Identify Phishing Emails

Phishing emails appear to be from companies or people that you know, but are actually from scammers. These threats attempt to obtain the university's or your private information, passwords or account numbers to allow scammers to commit fraud. Below are common red flags found in phishing emails.

RANDOM CAPITALIZATION
Official Elon emails do not use all caps for the sender's name.

From: JANE Doe <janedoe123.elon.edu@gmail.com>
To: John Doe <johndoe456.elon.edu>
Sent: Friday, March 1, 2019 10:16 AM
Subject: Hello are you available?

SENDER'S ADDRESS
Official Elon emails are sent from @elon.edu; use caution with external providers.

Hello John,

Good day, I'm stuck in a seminar right now and i need your assistance which i will appreciate your help a lot. Kindly drop your cellphone number to send text message.

Thanks

REQUESTS
Sender often asks for reply to gain access.

BAD GRAMMAR
Misspelled words and language errors are common.

URGENT SUBJECT LINE
Subjects often create a sense of urgency.

From: ELON University help desk <helpdesk.elon.edu@gmail.com>
To: John Doe <johndoe456.elon.edu>
Sent: Monday, March 11, 2019 2:10 PM
Subject: Urgent Warning!

There have been several login attempts on your Elon account. There is now security problems with your account. We added a verification process to confirm your identity and your account security.

Click here to confirm your account

ODD PHRASING
Message body typically includes incorrect sentence structure and details that invoke fear, greed, or other strong emotions.

SUSPICIOUS LINKS
Outlook: Elon utilizes Safe Links, which generally protects Outlook users from potentially malicious websites. The only exceptions are elon.edu links, which show the full URL path.

Gmail: Hovering over a link to see its true destination may be helpful. If the link is strange or unfamiliar, it may be fraudulent.