PREVENT YOUR EMAILS FROM LOOKING PHISHY

FOLLOW THESE FIVE QUICK TIPS

The Office of Information Security offers these best practices for drafting emails:

Send a "heads-up" communication. If possible, notify your target audience in advance of sending the actual email through a TU Today post or a direct "heads-up" email. Reference the TU Today post, if applicable.

Personalize the greeting. If including a greeting in the email, try to customize it. Using "Dear John Smith" as opposed to "Dear Employee" makes it feel like less of a potential scam.

Polish the visual content. Keep font sizes, styles, and colors the same when sending mass emails. It's also helpful to avoid including attachments, although that's not always possible.

Link safely. Link to TU-related resources as opposed to outside sources. If linking to non-TU websites, type out the entire link and use descriptive text so the reader knows the destination. Keep links to a minimum.

Provide a point of contact. Include a TU-branded email signature, and list a TU Department or faculty/staff member as a point of contact in case the recipient has questions or wants to confirm the email is legit.

For more resources on phishing, and to see examples, visit towson.edu/phishing.