Dear colleagues,

Too many Terriers continue to fall for phish. Please remember these **4 warning signs**:

1. **Context**: Ask yourself if this is how the sender normally communicates with you. For example, if a delivery company normally communicates with you via personal email, an email to your BU email may be a phish.

2. **Links/Attachments**: Verify all links before clicking on them, by hovering your mouse over the link to see the true address of the link. Since hovering (aka mousing) over links on mobile devices is difficult, there's a chance you will click on the link instead of hover over it. Consider checking links on a desktop or laptop computer. Likewise, don't click on attachments that are not expected because they can contain malware.

3. **Urgency**: Pause and re-read any email that requests you "take action immediately" or respond within a timeframe. And remember, BU will never ask you for your passwords or sensitive information, like SSNs, by regular email.

4. **Sender**: Look out for similar but fraudulent email addresses that try to look like the supposed sender, such as corbettd@bx.edu or corbettdbuedu@gmail.com.

How can I get better at spotting phish?

- Check out the latest phish we've caught here to get better at spotting them: https://www.bu.edu/tech/support/information-security/bus-phish-bowl/
- Faculty and staff should go here to take our succinct training on Phishing: https://bostonuniversity.sumtotal.host/core/pillarRedirect?relyingParty=LM&url=app%2Fmanagement%2FLMS_ActDetails.aspx%3FActivityId%3D38957%26UserMode%3D0
- Students can review the PPT version of the training on our How to Fight Phishing Page: https://www.bu.edu/tech/support/information-security/security-for-everyone/phishing/

What should I do when I spot a phish?

- Forward phishy emails to abuse@bu.edu to protect you and the rest of the BU Community from further attack