Protect your UMN account

UMN PASSWORD REQUIREMENTS

**PASSWORD** (16 or more characters)

At least one of each:

- **UPPERCASE LETTERS** + **lowercase letters**

You can also use special characters (such as - @ # $) and numbers, but the University only requires the use of uppercase and lowercase letters in passwords that have more than 16 characters.

CREATE A PASSPHRASE!

Instead of using a string of characters with a variety of types (uppercase, lowercase, special characters, and/or numerals), you can use more words with fewer character types (spaces count as characters too!).

**PASSPHRASE** (random words)

E.g. Squid Architecture, I love cheese sauce
PROTECT YOUR UMN PASSWORD AND DUO SECURITY ACCESS

- Do not share your password, passphrase, or bypass codes with anyone.
- Create a different password or phrase for each of your accounts.
- Store hints about your passwords and your Duo bypass codes in a secure location like an encrypted file or password manager application.
- Change your password or passphrase if you suspect someone else knows it.
- When using public computers or shared devices, completely close all applications and browsers when you leave.

REPORT INFORMATION SECURITY INCIDENTS

Report suspected misuse of UMN internet password or Duo Security access to University Information Security at security@umn.edu.

REPORT EMAIL SCAMS

Report email scams ("phishing") targeting the University to phishing@umn.edu and learn more at it.umn.edu/phishing.

Learn more at it.umn.edu/safe-computing.

Questions? Send general information security or policy inquiries to security@umn.edu.