Anatomy of a Phishing Email

Phishing is a method through which bad actors attempt to gather personal information – including usernames, passwords, credit card numbers and more – through malicious email links or attachments. More often than not, phishing messages follow a standard framework that can be easy to spot if you now what you're looking for. Here's a look at the anatomy of a typical phishing email...

Random capitalization

Official emails will never use all caps for the University's name.

From: THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL <johndoe@ad.unc.edu>
Date: May 12, 2016 at 9:27:35 AM EDT
Subject: **Warning! Your Urgent Attention Is Needed**

Urgent subject line

Phishing emails try to create a sense of fear and urgency. Official emails typically do not.

Thank your for being part of THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL webmail Services. We're excited to contact your email!

Bad grammar and odd phrasing

This entire paragraph illustrates language mistakes common when emails come from outside the United States.

What to do now!

We are currently updating our UNIVERSITY of NORTH CAROLINA at CHAPEL HILL services, due to this upgrade we sincerely call your attention
to follow below link and reconfirm your UNIVERSITY of NORTH CAROLINA at CHAPEL HILL email account details.

Out of context sentences

This phrase does not make sense in the context of the email, particularly one with a sense of urgency.

Click here to reconfirm your email account

Thank You

Bad links

Hover your mouse over a link to see the target destination. If you see a long, strange link that doesn't look familiar, it's probably phish.

UNC INFORMATION TECHNOLOGY SERVICES