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

Spoofed Links/Websites

Always be vigilant and suspicious.

Grammatical Errors

Imitating Authority Figure

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.