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 the 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.
- Student responds to the text message. (Copy paste don’t disable my access. The Duo PIN I received is 20093)
  Do not fall for this scam!

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 Jai, 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.

CAUTION: This email originated from outside the organization. DO NOT CLICK ON LINKS OR OPEN ATTACHMENTS. If you know and trust the sender,

Report Phishing Emails ASAP!
If you suspect a message to be a phishing attempt, you can quickly report it using Outlook’s “Report Message” feature.

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

REMEMBER:
Security Is Everyone’s Responsibility!