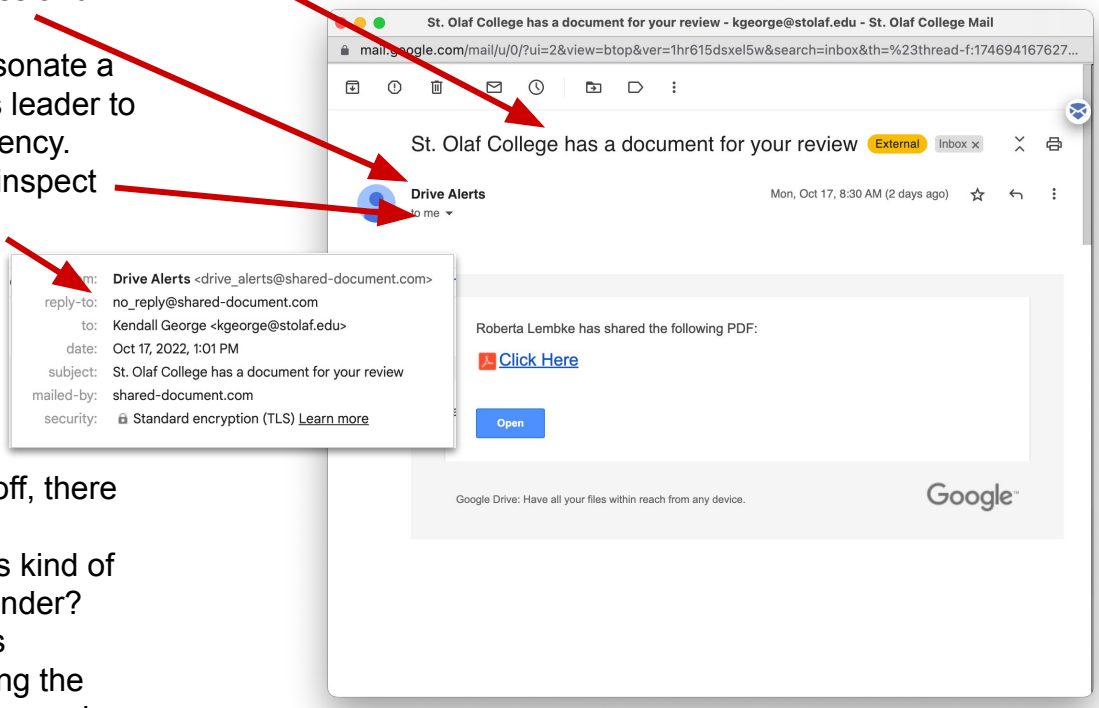
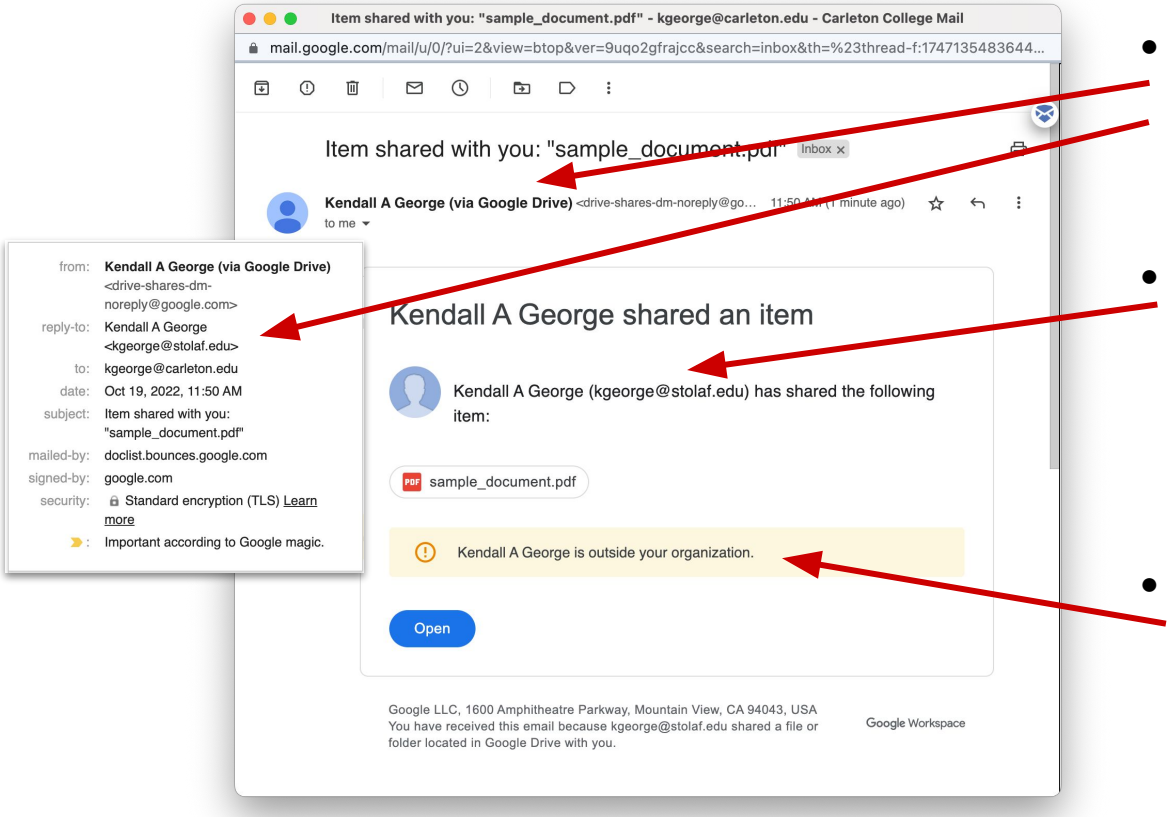
TO CATCH A PHISH

- Look for odd or unexpected language an formatting.
- Check the sender address. Is this the correct address and domain name?
- Scammers will impersonate a supervisor or campus leader to create a sense of urgency.
- Use the pull down to inspect the sender address.



- If a message seems off, there is probably a reason.
- Are you expecting this kind of message from this sender?
- Confirm a message is legitimate by contacting the sender using a known-good email address or phone number.

Here's an example of a genuine Google drive sharing notification for comparison. You can see that the phish superficially resembles a genuine sharing notification. Our simulation was specifically constructed not to be identical to a genuine sharing notification. Scammers will try to make these look as similar as possible.



- With a genuine Google Drive notification, the display name and reply-to address will be the real user's name and email address.
- Is this the correct address? Scammers will sometimes use an address that will make you think that maybe the sender used their personal account by accident.
- Google will try to help you out with warnings like this one.