START HERE

Did you receive an email?

YES  →  Were you expecting it?

NO  →  It's time to be highly skeptical!

YES  →  Does it contain any links or attachments?

NO  →  Do you recognize the sender?

YES  →  Is there anything strange or unusual about the email?

YES  →  Anyone can insert a fancy logo and make text look pretty.

NO  →  The email is probably safe.

YES  →  Are there any spelling or grammatical errors?

NO  →  Never click on links or attachments in unexpected emails.

YES  →  Does the email look genuine?

NO  →  Don't judge. Everyone makes mistakes, but this is a red flag.

If you suspect you are being phished, forward the email (as an attachment) to PHISHING@SC.EDU

Remember, a sender's address can be easily spoofed! Always double-check the authenticity of an email before proceeding.