PROTECTING YOUR PASSWORDS

A password or passphrase can include letters, numbers, and special characters (including spaces). Passphrases are phrases and sometimes are from a favorite song lyric or quote. A strong password or passphrase uses a combination of length and character types. Longer passwords or passphrases increase the strength.

When creating a password or passphrase, steer clear of:
- Numbers added to the beginning or end of a word,
- Personal information (e.g., user ID, family or pet names, or birthdays),
- Common keyboard patterns (e.g., qwerty), or
- Duplicate characters (e.g., aabbccdd).

EXAMPLES OF A STRONG PASSWORD AND PASSPHRASE

Password: a!Phab3T50Up (The words alphabet soup with other characters)
Passphrase: Superman is $uper str0ng!

PROTECT

your U of M internet password and Duo Two-Factor Authentication access. Do not share your password or use the same phrase for multiple accounts.

CHANGE

your University Internet Password and account secrets periodically. For help, contact UMN Technology Help at 612-301-4357 or help@umn.edu.

REPORT

suspected abuse of U of M internet password and Duo Two-Factor Authentication access to University Information Security at abuse@umn.edu.

STORE

hints about passwords or passphrases in a secure location like a locked file or password manager application.

LEARN

more about the do’s and don’ts of secure passwords at it.umn.edu.

QUESTIONS?

Contact the Information Security team at infosecurity@umn.edu or visit it.umn.edu/safe-computing.