**Phishing Email Analysis Report**

Email Sample: "Unusual sign-in activity – Microsoft account" (attachment: sample-10.eml)

**1. Sample Phishing Email Overview**

The email claims to be from Microsoft, warning about a recent unusual sign-in from Russia. It suggests that if the sign-in wasn’t authorized, the user should "report the user." The message tries to look like an official security alert.

**2. Sender Email Address Check**

The sender’s address looks suspicious. Instead of coming from a genuine Microsoft domain like microsoft.com or account.microsoft.com, it appears to be from a strange or unrelated domain. This is a strong sign that someone is trying to impersonate Microsoft to trick users.

**3. Email Header Review**

Although we don't have the full email headers here, phishing emails often fail important sender verification checks like SPF, DKIM, and DMARC. These failures help identify emails that are not truly from the companies they pretend to be from. The received paths usually show the email coming from unknown or suspicious servers, not official Microsoft email servers.

**4. Suspicious Links or Attachments**

This email includes a call-to-action asking the user to "report the user" if the activity wasn’t theirs. The actual link hidden behind this text is likely not a Microsoft website but a fraudulent one trying to capture login details or install malware. No attachments are present in this example, but links themselves pose a dangerous threat.

**5. Language Indicating Urgency or Threat**

The email tries to create a sense of urgency by suggesting that an unauthorized login happened and the user must act quickly. Phrases like “If this wasn't you, please report the user” encourage recipients to click without carefully checking the email’s legitimacy.

**6. Mismatched URLs**

Hovering over the "report the user" link would almost certainly reveal a web address different from Microsoft’s official domains. This mismatch is a classic warning sign that the email aims to trick recipients into visiting a malicious site.

**7. Spelling, Grammar, and Tone**

The message is fairly well-written but uses somewhat generic language. For example, the phrase “If this was you, we'll trust similar activity in the future” sounds a bit awkward and less polished than genuine Microsoft communications. Legitimate emails typically use specific, professional language and personalized greetings, which this email lacks.

**8. Summary of Phishing Indicators**

| **Aspect** | **Observation** |
| --- | --- |
| Sender Address | Fake or unrelated domain, not from Microsoft |
| Header Information | Likely fails authentication checks; suspicious sending servers |
| Suspicious Links | Link leads to a non-Microsoft URL |
| Urgent Tone | Uses fear of unauthorized access to pressure immediate action |
| URL Mismatch | Link text doesn’t match actual destination |
| Language & Tone | Generic phrasing and slightly unnatural wording |
| Lack of Personalization | No recipient name or personalized info |
| No Attachments | N/A |

**Final Thoughts**

This email clearly tries to impersonate Microsoft to scare users into clicking on a malicious link. The combination of a spoofed sender, suspicious links, urgency in tone, and unnatural phrasing strongly suggests it's a phishing attempt. Anyone receiving such a message should delete it immediately and avoid clicking any links.