What is phishing and how does the email security appliance help?

Tell Me

This tool is currently being tested by early adopters. This functionality will be rolled out to the campus community Fall 2020.

1. Cybercriminals can use email to impersonate employees or send spoofed links to your University account to steal your money or personal information. These crimes often target higher education employees and can have devastating effects.
2. To reduce the likelihood that users will be baited by malicious email scams, an email security appliance warns recipients when an email originates from outside the @uncc domain (sender addresses that do not end in @uncc).
3. The following tags EXTERNAL and UNTRUSTED ATTACHMENT within subject lines and in-emails help readers quickly recognize emails from outside the @uncc domain and to remind readers to practice caution before clicking or opening links:
   a. Emails from a non-UNCC email address will display a subject beginning with [EXTERNAL] and an in-email alert:

```
From: Office of State Human Resources
Subject: [EXTERNAL] NCFlex Member Alert - FSA Changes

[Caution: Email from External Sender. Do not click or open links or attachments unless you know this sender.]
```

b. Emails (from a non-UNCC email address) that contain an unscannable attachment will display a subject beginning with [UNTRUSTED ATTACHMENT] and an in-email alert:

```
From: Kathy
Subject: [UNTRUSTED ATTACHMENT] Red Hat invoicing

[Caution: Attachment could not be scanned by our email security antivirus. Do not open links or attachments unless you trust this sender.]

Hi,
We haven't had this invoice paid yet.
```

Related FAQs

- How do I report SPAM or phishing emails?
- How do I prevent an email from being marked as [EXTERNAL]?
- What do I do if I think email is missing and/or it is not being delivered to me?
- Why are some UNC Charlotte messages going into the SPAM label?
- What do I do when I receive an email that says the attachment couldn't be scanned?