

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**.

The diagram illustrates a phishing email with several red flags highlighted by callouts:

- External Domain (i.e. gmail)**: Don't be fooled by what's in front of @. (Callout points to the email address: John.Smith.uncc.edu@gmail.com)
- Urge to Act Promptly**: (Callout points to the subject line: Available???)
- Excuse for Email vs. Call**: (Callout points to the text: Are you available? I'm in a conference right now and don't have any idea when it will be over.)
- Request for Purchase**: (Callout points to the text: 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)
- Spooled Links/Websites**: (Callout points to the link: https://ourevent.uncc.edu. and a suspicious link: http://69.195.82.136/51.html)
- Grammatical Errors**: (Callout points to the text: I would appreciate if you could complete this tsak today.)
- Imitating Authority Figure**: (Callout points to the signature: Thanks, John Smith, Manager, OneIT)

Remember to use common sense.

Always be vigilant and suspicious.

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

1. Do not respond.
2. Forward email to ReportSpam-group@uncc.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>.

