It is important to know that when reading an email header every line can be forged, so only the **Received:** lines that are created by your service or computer should be completely trusted.

* The from field displays who the message is from, however, this can be easily forged and can be the least reliable.

Return-Path

* The email address for return mail. This is the same as "Reply-To:".

Received

* The received is the most important part of the email header and is usually the most reliable. They form a list of all the servers/computers through which the message traveled in order to reach you.

The received lines are best read from bottom to top. That is, the first "Received:" line is your own system or mail server. The last "Received:" line is where the mail originated.

Finding the Original Sender

The easiest way for finding the original sender is by looking for the **X-Originating-IP** header. This header is important since it tells you the IP address of the computer that had sent the email. If you cannot find the **X-Originating-IP** header, then you will have to sift through the **Received** headers to find the sender's IP address.

**A. Initial Assessment**

1. **Sender’s Email Address**:
   * Check the sender's email address closely. Look for slight misspellings or unusual domain names (e.g., @gmaill.com instead of @gmail.com).
2. **Subject Line and Content**:
   * Evaluate the subject line and the body of the email. Is it generic (e.g., "You have won a prize")? Does it contain urgent calls to action?

**B. Analyzing Email Headers**

1. **Check the 'From' Field**:
   * Identify the "From" address and verify if it matches the domain of the organization purportedly sending the email.
2. **Look at the 'Return-Path' and 'Reply-To' Fields**:
   * See if the return-path aligns with the sender's domain. Phishing emails often have mismatched return-paths.
3. **Examine the Received Lines**:
   * Review the “Received” lines to trace the email’s path. Look for suspicious or unfamiliar IP addresses.
4. **Check for DKIM, SPF, and DMARC**:
   * Look for DKIM (DomainKeys Identified Mail) signatures and SPF (Sender Policy Framework) records to verify if the email is sent from an authorized server.
   * DMARC (Domain-based Message Authentication, Reporting, and Conformance) can provide insights on how the domain owner wants unauthenticated emails to be handled.

**C. Content Analysis**

1. **Grammar and Spelling**:
   * Phishing emails often contain poor grammar and spelling mistakes. Legitimate organizations usually have well-proofread content.
2. **Links and Attachments**:
   * Hover over any links to see the actual URL. Avoid clicking on them until verified.
   * Be wary of unexpected attachments, especially executable files.
3. **Urgency and Threats**:
   * Assess the tone of the email. Phishing attempts often create a sense of urgency or threat (e.g., “Your account will be suspended!”).