Phishing 101

WHAT IS PHISHING?

The activity of defrauding an online account holder of financial or sensitive information by posing as a legitimate authority. At UNC, this typically means posing as the HelpDesk, Finance or HR department, or other official party to gain Onyen, password or other valuable information.

TOP TIP

UNC will never ask you to confirm your Onyen or password via email. If an email asks you do so, forward it to phish@unc.edu.

UNC
INFORMATION
TECHNOLOGY SERVICES

HOW TO SPOT A PHISHING EMAIL

Email Tone

Phishing emails tend to create a sense of urgency or fear. Click here or lose access! You won't get paid this week if you don't confirm credentials! Be suspicious of any email that uses such a tone.

Sender Address

Does the "from" name make sense with or match the actual email address? For example, From: John Doe, UNC Help Support with an email address of d2381k@nl.eg.com? If it looks odd, it's probably because it's phish.

Bad Grammar and Spelling

Closely read any email requesting urgent action. Bad grammar, spelling mistakes, random capitalization, odd word spacing -- these are all signs of a phishing email.

Link URLS

You don't need to be a tech expert to spot a bad URL. Official messages should have links that include unc.edu or other familiar pathways. Random letters or foreign country abbreviations are a warning flag! Tip: Hover over a hyperlinked phrase.