Phishing Email Detection & Analysis

1. **What is Phishing?**

   Phishing is a cybercrime where attackers pretend to be trustworthy entities (like banks, tech companies, or even friends) trick you into clicking false links, sharing confidential information, or installing malware. Most phishing comes via email, but it can happen through SMS (smishing), phone calls (vishing), and fake websites.

2. **Types of Phishing**

- **Email Phishing**: Attackers send malicious emails pretending to be a legitimate company.
- **Spear Phishing**: Targeted Phishing aimed at individuals or specific organizations, with personalized info.
- **Whaling**: A type of spear phishing targeting executives or high-profile targets.
- **Smishing**: Phishing via SMS text messages.
- **Vishing**: Phishing via voice calls.
- **Clone Phishing**: Attackers make a near-identical copy of a real email with a malicious link or attachment.
- **Business Email Compromise (BEC):** Hacking or spoofing business emails to trick staff into sending money or data.

3. **About the sample that I took:**
   The analysed email is a classic **Email Phishing** attack using "**typosquatting**" (the use of "micr0soft" with a zero) to mimic Microsoft.

4. **The Phishing Email Sample:**
   From: account-security@micr0soft-support.com
   To: you@example.com
   Subject: Urgent: Unusual Sign-in Activity Detected on Your Microsoft Account

   Dear User,

   We detected an unusual sign-in attempt to your Microsoft account from a new device.

   Location: Moscow, Russia
   Device: Windows 10 - Chrome Browser
   Time: August 5, 2025, 03:24 AM GMT

   If this was you, you can safely ignore this email.
   If not, we recommend you **verify your identity immediately** to secure your account.

[Click here to verify your account] (http://micr0soft-verify-login.com/login?session=compromised)

Failure to act within 24 hours may result in temporary suspension of your account.

Thank you,
Microsoft Security Team
support@micr0soft-support.com

5. Step-by-Step Detection

A. Check the Sender's Email Address

- **We can see as below:**
  account-security@micr0soft-support.com
  - *Looks like Microsoft, but "micr0soft" uses a zero instead of "o".*
  - This is called "typosquatting"- a common technique in phishing.

B. Email Headers

- I analysed sample headers on MX Toolbox's Header Analyzer - https://mxtoolbox.com/EmailHeaders.aspx. - refer "header-analysis.txt" for sample header.
- **See attachment for results.**
  - I have extracted all the information and uploaded as "Sample Email Header Analyzer – MxToolbox"
  - **SPF:** Fail (sender not authorized for the "micr0soft-support.com" domain).
  - **DKIM/DMARC:** Not found (no authentication).
  - **Source IP:** Does not match Microsoft's legitimate mail servers.

6. Noticed Urgent/Threatening Language

- Phrases like "Urgent," "Unusual Sign-in," "Failure to act within 24 hours," and "may result in temporary suspension" are intended to worry and rush a user.

7. Greeting and Grammar

- Greets you as "Dear User" (not your name).
- Language is formal but generic. Phishers often avoid using personal info to reach more people at once.

8. Attachments or Other Evidence

- No attachments in this case.
- Need to be extra cautious if there are files to download, especially if they're .exe, .zip, .scr, etc.

9. How to Stay Safe from Phishing

1. **Always check the sender's email address carefully.**
2. **Hover over links before clicking**, make sure the link matches the supposed company's real website.
3. **Look for urgent or threatening language** trying to scare or rush you.
4. **Check for misspellings and typos** in brand names, domains, or message text.
5. **Never download or open attachments** you weren't expecting.
6. **If in doubt, go directly to the official website,** don't use links in the email.
7. **Keep your computer and browser up to date** to defend against malware.
8. **Confirm any suspicious request by contacting the company directly.**