UTSA®

The Office of Information Technology

Two-Factor Authentication

Agenda

What is two-factor authentication?

Why are we implementing two-factor?

What is affected?

What tool is used and how does it work?

What is two-factor authentication?

- To provide assurance of a user’s identity, we require users to authenticate
- Authentication is based on *factors*
  - *Knowledge* factors (something you know, like a password)
  - *Possession* factors (something you have, like a phone)
  - *Inherence* factors (something you are, like a fingerprint)
- Adding a check of “something you have” to the regular myUTSA ID password check (“something you know”) provides two-factor authentication

Why are we implementing two-factor authentication?

- UT System memo requiring two-factor authentication in certain cases
- Phishing attacks at UT System institutions resulted in financial losses
- If the secret in a single-factor authentication scheme gets compromised, full authentication is possible
- Successful phishing attacks can compromise single-factor authentication

What services will be affected by two-factor authentication?

- When an employee connects to the UTSA network via VPN or terminal services such Citrix
- Modification of employee banking or financial information
- Server admin or other individual working from a remote location uses admin credentials to access a server containing confidential university data
- Faculty services tab in ASAP – November 2015

What tool is used and how does it work?

- We will use mobile devices to provide two-factor authentication using a tool called Toopher
- Toopher works with both iPhones and Android phones, and provides an SMS (text messaging) option

How does it work?

- The first time a user accesses a Toopher-protected application, he/she is asked to download the free Toopher app or use the SMS text option to “pair” their mobile device with their myUTSA ID
- The user then completes the two-factor authentication using the Toopher app, SMS option, or pre-generated one-time password