Passwords [1]

Key Actions

- Use a different password for each online account.
- To remember all your passwords, Duke offers the premium version of LastPass [2] password manager service free to all faculty, staff and students. LastPass allows you to generate a random, lengthy password to protect each of your accounts.
- Don't share your NetID password with anyone, including your parents or other family members. Students can set up a guest account for their parents which will let you share some or all of your Duke information with them.

Duke rules and recommendations

According to Duke requirements, passwords must contain at least 8 characters, including a mix of:

- A combination of upper- and lowercase characters
- A number or special character, such as * ! _ $ # & % @ ^ = ~ + -

Passwords cannot be equal to a current password or password reset answer; equal to your NetID or name; or a single word that appears in the dictionary (English or non-English). Passwords must be composed only of characters in the Roman alphabet, numbers or symbols on the U.S. keyboard. (Examples include characters such as # $ % ! @.)

Tips for creating a stronger password

Duke's IT Security Office recommends a password of 16 or more characters, composed of words or pass-phrases.

Longer passwords are better because the increased length means it takes hackers and their password-cracking tools longer to guess or brute-force the password. We recommend stringing together 4 or more words that are not related to each other or to you. For example, you might start with:

flower wall brown cat

Now add some capitalization, symbols and numbers to make the password more unguessable:
Fl0wer-wall-br0wn-cat

This password is 21 characters, but easy to remember and type. The length makes it difficult for a hacker to guess or crack. To test your password strength, try this calculator [3].

Source URL: https://security.duke.edu/passwords

Links
[1] https://security.duke.edu/passwords
[2] https://security.duke.edu/lastpass