Recognize Phishing Email

Phishing email messages, websites, and phone calls are designed to steal money. Cyber-criminals can do this by installing malicious software on your computer or stealing personal information off of your computer. 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.

Urgent subject line

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

From: THE UNIVERSITY of NORTH DAKOTA <john.doe@und.edu>
Date: January 6, 2018 at 9:27:35 AM EDT
Subject: Warning! Your Urgent Attention Is Needed

Bad grammar, spelling, and odd phrasing

This entire paragraph illustrates language mistakes commonly found in phishing emails.

Thank your for being part of THE UNIVERSITY of NORTH DAKOTA at GRAND FORKS webmail Services. We're excited to contact your email!

What to do now!

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

Click here to reconfirm your email account

Thank You

Out of context sentences

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

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.

UNIVERSITY OF NORTH DAKOTA
UNIVERSITY INFORMATION TECHNOLOGY