Don't Get Phished!
Learn how to protect yourself and stop identity theft.

Anatomy of a Phishing Email Attack:

**STEP 1**
- Student receives an email stating that their access will be terminated, and that action needs to be taken by clicking a link.

**STEP 2**
- Student clicks on the link.
- Student fills out the malicious form.

**STEP 3**
- Student receives a text message.
  Hi, this is your IT help desk. In order to prevent your account from being disabled, you will be receiving a PIN shortly. Please copy the PIN, paste it on the text message, and send it to me.

**Email Best Practices to Stay Safe:**
- Do not click on links or attachments from senders that you do not recognize.
- Do not provide usernames, passwords, and/or Duo access codes.
- Be suspicious of any email where the name and email address are different. For example, the sender's name is Sebastian Dias, but the email address is Jane.Doe@gmail.com.
- Be aware that emails coming from outside the organization will have a banner like the one below.

**Report Phishing Emails ASAP**
If you suspect a message to be a phishing attempt, you can quickly report it using Outlook's ‘Report Phish’ feature. Using this feature immediately notifies the IT Security team.

Alternatively, you can forward the suspicious email to phish@miami.edu.

**REMEMBER:**
Security is everyone's responsibility!