Phishing Email Analysis Report

1. Obtain a Sample Phishing Email

The phishing email sample was obtained from PhishTank (https://www.phishtank.com), a reliable source for real-world phishing data. The selected entry was PhishTank ID 9175576, with a suspicious URL pointing to http://allegrolokalnie.pl-oferta2719472.cfd. The phishing campaign appeared to mimic Allegro Lokalnie, a Polish e-commerce platform.

2. Examine Sender's Email Address for Spoofing

The email claimed to be from support@allegrolokalnie.pl. However, the linked domain and header analysis revealed that the actual sender was likely spoofed. The mismatch between sender address and email infrastructure is a classic sign of spoofing.

3. Check Email Headers for Discrepancies

Using Google's Messageheader Analyzer, the headers showed SPF failure and mail originating from an unauthorized IP address unrelated to allegrolokalnie.pl. These technical discrepancies confirmed sender spoofing and forged identity.

4. Identify Suspicious Links or Attachments

The email contained a single hyperlink labeled 'Reactivate Listing Now' pointing to http://allegrolokalnie.pl-oferta2719472.cfd. No attachments were included, but the embedded URL alone was deemed highly suspicious.

5. Look for Urgent or Threatening Language in the Email Body

The email used urgency tactics such as account suspension warnings and a 24-hour deadline. Phrases like 'Your listing has been temporarily suspended' and 'Failure to act will result in removal' were designed to create panic and immediate action.

6. Note Any Mismatched URLs (Hover to See Real Link)

The visible text of the link seemed to suggest legitimacy, but hovering over it revealed a clearly mismatched and malicious `.cfd` domain, which does not belong to Allegro Lokalnie.

7. Verify Presence of Spelling or Grammar Errors

The email had mostly correct grammar but used generic and robotic language, which is typical of mass phishing campaigns. The lack of personalization (e.g., no recipient name) further indicated phishing.

8. Summarize Phishing Traits Found in the Email

The email exhibited multiple phishing characteristics: spoofed sender address, failed SPF checks, unauthorized sending IP, suspicious and mismatched URL, use of urgency to manipulate the recipient, and a lack of personalization. These factors clearly indicate a phishing attempt, and users are advised to avoid interacting with such emails and report them immediately.