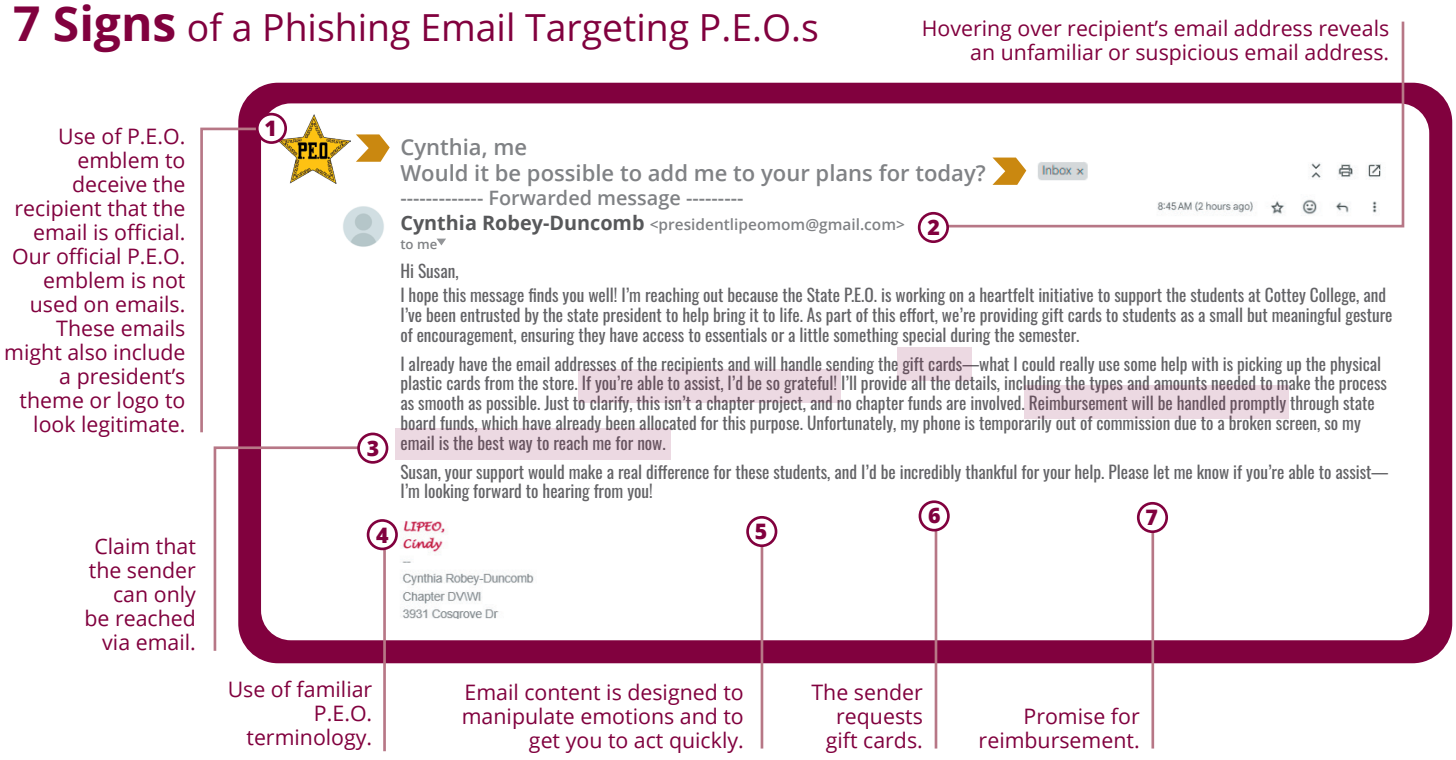
Protect Yourself from
EMAIL PHISHING SCAMS

Email phishing is a type of online scam where criminals impersonate legitimate people or organizations in order to steal sensitive information. It is one of the most common online threats, and artificial intelligence (AI) is making it easier for bad actors to generate fraudulent emails that look and feel like they are from a P.E.O. sister—they even use familiar P.E.O. terminology. These emails are malicious and are designed to get you to take action so they can steal data or financial resources or spread malicious software.

HOW TO IDENTIFY SUSPICIOUS EMAILS, LINKS AND ATTACHMENTS

- **Always check the sender's email address.** The email address may say it came from a P.E.O. chapter officer or sister, but look closer to verify it is not malicious. Make it a habit to check the sender's email address by hovering over (if on a desktop) or clicking on (if on a cellphone or other mobile device) the sender's address to reveal the true address. If the address looks unfamiliar or is different than the reply address, verify it against your trusted chapter yearbook or the P.E.O. International member database before taking action. For example, you may see presidentlipeo@gmail.com as the address, but when you hover over it, the sender's email address is actually a series of unusual characters or numbers.
- **The email is designed to manipulate your emotions and help fraudsters further their own criminal intent.** Recent email scams directed at P.E.O.s have asked members to purchase gift cards for students at Cottey College or to help with needs for conventions or other initiatives by sending electronic funds. There is almost always a promise of reimbursement once gift cards or funds are received.

7 Signs of a Phishing Email Targeting P.E.O.s



WHAT TO DO IF YOU RECEIVE A SUSPICIOUS EMAIL

- **Pause.** Don't click on links or attachments without first looking at where it is from.
- **Validate.** Confirm the information is coming from a real person. Is it a P.E.O. email? Is it an email address known to you?
- **Act.** Place a phone call to the P.E.O. member who is named as the sender in the email. Be sure to use a known number from your yearbook or call the P.E.O. Executive Office. Only open links and respond when you are confident the information is legitimate. If you believe it is a phishing attempt, report the suspicious email immediately to your state, provincial or district (s/p/d) president.