

7 WAYS TO SPOT A PHISH



[EXTERNAL] Account update required - Message (HTML)

File Message Help Acrobat Tell me what you want to do

Message: [EXTERNAL] Account update required **1**

From: Information Resources & Technology <support-rowan@gmail.com> **2**
To: doe@rowan.edu
CC: doe@rutgers.edu; doe@montclair.edu; doe@stockton.edu **4**

Actions: Reply Reply All Forward **3**

Date: Tue 9/6/2023 3:18 AM

Attachment: Rowan Secured Doc... 394 KB **5**

Content: Your account has been inactive for 180 days and has been flagged for deletion. **6**
Log in now to maintain access to your account!
[Account Login](#)
Sign in using your User ID and password **7**

STOP & THINK BEFORE YOU CLICK.

1 Subject Line
STOP & ASK YOURSELF:
Does the subject line have [EXTERNAL] or another label on it? Does the subject line create a sense of urgency?

2 From Address
STOP & ASK YOURSELF:
Do I know this sender? Does the email address match the sender's name, and is the account one they typically use?

3 Sent Date & Time
STOP & ASK YOURSELF:
Do I typically receive these types of messages on days like this and at times like this?

4 Recipients
STOP & ASK YOURSELF:
Do I know the other recipients on this email? Do I typically receive messages addressed to this group?

5 Attachments
STOP & ASK YOURSELF:
Was I expecting an attachment? Does the sender usually send information via attached documents?

6 Content
STOP & ASK YOURSELF:
Does the tone or language seem out of the ordinary? Are unusual phrases or naming conventions being used?

7 Links*
STOP & ASK YOURSELF:
Does the URL look familiar to me? Does the URL include a misspelling or a slightly modified version of a known website? **Security and marketing features may legitimately rewrite the destinations of URLs in emails, but it's still good practice to inspect hyperlinks by hovering over them before clicking. For more information, visit go.rowan.edu/safelinks.*