Don’t take the bait!

Learn to recognize and avoid common phishing attacks

1. **Sender’s email address**: Official UTK communications will always be sent from a utk.edu address. However, be cautious; just because it does come from a utk.edu address does not guarantee that it is legit either.

2. **Don’t be duped by aesthetics**: Phishing emails often contain convincing logos, links to actual company websites, legitimate phone numbers, and e-mail signatures of actual employees.

3. **Impersonal or awkward greeting**: Most phishing emails DO NOT refer to the recipient by name.

4. **Check for errors**: While scam emails are becoming more sophisticated, many scam emails contain misspellings and grammatical errors. Read your emails carefully and report anything that seems suspicious.

5. **Urgency/Fear**: Scammers use threats and urgency to scare you into acting immediately. If you are concerned, always contact the organization directly whether by phone or online. Never reply to a suspicious email.

6. **Bad Links**: Always hover your mouse over a link to see the true destination. If you see a long, unfamiliar link, it’s likely a phish.

For more information go to oit.utk.edu/phishing
When in doubt, contact the OIT HelpDesk for assistance at 865-974-9900 or visit help.utk.edu.