

# HOW TO RECOGNIZE AND REPORT PHISHING ATTACKS

**Phishing attacks** are used by criminals to install malware or con you out of money or sensitive information. While the ways in which cybercriminals target victims is **ever-evolving**, the tips below can help you **recognize phishing emails**.

**External Domain (i.e. gmail)**  
Don't be fooled by what's in front of @.

**Urge to Act Promptly**

**Remember to use common sense.**

**Excuse for Email vs. Call**

**Request for Purchase**

**Spooled Links/Websites**

**Always be vigilant and suspicious.**

**Grammatical Errors**

**Imitating Authority Figure**

From: John.Smith.charlotte.edu@gmail.com  
To: Jane.Doe@charlotte.edu  
Cc:  
Subject: Available???

Are you available? I'm in a conference right now and don't have any idea when it will be over.

To add to our upcoming event giveaway, I need you to purchase five gift cards and send me a photo of the codes after you scratch off the film <http://69.195.82.136/51.html>

See more about the event at <https://ourevent.uncc.edu>.

I would appreciate if you could complete this task today.

Thanks,  
John Smith  
Manager, OneIT

**If you suspect you have received a phishing email or spam:**

1. Do not respond.
2. Forward email to ReportSpam-group@charlotte.edu.
3. Delete immediately.

Malicious attacks can also occur via phone calls and text messages.

For more information on cyber safety and phishing attacks,

visit <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>.

