Beginning next week the Cyber Security Team here at UTSA will begin a series of mock Phishing Email training events.

Employees are expected to report any externally received emails that seem suspicious or seem to be asking for personally identifiable information or any information that the company would seek to keep private.

Following any links or opening any attachments that come with these emails in a real environment could cause serious harm to employee personal data or company information as a whole. Failure to notice the difference between phishing attempts and following links or downloading attachments will result in the employee needing to complete mandatory remedial training.

Phishing attempts can look like having won a competition, it can look like an 3rd party contractor that is asking for a suspicious amount of information, or it can look like an email from a coworker that has had their email account stolen.

With the implementation of these measures, we are hoping to all become a more information security minded team.