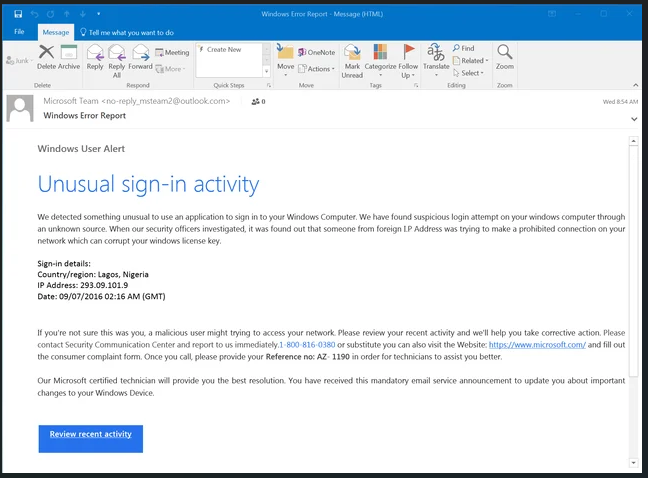
Task 2: Analyze a Phishing Email Sample

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



This is a sample phishing email that mimics a **Microsoft Windows Error Report** message.

## Examine Sender’s Email Address for Spoofing

* **Sender:** Microsoft Team <rep\_msteam2@outlook.com>
* 🚩 **Red flag**: Official Microsoft messages would come from a **microsoft.com** domain (e.g., support@microsoft.com), not **Outlook.com**.

## Identify Suspicious Links or Attachments

* The button says **“Review recent activity”**, but the actual destination is **unknown**.
* These buttons are commonly **hyperlinked to malicious websites** or **phishing forms**.
* Also includes a **phone number**, which is a classic **tech support scam tactic**.

## Look for Urgent or Threatening Language

* Phrases like:  
  + “Unusual sign-in activity”
  + “someone from foreign IP Address”
  + “corrupt your windows license key”
  + “Please review your recent activity”
  + “immediately”
* 🚨 These are meant to scare the reader into taking quick, irrational action.

## Note Any Mismatched URLs

* Since this is a screenshot, we can’t hover. But legitimate emails from Microsoft would link to:  
  + https://account.microsoft.com
  + https://login.live.com
* The button might redirect to a fake login page or malware site if hovered.

## Verify Spelling or Grammar Errors

There are a few oddities:

* “an application to sign in to your Windows Computer” → awkward phrasing.
* “prohibited connection on your network which can corrupt your windows license key” → unlikely technical statement.
* Missing commas, inconsistent capitalizations (e.g., "Microsoft certified technician").

## Summary: Phishing Traits Found

* Spoofed Email: Uses an Outlook email instead of Microsoft’s official domain.
* Header Not Available: But the sender domain alone is suspicious.
* Suspicious Link/Button: “Review recent activity” likely leads to a phishing/malware site.
* Urgency/Threat: Warns about account compromise, corrupted license key, and urges immediate action.
* Mismatched Contact: Asks user to call a non-Microsoft number (1-800-816-0830).
* Grammar/Phrasing Issues: Several awkward or technically incorrect phrases.
* Branding: Uses Microsoft logo and style to build false legitimacy.
* Scam Pattern: Classic \*\*tech support scam\*\* meant to scare users into calling and giving control or paying.