1. Obtain a sample phishing email:
- Subject: Security Alert: Unusual sign-in detected
From: "Microsoft Support"
Body:
Dear User,
We detected an unusual sign-in attempt to your account from an unknown device.
If this was not you, please verify your account immediately:
https://login.microsoft.com.account-verify-alert.net
If you do not confirm within 12 hours, your account will be locked.

2. Examine sender's email address for spoofing:
- Address: alert@m1crosoft-support.com — "i" in Microsoft replaced with "1", and domain is not microsoft.com.

3. Check email headers for discrepancies:
- The sending server's IP does not belong to Microsoft; SPF/DKIM/DMARC checks fail.

4. Identify suspicious links or attachments:
- Link: https://login.microsoft.com.account-verify-alert.net — domain is actually account-verify-alert.net, not microsoft.com.
- No attachments here, but phishing emails often contain malicious documents.

5. Look for urgent or threatening language:
- "Your account will be locked in 12 hours" — forces quick action.

6. Note any mismatched URLs:
- Visible link looks like Microsoft but points to a completely different domain.

7. Verify presence of spelling or grammar errors:
- Slightly awkward phrasing: "If this was not you, please verify your account immediately."

8. Summarize phishing traits found:
- Spoofed sender address using character substitution.
- Domain mismatch and impersonation of a trusted brand.
- Suspicious URL resembling Microsoft but hosted on another domain.
- Urgent warning to pressure the victim.
- Slight grammar and tone issues.
- Generic greeting instead of personalized name.