Is This Email Legitimate?

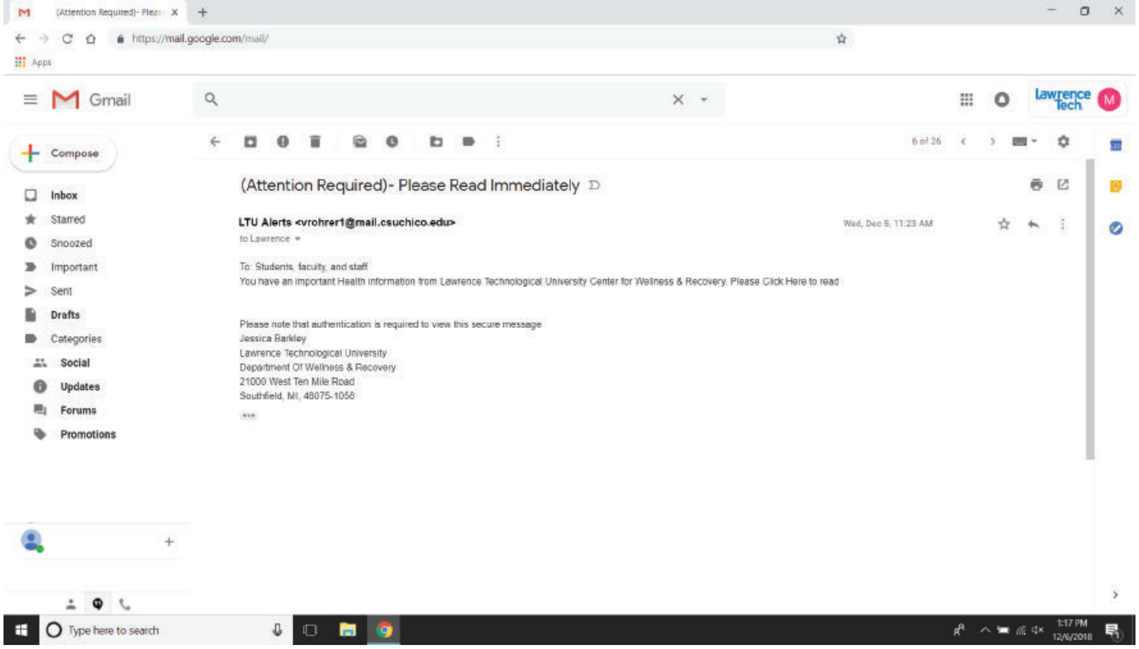
Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share personal information such as account numbers, social security numbers, login IDs, passwords, etc. These items can be then used to steal your money and/or identity.

Scammers also use phishing emails to get access to your computer or network then install programs like ransomware that can lock you out of your computer or specific files on your computer. Do not click on a link just to see what's there. Simply accessing a malicious site could result in the compromise of your computer.
If something else about it doesn't seem right, please mark the email as Spam or Phishing attempt or you may contact helpdesk@ltu.edu.

The Phish

Below is a real phish received by many LTU webmail accounts during December 2018. Let's start by clearing up one misconception; the "From" address and "Reply To" address mean nothing. They are merely text fields, and if a mail server isn't configured to check these addresses, the email can say anything the phisher or spammer wants it to say.

The phisher isn't going to give you his or her real email address. The idea is for the email to appear to be legitimately coming from the company it claims to represent, but not an actual address at the company so as to tip them off.



(Attention Required)- Please Read Immediately

LTU Alerts <vrohrer1@mail.csuchico.edu>
to Lawrence
Wed, Dec 5, 11:23 AM

To: Students, faculty, and staff
You have an important Health information from Lawrence Technological University Center for Wellness & Recovery. Please Click Here to read

Please note that authentication is required to view this secure message
Jessica Barkley
Lawrence Technological University
Department Of Wellness & Recovery
21000 West Ten Mile Road
Southfield, MI, 48075-1058

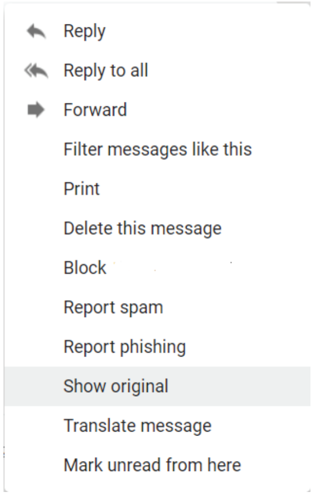
Test 1: Where Did it Really Come From?

Since the “from” and “reply to” addresses can be easily faked, it is important to view the header information. Every email contains a header that lists each mail server that it has passed through. Each entry is set apart with the word "Received" with the top-most entry being the last entry (which should be your mail server.)

IT Services requests that you send the header information to helpdesk@ltu.edu if you suspect an email may be fraudulent. Please used these instructions to obtain the headers, and send them to us for closer examination.

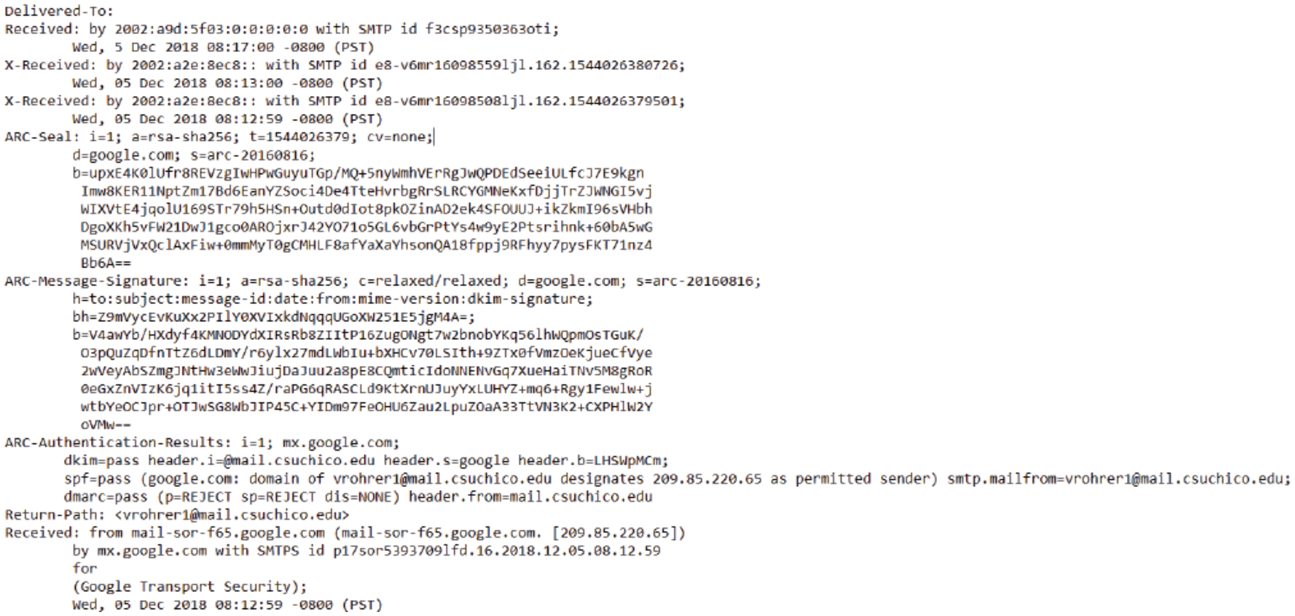
Viewing Headers in LTU Webmail:

1. Log in to Gmail
2. Open the message you'd like to view headers for.
3. Click the down arrow next to Reply, at the top of the message pane.
4. Select Show Original.
5. A new webpage opens



How to copy and send header information:

Below is a portion of the text from the webpage that opens showing the header of your email. Please copy and paste the header information into an email and forward it to helpdesk@ltu.edu.



```
Delivered-To:
Received: by 2002:a9d:5f03:0:0:0:0:0 with SMTP id f3csp9350363oti;
        Wed, 5 Dec 2018 08:17:00 -0800 (PST)
X-Received: by 2002:a2e:8ec8:: with SMTP id e8-v6mr16098559ljl.162.1544026380726;
        Wed, 05 Dec 2018 08:13:00 -0800 (PST)
X-Received: by 2002:a2e:8ec8:: with SMTP id e8-v6mr16098508ljl.162.1544026379501;
        Wed, 05 Dec 2018 08:12:59 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1544026379; cv=none;
        d=google.com; s=arc-20160816;
        b=upxE4K0lUfr8REVzgIwHPwGuyuTGp/MQ+5nyWmhVErRgJwQPDEdSeeiULfcJ7E9kgn
         Imw8KER11NptZm17Bd6EanYZSoci4De4TteHvrbgRrSLRCYGMNeKxfDjjTrZJWNGI5vj
         WIXVtE4jqolU169STr79h5HSn+Outd0dIot8pkOZinAD2ek4SFOUUJ+ikZkmI96sVHbh
         DgoXKh5vFW21DwJ1gco0AROjxrJ42YO71o5GL6vbGrPtYs4w9yE2Ptsrihnk+60bA5wG
         MSURVjVxQclAxFiw+0mmMyT0gCMHLF8afYaXaYhsonQA18fppj9RFhyy7pysFKT71nz4
         Bb6A==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=to:subject:message-id:date:from:mime-version:dkim-signature;
        bh=Z9mVycEvKuXx2PIlY0XVIxkdNqqqUGoXW251E5jgM4A=;
        b=V4awYb/HXdyf4KMNODYdXIRsRb8ZIItP16ZugONgt7w2bnobYKq56lhWQpmOsTGuK/
         O3pQuZqDfnTtZ6dLDmY/r6ylx27mdLWbIu+bXHCv70LSIth+9ZTx0fVmzOeKjueCfVye
         2wVeyAbSZmgJNtHw3eWwJiujDaJuu2a8pE8CQmticIdoNNENvGq7XueHaiTNv5M8gRoR
         0eGxZnVIzK6jq1itI5ss4Z/raPG6qRASCLd9KtXrnUJuyYxLUHYZ+mq6+Rgy1Fewlw+j
         wtbYeOCJpr+OTJwSG8WbJIP45C+YIDm97FeOHU6Zau2LpuZOaA33TtVN3K2+CXPHlW2Y
         oVMw==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@mail.csuchico.edu header.s=google header.b=LHSWpMCm;
       spf=pass (google.com: domain of vrohrer1@mail.csuchico.edu designates 209.85.220.65 as permitted sender) smtp.mailfrom=vrohrer1@mail.csuchico.edu;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=mail.csuchico.edu
Return-Path: <vrohrer1@mail.csuchico.edu>
Received: from mail-sor-f65.google.com (mail-sor-f65.google.com. [209.85.220.65])
        by mx.google.com with SMTPS id p17sor5393709lfd.16.2018.12.05.08.12.59
        for
        (Google Transport Security);
        Wed, 05 Dec 2018 08:12:59 -0800 (PST)
```

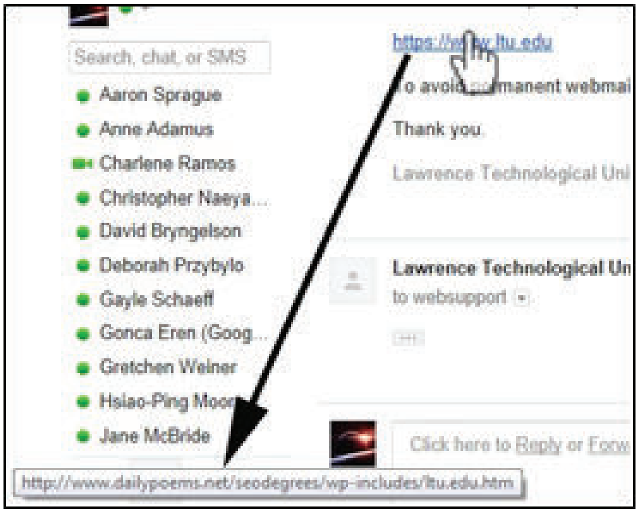
Test 2: If There’s a Link in the Email, is it Legitamate?

If the phish has a link for you to click on, as most do, you can check to see what the real link is. When you see a link in an HTML email message, it can be any text the author desires. How can you tell what the link is? There are two ways.

Hover the mouse over the link to display the real link:

Hold your mouse over the link, in a couple of moments the real link address will show. In this example it shows near the bottom left of the browser. As you can see, that link is from dailypoems.net.

Ask yourself, “Should a message from LTU have link about your email status that leads to dailypoems.net?” Absolutely not! Conclusion Spam! Therefore do not click on the link and mark the message as Spam



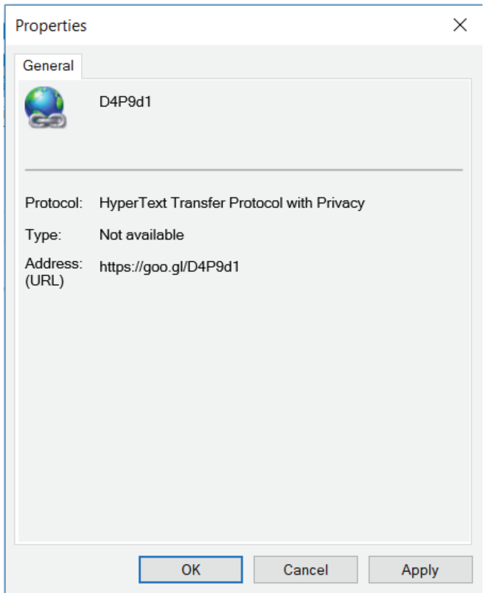
http://www.dailypoems.net/seodegrees/wp-includes/ltu.edu.htm

View the Link Properties:

Internet Explorer:

Right click while the mouse pointer is located somewhere on the message. Select "Properties" from the context menu that comes up. A dialog box opens with the link’s information. In this example, once again, you can see that the link is from dailypoems.net.

Ask yourself, “Should a message from LTU have link about your email status that leads to dailypoems.net?” Absolutely not! Conclusion Spam! Therefore do not click on the link and mark the message as Spam



D4P9d1

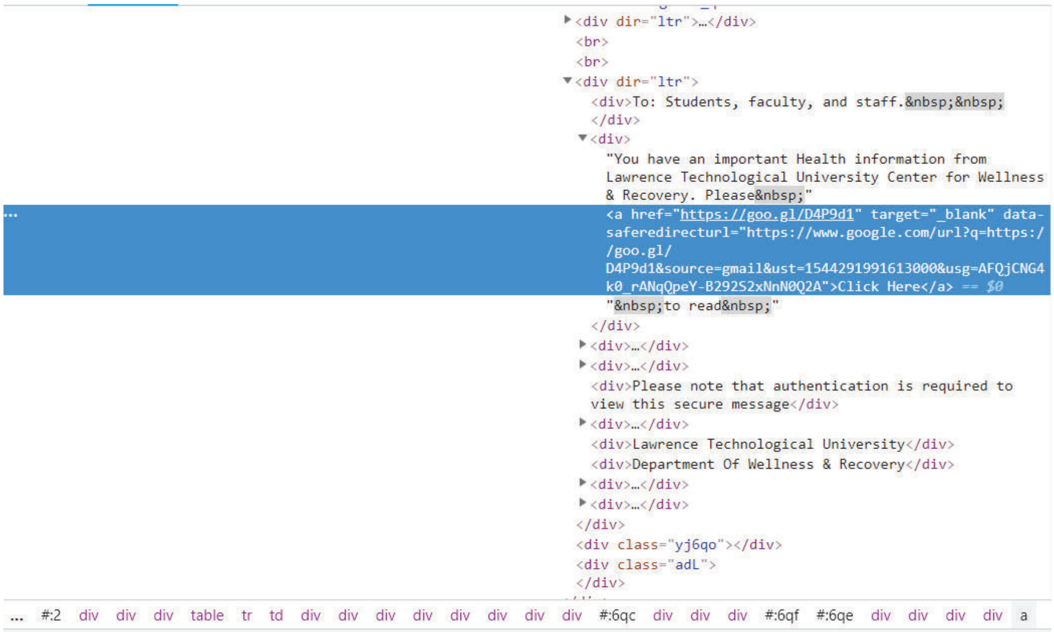
Protocol: HyperText Transfer Protocol with Privacy

Type: Not available

Address: (URL) https://goo.gl/D4P9d1

Firefox or Chrome:

Right click while the mouse pointer is located somewhere on the message. Select "Inspect Element" from the context menu that comes up. An area opens at the bottom of the window with the link's information. In this example, once again, you can see that the link is from dailypoems.net.
Ask yourself, “Should a message from LTU have link about your email status that leads to dailypoems.net?”
Absolutely not! Conclusion Spam! Therefore do not click



```
▶<div dir="ltr">…</div>
 <br>
 <br>
▼<div dir="ltr">
   <div>To: Students, faculty, and staff.&nbsp;&nbsp;
   </div>
  ▼<div>
     "You have an important Health information from
     Lawrence Technological University Center for Wellness
     & Recovery. Please&nbsp;"
     <a href="https://goo.gl/D4P9d1" target="_blank" data-
     saferedirecturl="https://www.google.com/url?q=https:/
     /goo.gl/
     D4P9d1&source=gmail&ust=1544291991613000&usg=AFQjCNG4
     k0_rANqQpeY-B292S2xNnN0Q2A">Click Here</a> == $0
     "&nbsp;to read&nbsp;"
   </div>
  ▶<div>…</div>
  ▶<div>…</div>
   <div>Please note that authentication is required to
   view this secure message</div>
  ▶<div>…</div>
   <div>Lawrence Technological University</div>
   <div>Department Of Wellness & Recovery</div>
  ▶<div>…</div>
  ▶<div>…</div>
 </div>
 <div class="yj6qo"></div>
 <div class="adL">
 </div>
```

… #:2 div div div table tr td div div div div div div div div #:6qc div div div #:6qf #:6qe div div div div a

So to recap, if the email link doesn't match what it claims to be, something is amiss and you shouldn't follow the link. Mark the message as Spam.