FOLLOW THESE TIPS

Be aware of phishing emails and online ads while remote teaching and working.

*Keep your equipment secure and up-to-date.* Ensure that your computer, mobile devices, and programs have security patches, antivirus applications, and updates installed and running.

*Think before you print.* Don’t print files containing confidential data.

*Avoid connecting to public Wi-Fi networks* to complete TU job-related tasks.

*Be extra cautious of unexpected emails.* Do not click on links or fulfill any unusual request. And use caution when downloading any unexpected attachments.

*Work from a safe and quiet place* and limit access to the device you use for work. If it’s a university-owned device, only you the TU employee, should have access to it.

*Report all* suspicious emails by using the ‘Report Phish’ button in Outlook or by forwarding the email to phishing@towson.edu.