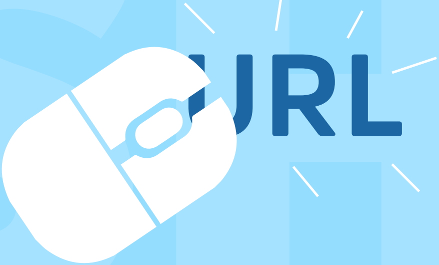
PHISHING ATTACK

emergency procedures

1. READ YOUR EMAIL

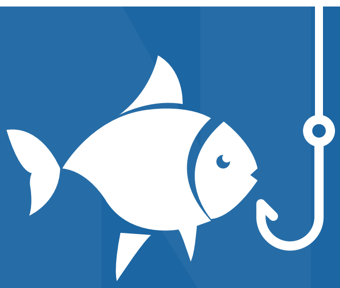
Don't skim your emails! Look at the sender's address and read the email for grammatical errors or other inconsistencies that might suggest a phishing email. You can forward suspicious emails to:
University IT- **abuse@rochester.edu** or
ISD- **abuse@urmc.rochester.edu**

2. DON'T CLICK THE LINK



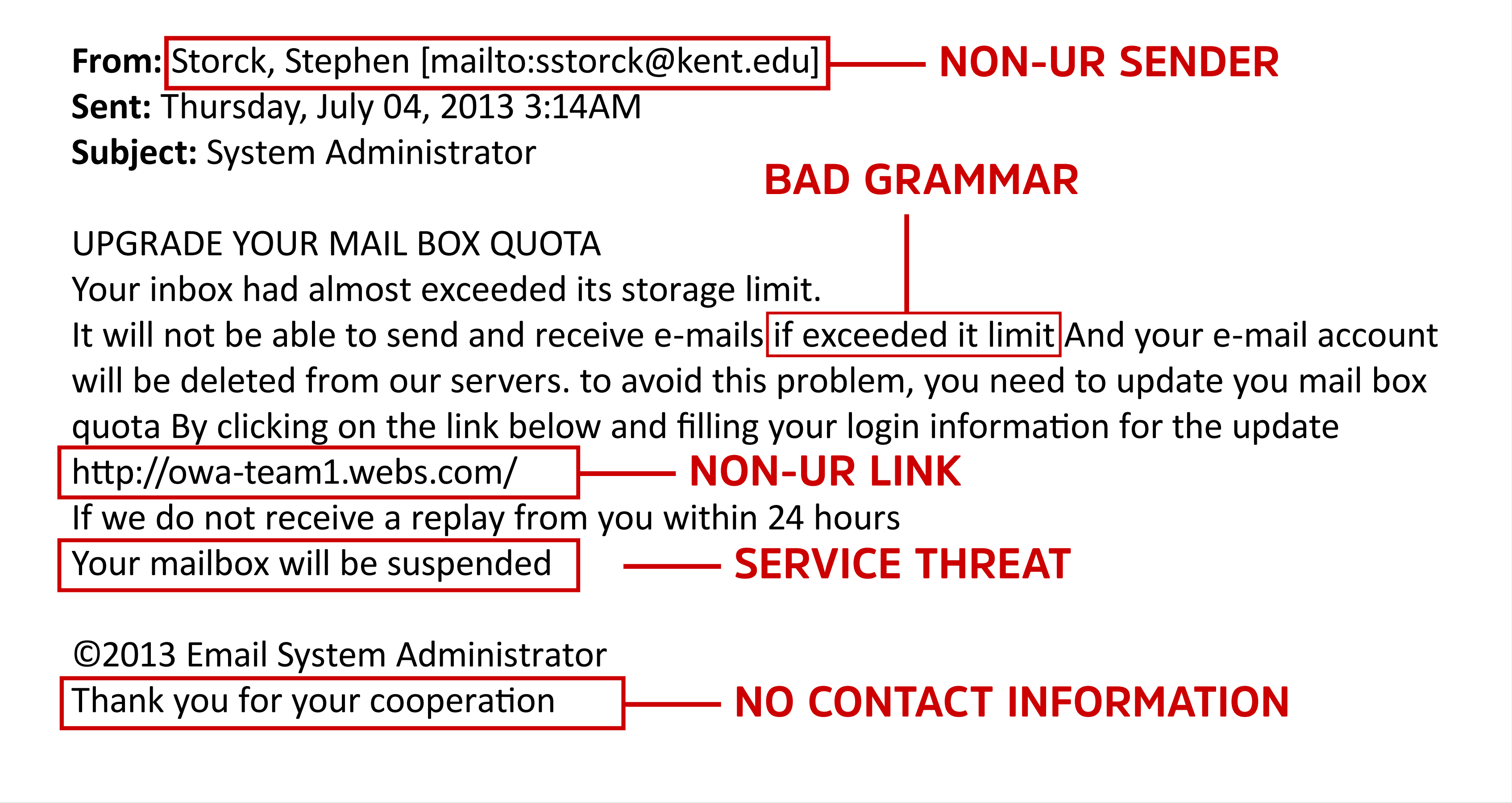
Look at the email links carefully. If you haven't heard of the website or you are unsure about the URL, look for the official website or the company's contact information. If you are still unsure, contact:
University IT Help Desk: **585.275.2000** or
ISD Help Desk: **585.275.3200**

3. DO DAMAGE CONTROL



If you click a link that is part of a phishing attack, contact your Help Desk immediately! You can find out more information on phishing and how to better protect yourself online at:
tech.rochester.edu/security/phishing-scams

Know the Signs



From: Storck, Stephen [mailto:sstorck@kent.edu] — **NON-UR SENDER**
Sent: Thursday, July 04, 2013 3:14AM
Subject: System Administrator

UPGRADE YOUR MAIL BOX QUOTA
Your inbox had almost exceeded its storage limit.
It will not be able to send and receive e-mails if exceeded it limit And your e-mail account will be deleted from our servers. to avoid this problem, you need to update you mail box quota By clicking on the link below and filling your login information for the update

BAD GRAMMAR

http://owa-team1.webs.com/ — **NON-UR LINK**
If we do not receive a replay from you within 24 hours
Your mailbox will be suspended — **SERVICE THREAT**

©2013 Email System Administrator
Thank you for your cooperation — **NO CONTACT INFORMATION**

Phishing Resources

University Email Abuse & Help Desk
University IT: abuse@rochester.edu 585.275.2000 | **Medical Center:** abuse@urmc.rochester.edu· 585.275.3200

tech.rochester.edu/security/phishing-scams