Is this email legitimate?

It’s amazing how easy it is to convince people that an email is legitimate. But how can you tell if an email is really coming from where it claims? Here’s an explanation of two checks you can do to quickly tell if an email is legitimate. It shouldn't take more than a few minutes to master and, if it saves you even once, it will have been well worth the time you invested.

If an email fails either of these tests or if something else about it doesn’t seem right, please mark the email as Spam or you may contact helpdesk@ltu.edu for help.

Also remember that some phishes may actually just be trying to get you to go to the fake site where crafted code may exploit a vulnerability and attempt to compromise your PC, so don’t click on a link just to see what’s there. Simply accessing a malicious site could result in the compromise of your PC.

The Phish

Below is a real phish received by many LTU webmail accounts during July 2013. 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.
Test 1: Where Did it Really Come From?
As mentioned above, the "From" and "Reply To" addresses can be easily faked. What can we check then? 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.)

What we want to do is look at the email's full message header to see where this email originated from. Since people generally don't want to look at this most of the time, your mail program hides it from you.

To view 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 read header information
Below is a portion of the text from the webpage that opens showing the header of your email. Let's look at the "Received:" entries (yellow highlight.) Some of these entries could actually be faked, but the last two entries can be trusted. The reason they can be trusted is because the last entry is your mail server, which you can trust, and the next to the last is the server that sent it to your mail server, which your mail server verified before accepting the email. (Note: You may actually see two or even three entries from your server domain if your company or Internet Service Provider (ISP) passes mail through multiple servers. You can just group these together and think of them as one.)

In the example above, look at where the ISP's mail server got the email from, the third received entry: fed1rmfepo103.cox.net. It also appears to originate from fed1rmimpo210.

Ask yourself, “Should an email from LTU come from these servers?” No way! If it's from someone large (i.e.: eBay, Amazon, your financial institution, etc.) LTU’s servers should receive it directly from that company's mail servers.

So what did we do here again? We looked at all the mail servers that the email passed from. Generally, if a company is sending you an email it should go directly from their mail system to yours. There's no reason for it to go through fed1rmimpo210, fed1rmfepo103.cox.net or any other mail system. In fact, if this happens, it's generally a good indication that the email came from a compromised PC or unsecured mail server. Mark the message as Spam.
Test 2: If There's a Link in the Email, is it Legitimate?
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.

First, 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.

Second, view the links properties
To do this in:

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.

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 on the link and mark the message as Spam.

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.