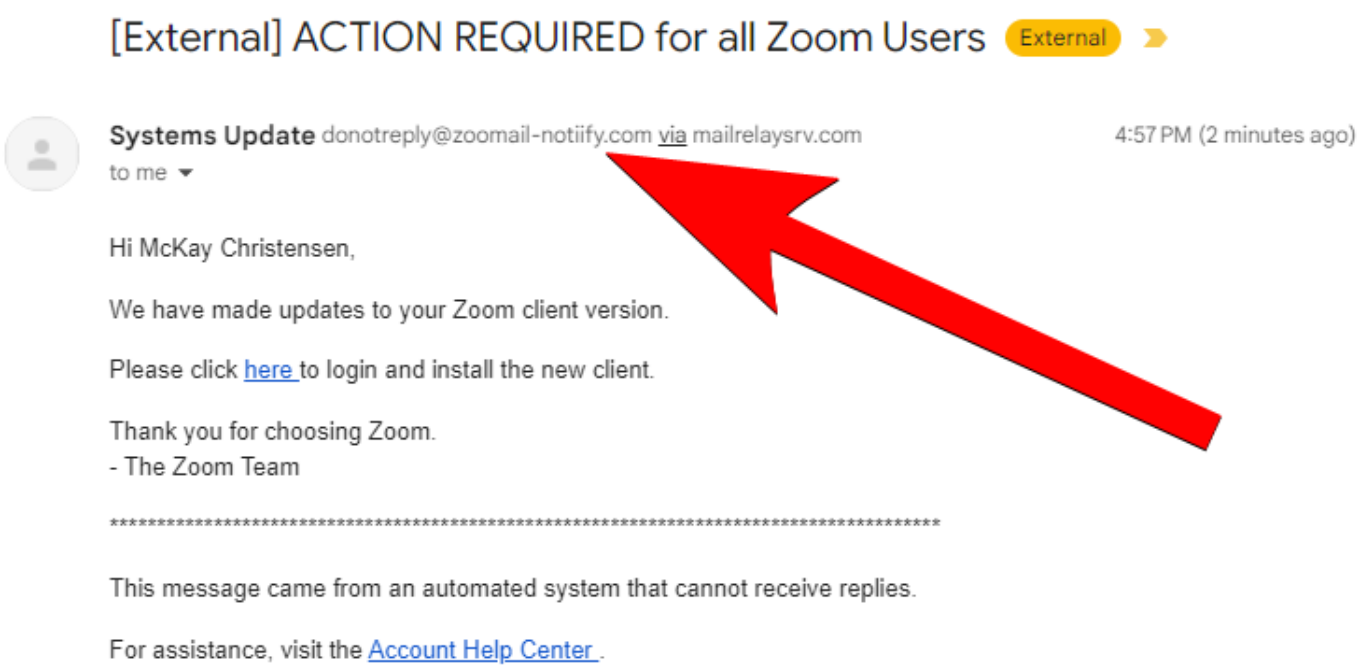
Three Things to look for in Phishing Emails - Phishing Training

Phishing emails can be hard to spot. Here are three things you should check before you click on a link in your email:

Check the sender email address.

Look at the email address. It it does not make sense, has typos, or seems suspicious then ignore the email or forward it to phishing+security@revverdocs.com



Check the body of the email. Are you expecting an email like this?

If the email seems out of place or does not seem completely logical, there is a good chance it is a phishing email.

Hi McKay Christensen,

We have made updates to your Zoom client version.

Please click here to login and install the new client.

Thank you for choosing Zoom.
- The Zoom Team

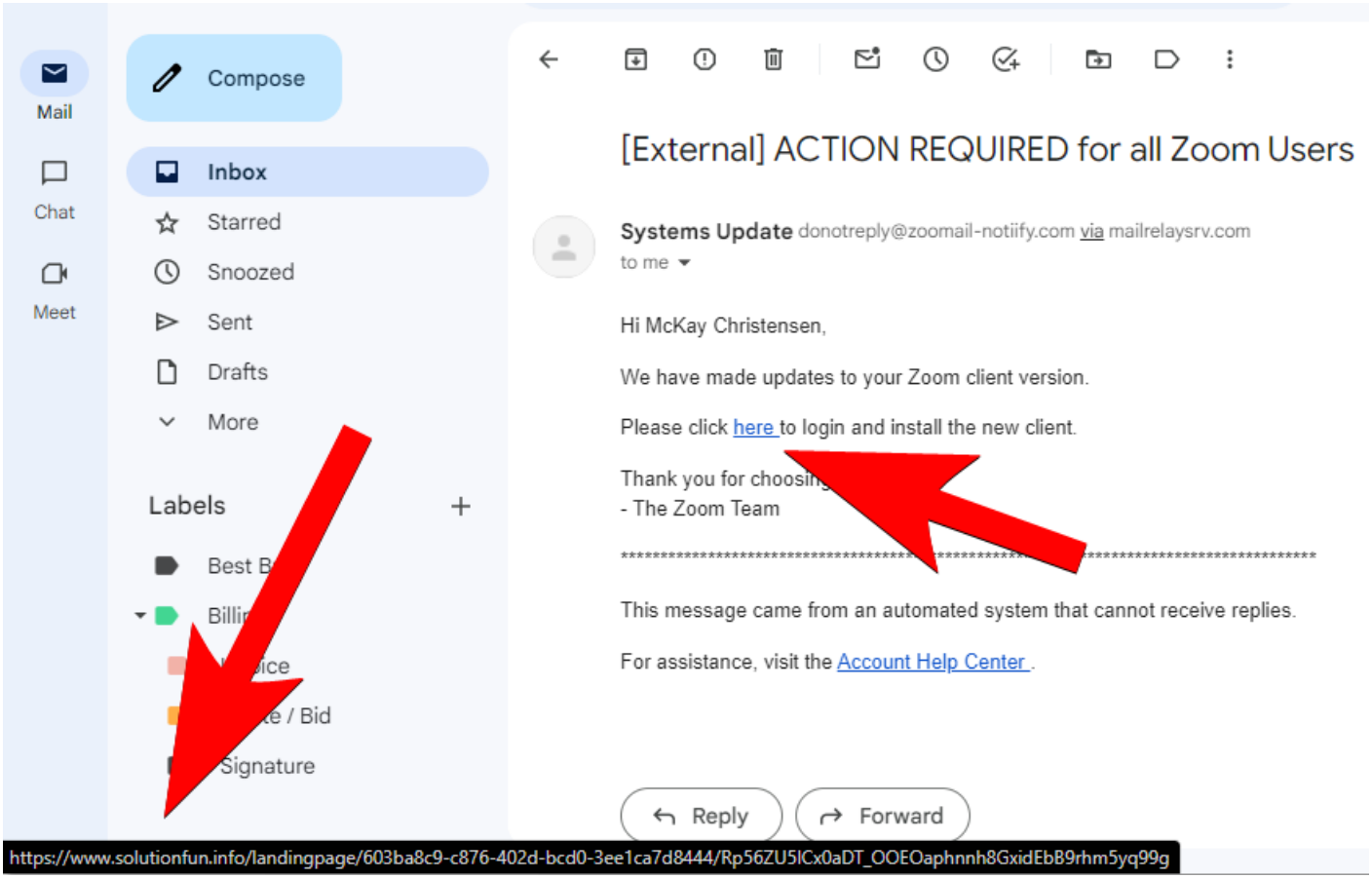
****

This message came from an automated system that cannot receive replies.

For assistance, visit the Account Help Center .

Hover over the link before clicking on it.

When you hover your mouse cursor over a link, it will say what the URL is. If the URL looks suspicious, then don't click on it. **IMPORTANT NOTE**: We use Barracuda for our email security; Barracuda takes extra security measures to protect links. If you see a link that starts with https://linkprotect... then the link is from Barracuda. If you click on it and it is a valid link, Barracuda will redirect you. If the link is malicious, Barracuda will not allow you to open the link.



Revision #2
Created 13 May 2024 22:50:27 by McKay Christensen
Updated 13 May 2024 23:10:39 by McKay Christensen