**Step-by-Step Phishing Email Analysis Guide**

**Overview**

This guide walks you through the complete process of analyzing a suspicious email to determine if it's a phishing attempt. Follow these steps systematically for thorough analysis.

**Prerequisites**

* Email client or .eml file access
* Internet access for tool usage
* Basic understanding of email headers
* Note-taking capability

**Step 1: Initial Email Assessment**

**1.1 First Impression Check**

1. **Don't click anything** in the email yet
2. Note your initial reaction - does something feel "off"?
3. Check if you were expecting this email
4. Verify if the sender is known to you

**1.2 Quick Visual Scan**

1. Look for obvious spelling/grammar errors
2. Check for generic greetings ("Dear Customer")
3. Note any urgent language or threats
4. Observe branding quality and consistency

**Red Flag Counter**: Start counting suspicious elements

**Step 2: Sender Analysis**

**2.1 Email Address Examination**

1. **Compare display name vs email address**
2. **Domain verification**
3. **Check Reply-To address**

**2.2 WHOIS Domain Lookup**

1. Open WHOIS lookup tool ([whois.net](http://whois.net))
2. Search for "[microsft-securityteam.com](http://microsft-securityteam.com)"
3. Check registration date, registrar, location
4. Compare with legitimate [microsoft.com](http://microsoft.com)

**Step 3: Header Analysis**

**3.1 Access Email Headers**

**For Gmail:**

1. Open email
2. Click three dots (⋮)
3. Select "Show original"
4. Copy full header

**For Outlook:**

1. Open email
2. Click File → Properties
3. Copy "Internet headers" content

**3.2 Use Header Analysis Tool**

1. Go to [MXToolbox.com/EmailHeaders.aspx](http://MXToolbox.com/EmailHeaders.aspx)
2. Paste headers in text box
3. Click "Analyze Header"

**3.3 Authentication Analysis**

Look for these results:

Received-SPF: fail (domain does not designate IP as permitted sender)  
dkim=fail (signature verification failed)  
dmarc=fail (p=QUARANTINE sp=QUARANTINE dis=NONE)

**3.4 IP Address Analysis**

1. Find originating IP in headers
2. Use IP lookup tool ([whatismyipaddress.com/ip-lookup](http://whatismyipaddress.com/ip-lookup))
3. Check IP geolocation and ISP
4. Verify if IP matches claimed sender location

**Step 4: Content Analysis**

**4.1 Subject Line Breakdown**

**Phishing Indicators:**

* creates false urgency
* pressure tactic
* Security threat claim - fear induction

**4.2 Email Body Analysis**

1. **Greeting**: "Dear Valued Customer"
2. **Content Claims**:
3. **Call to Action**:

**Step 5: Link Analysis**

**5.1 Link Inspection**

**5.2 URL Analysis Tools**

**5.3 Domain Age Check**

**Step 6: Technical Validation**

**6.1 Legitimate Channel Verification**

**6.2 Account Status Check**