

# PHISHING EMAIL RED FLAGS

## ✓ CHECK THE FROM EMAIL ADDRESS

- Is the sender someone you recognize?
- Is the sender from outside your organization?
- Is the sender someone your job would require you to contact?
- Is the email written as you would expect it to be?
- Is the sender's email address from an unusual domain?
- Is the sender someone you know, or can someone you trust vouch for them?
- Is the sender someone you'd expect an email from?

## ✓ CHECK THE TO EMAIL ADDRESS

- Is the email to you personally, or are you just one recipient in a large list?
- Is the email being sent to people you know personally or at least recognize?
- Is the mix of people the email was sent to random, or all part of an odd pattern?

## ✓ CHECK THE SUBJECT LINE

- Is the subject line representative of what is in the message itself, or is it unrelated to the actual message?
- Is the subject line suggesting that the email is a reply, but you never sent a message or requested a response?

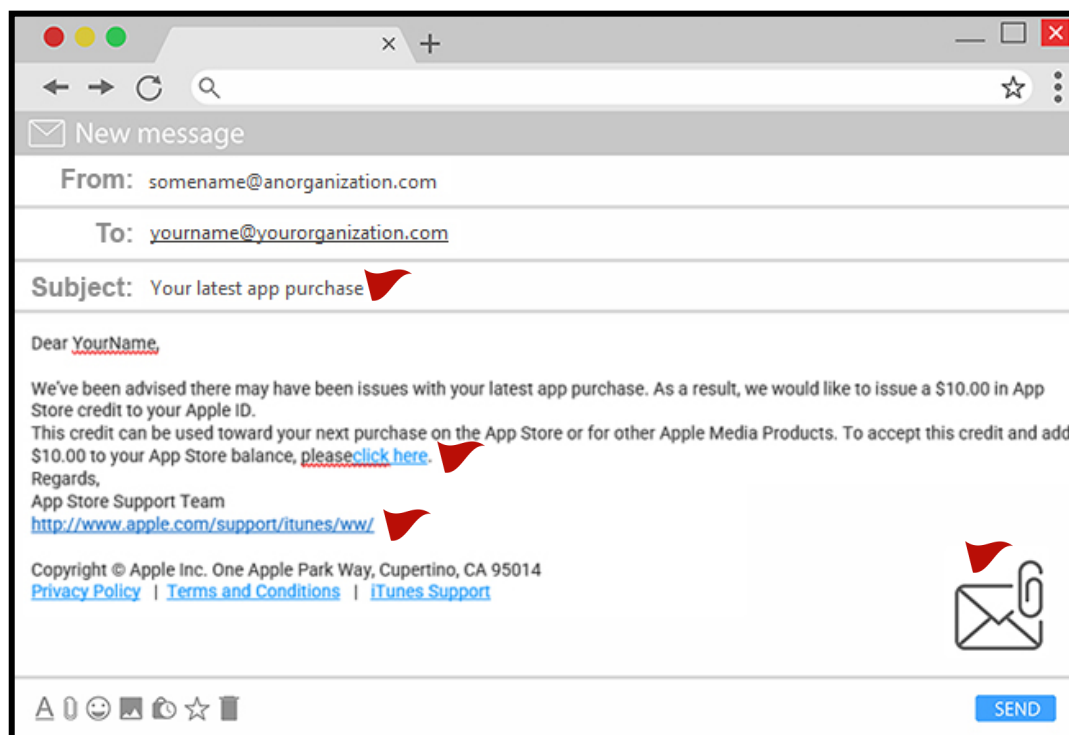
## ✓ WHAT DOES THE CONTENT SAY?

- Is there any pressure to open an attachment or click a link, particularly to avoid a negative consequence.
- Is there a promise of excessive value, considering what is being asked of you?
- Is there anything unprofessional about the content, particularly grammatical or spelling errors?
- Is there any logic to the attachment that is allegedly included?
- Is there any threat outlined in the content, like the claim that the sender has compromising information about you or others?

## ✓ WHAT ABOUT LINKS OR ATTACHMENTS

- Is the website that a link allegedly goes to a match to what appears when you hover your mouse over it?
- Is the email entirely composed of a hyperlink, with no context or explanation?
- Is the hyperlink a misspelled version of a well-known website?
- Is there an unexpected attachment included, particularly one that is unrelated to the content of the message or not usually included in a message from the purported sender?
- Is the attachment a potentially dangerous file type, like an .exe, zip, img, iso or an office file type?

### EXAMPLE PHISHING EMAIL



Spread phishing awareness! These are all signs that a message is a phishing attempt, so if you see them:

**Don't Click!**  **Don't Respond!**  **Report to Support!**