COLLEGE of the DESERT

Identifying Phishing Emails

- A yes to any of these questions should make you suspicious of the emails origin.
- Never click on or follow links, nor reply directly to email link.
- Always authenticate by entering user address from a verified source.

FROM:

1. Is the sender's email address someone I do not recognize or normally communicate with?
2. Is the email from someone not part of my organization and unrelated to my job duties?
3. Is the email from someone part of my organization (Staff, Faculty, Administration, student) but is unusual or not in character?
4. Is the email address from a suspicious domain or misspelled look-alike domain (CollegeoftheDessert.edu)?
5. Is the sender someone you do not know personally?
6. Is the email from someone you have not held a business relationship or had past communication with?
7. Was the email unexpected or unusual?
8. Does the email contain an embedded link or attachment from someone you have not communicated with recently?

TO:

1. Were you cc'd on an email that was sent to one or more people that you do not personally know?
2. Was the email sent to an unusual collection of people? (For example: Was it sent to a random group of colleagues with the same first letter of their last name, or a list of totally random addresses)

HYPERLINKS:

1. When you hover over a hyperlink in the email, does it display a link-to address for a different website?
2. Does the content of the email consist only of long hyperlinks with no real explanation?
3. Does the email contain a hyperlink that is a misspelling of a known website? (CollegeoftheDessert.edu or ArnericanAirlines.com)

DATE:

1. Did you receive the email or was it sent at an unusual time for that sender to communicate (3 am or Sunday)?

SUBJECT:

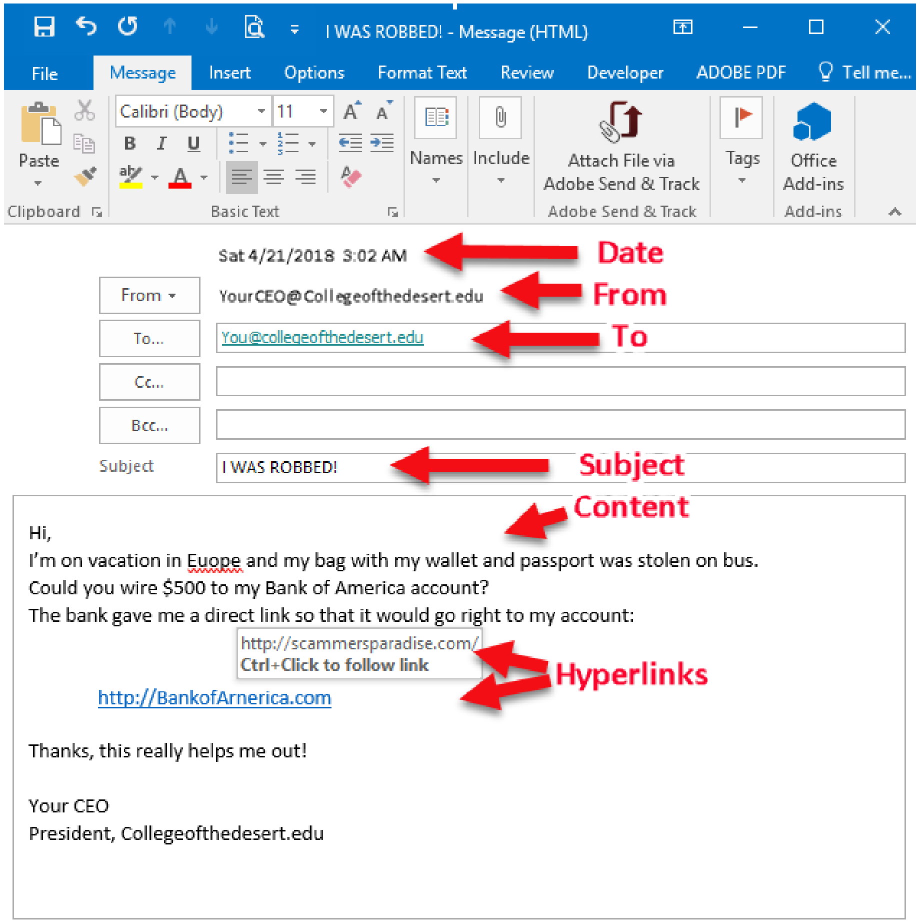
1. Is the subject line irrelevant or out of character with the content?
2. Is the email a reply to something you never sent or requested?

ATTACHMENTS:

1. Does the email include an attachment you did not expect or that seems unrelated to the email message?
2. Does the email contain an attachment or attachment type not usually included by this sender?
3. Does the email include a possibly dangerous file type as an attachment? (Note: the only completely safe attachment is a text ".txt" file.)

CONTENT:

1. Does the sender want me to click on a link or open an attachment in order to gain something of value or avoid a negative consequence?
2. Does the email contain spelling or grammatical errors, or does it seem to be out of the ordinary?
3. Does the email ask me to click a link or attachment that seems illogical or odd?
4. Does the email ask me to look at compromising or embarrassing pictures of you or an acquaintance?
5. Does the request to click on a link or open an attachment not fell "right"?



Sat 4/21/2018 3:02 AM

From YourCEO@Collegeofthedesert.edu

To... You@collegeofthedesert.edu

Cc...

Bcc...

Subject I WAS ROBBED!

Hi,
I'm on vacation in Euope and my bag with my wallet and passport was stolen on bus.
Could you wire $500 to my Bank of America account?
The bank gave me a direct link so that it would go right to my account:

http://scammersparadise.com/
Ctrl+Click to follow link

http://BankofArnerica.com

Thanks, this really helps me out!

Your CEO
President, Collegeofthedesert.edu