Always check the sender's email address. If the person or domain that the email is coming from is unfamiliar, this could indicate a phishing attempt.

From: Donna Aldridge <donna.aldridge@wheaton.edu>
Sent: Monday, July 3, 2017 1:10 PM
To:
Subject: CAMPUS HEALTH ISSUE REVIEW

Hello

Spelling and other grammatical errors could indicate a possible phishing attempt.

Safety Department reported a health scare on Campus. Read released Memo as below for update;

Small, unclear images could be used to entice an individual to click on the image to see a larger view. In this case, this image was hyperlinked to a malicious website.

Hovering your pointer over a hyperlink will show you what website the link is pointing to. Sometimes hyperlinks that state a "fau.edu" web address may be taking you to a malicious website instead.

Thanks

Donna Aldridge

Health and Safety Unit.

If the sender is claiming to be an FAU employee, look that person up in Workday or the FAU people directory. Both resources will provide someone's real FAU email address and then you can contact that individual asking them to confirm any email communication that appeared to have come from him/her.

© 2017 Florida Atlantic University

777 Glades Road, Bldg SU80 Rm 233

Boca Raton, FL 33431

Rights reserved

Generic information like this is sometimes provided to make an email appear more legitimate. Fake building/room numbers and a room number that doesn't belong to the sender may indicate a possible phishing attempt.