(Draft) Two Factor Authentication

Background information:

Email has become the most popular attack vector for cybercriminals to steal usernames and passwords. As a major research university, we are constantly targeted by nation-state actors seeking to steal research and academic data, and intellectual property. Hackers attacking University email systems, networks, desktop computers and research labs have become the new normal and, unfortunately, the damage done can be very serious. In March, the Department of Justice revealed a 'spearphishing' campaign in which nation-state actors targeted more than 100,000 accounts of professors around the world. Hackers successfully compromised 8,000 email accounts across 144 U.S. based universities and managed to steal 31.5 terabytes of academic data and intellectual property causing losses estimated in the billions of dollars.

Securing our email services with two-factor authentication (2FA) is the first step to help address this growing problem. 2FA strengthens access security by requiring two methods to verify identity:

1. Something you know (your UT EID credentials)
2. Something you have (a device such as a smartphone or tablet)

2FA helps protect against phishing, password brute-force attacks, and attackers exploiting weak or stolen credentials. It’s already in targeted use at the university to secure highly sensitive information and services. For example, faculty and staff are required to use 2FA for claiming their W-2 or connecting to the VPN.

Many of you have received an email from Google instructing you to enable two-factor authentication on your UTmail. We would like to confirm that that was not a phishing email, but instructions on implementing a new university policy.

What do I do?

If you have Office 365:
- you can use Duo for 2FA
- instructions to implement this can be found here: https://ut.service-now.com/utss/KAhome.do?number=KB0017056

If you have UTmail:
- you must use Google’s platform for 2FA
- instructions to implement this can be found here: https://ut.service-now.com/utss/KAhome.do?number=KB0017061

How can I authenticate?

- A Smart Phone using the DUO App
- Text Message
- Phone Call
- Physical Key Fob (This is only in extreme circumstances)

For additional information:

- See additional information here
- Contact the CNS Help Desk