — outdated date, likely to confuse or mislead
The invalid IP address is a strong indicator of phishing.
5. Call to Action
The email urges the recipient to contact a "Security Communication Center" via phone number 1-800-816-0380 or visit the website https://www.microsoft.com/.
The phone number is suspicious and not verifiable as an official Microsoft support number.
The website link appears legitimate but could be a disguised hyperlink leading elsewhere (not verifiable from the image alone).
The email asks for a "Reference no: AZ-1190" to be provided when calling, a common tactic to make the scam appear official.
6. Visual and Structural Elements
The email uses a blue button labeled "Review recent activity" to entice clicking.
The button likely contains a malicious link (not visible in the image).
The email layout mimics Microsoft’s style but lacks official branding elements like logos or trademarks.
The sender’s profile picture is a generic placeholder, not a Microsoft logo.
7. Security and Phishing Indicators
Use of a free email service (Outlook.com) instead of official Microsoft domain.
Poor grammar and spelling mistakes.
Invalid IP address in the sign-in details.
Urgency and fear tactics to prompt immediate action.
Suspicious phone number and vague references to "Security Communication Center."
Potentially malicious call-to-action button.
Lack of official Microsoft branding and digital signatures.