

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 presidentlpeo@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

Hovering over recipient's email address reveals an unfamiliar or suspicious email address.

1. Use of P.E.O. emblem to deceive the recipient that the email is official. Our official P.E.O. emblem is not used on emails. These emails might also include a president's theme or logo to look legitimate.

2. Hovering over recipient's email address reveals an unfamiliar or suspicious email address.

3. Claim that the sender can only be reached via email.

4. Use of familiar P.E.O. terminology.

5. Email content is designed to manipulate emotions and to get you to act quickly.

6. The sender requests gift cards.

7. Promise for reimbursement.

Email Content:

Cynthia, me
Would it be possible to add me to your plans for today?

----- Forwarded message -----

Cynthia Robey-Duncomb <presidentlpeomom@gmail.com> to me

Hi Susan,

I hope this message finds you well! I'm reaching out because the State P.E.O. is working on a heartfelt initiative to support the students at Cottey College, and I've been entrusted by the state president to help bring it to life. As part of this effort, we're providing gift cards to students as a small but meaningful gesture of encouragement, ensuring they have access to essentials or a little something special during the semester.

I already have the email addresses of the recipients and will handle sending the gift cards—what I could really use some help with is picking up the physical plastic cards from the store. If you're able to assist, I'd be so grateful! I'll provide all the details, including the types and amounts needed to make the process as smooth as possible. Just to clarify, this isn't a chapter project, and no chapter funds are involved. Reimbursement will be handled promptly through state board funds, which have already been allocated for this purpose. Unfortunately, my phone is temporarily out of commission due to a broken screen, so my email is the best way to reach me for now.

Susan, your support would make a real difference for these students, and I'd be incredibly thankful for your help. Please let me know if you're able to assist—I'm looking forward to hearing from you!

Signature:

LIPEO, Cindy
Cynthia Robey-Duncomb
Chapter DVIII
3931 Cosgrove Dr



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.