COVID-19 Phishing Awareness Alert

EXECUTIVE SUMMARY

Yale has seen an initial influx of phishing attacks attempting to take advantage of COVID-19 uncertainty. Our peer institutions have reported a marked increase in phony messages using COVID-19 themes to grab attention. It's a fact of internet life that scammers will attempt to take advantage of any situation which commands attention.

KEY TIPS AND TRICKS

Stay Alert

Hover to discover

Click with Caution

KEY ACTIONS YOU CAN TAKE

- **Stay Alert**
  - Be suspicious of unexpected email messages, especially messages that seem urgent or try to instill fear.
- **Hover to Discover**
  - Hover over the email address to verify the sender is who they say they are. Often, the scammer appears to be a known entity or an @yale.edu email address, but when you hover over the sender's name or email address you may notice the sender is not really an @yale.edu email address.
- **Click with Caution**
  - If you receive any unexpected or suspicious email messages that contain links or attachments, do not click on the links or open the attachments. Instead, report the email (see below).

BACKGROUND

What is a phishing attack?
A phishing attack is an email message that attempts to steal confidential user information such as usernames, passwords, and credit card information. This message is often unexpected, urgent or comes from an unknown sender.

What can I do to prevent falling for a phishing attack?
- Be on heightened alert when it comes to unexpected emails.
- Recognize that scammers, hackers, and criminals will attempt to use the COVID-19 outbreak to their benefit.
- Review the tips & tricks in this document to spot a phishing message.

What should I do if a receive a phishing message?
If you receive a message via email that seems suspicious, call the ITS Help Desk at 203-432-9000 or report it using the instructions on How to Report Spam or Phishing Emails.

Yale Information Security