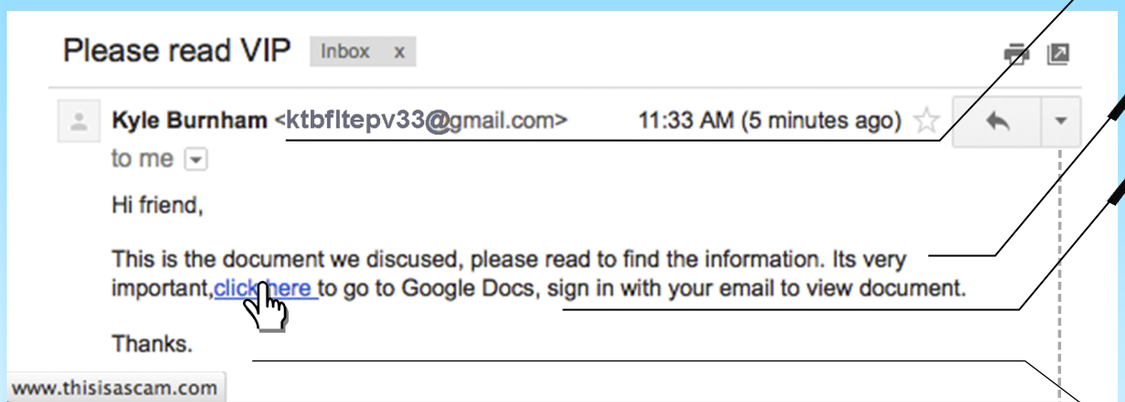
# PHISHING: How to Avoid Getting Hooked

## What is Phishing?

**Phishing is a fraudulent attempt to get information via email.** Like fishing, phishing relies on using tempting bait to reel you in. Phishers use email to manipulate you to get what they want. Often phishing messages attempt to make you reveal personal information, such as account numbers or passwords. Sometimes they use infected attachments or other scams. For more information, contact the Help Desk.


## How to Recognize Phishing:

These are some common patterns you can use to recognize phishing:




**A) Check the email address.** Even if it appears to be from someone you know, their account may have been hacked or their name stolen.

**B) Poor grammar and spelling** mistakes are often a sign of phishing.

**C) Examine the content.** Is it unexpected? Does it require immediate action, account information or for you to log in? It's best to call the organization or individual who purportedly sent the message to see if action really is necessary--but don't rely on contact information in the email!

**D) Don't click links or open attachments that you didn't expect!** Verify the link destination by hovering your cursor over the link. If you're at all suspicious, don't click!

## What to Do:

**If you've been phished, call the Help Desk immediately at 315-859-4181.** If you suspect a message is phishing, please report the message to your email provider. For Gmail and HillConnect, click the **down arrow** (next to the reply button) for reporting options.

Hamilton

Burke Library - 1st Floor helpdesk@hamilton.edu 315-859-4181 Help Desk hours: Summer M-F 8am - 4pm