Modernizing UA's Password Policies

Current Standard User Password Policy

- Length: 8 characters

- Minimum complexity requirements are some combination* of the following:
    - o 1 special character
    - o 1 lower case
    - o 1 upper case
    - o 1 number
    - o Cannot include first or last name, SSN, UAID, or username

- Expiration: 400 days

*varies by university

Problems with this Policy

- Short passwords take less time to crack

- Complexity requirements (like "@ut0Mat2!") make passwords easy for a computer to crack but harder for humans to remember

- Since it's hard to remember complicated passwords, people tend to:
  - Reuse them
  - Choose weak passwords, ie "November2024!"

UA is moving to Passphrases

- Longer than a standard password

- Easy for humans to remember

- Hard for computers to guess

- Keep for a longer period of time

How do I make a passphrase?

- Think of three or four random things that are meaningful to you but not related to each other

- Put them together

- You have a passphrase, like:

Sandy pumpkin 1776   18 characters

New Standard User Password Policy

- Effective Date: January 2025
- 16 characters
- Complexity requirements:
  - No more than four repetitive or sequential characters (e.g. aaaaa,12345, abcde)

  o May not contain user's first or last name or assigned UA username
- Expiration: 730 days