

Security @ND: Password security

Your Notre Dame account unlocks a wide range of applications and systems that provide access to research data, intellectual property, and personal/confidential information.

One of the most important precautions you can take in protecting you and your information is setting a strong password to your account. Weak passwords are easily compromised leaving you vulnerable to hackers and fraudulent use of your personal information.

Keeping your password secure is the first line of defence in preventing unwanted access to your account.

Password Requirements

Your new password must adhere to the following security requirements,

- Must be at least 7 characters in length.
- Must contain a capital letter, lowercase letters and a number e.g. (1, 2, 3, 4, and 5).
- Cannot contain your first name, last name or student number.
- Can contain symbols/characters if you wish to strengthen your password. e.g. (!@#\$\$%^&*+_)

Password cannot be changed more than once in 24 hours. You also cannot use the last 24 previously set passwords on your account.

It is best practice not to change the number or symbol to the next increment when your password expires. It is better to select a passphrase instead to keep your account secure.

Passphrase or Password?

Why should I use a Passphrase? Is it not the same as a Password? A password is easier to crack as it is created using a common word, number, and symbol not generally more than 10 characters long. A passphrase is harder to crack as it is longer than 14 characters and contains different practices such as full stops, spaces, and sayings that are not grammatically correct.

Creating your Passphrase

Passphrases can be created using the following information.

- Over 14 and up to 127 characters
- Adding spaces between words
- Using random words and phrase

| Type | Idea | Phrase | Passphrase |
|----------------|--|--|---------------------------------------|
| Location | You can use a town, city, country or state. A place that holds meaning to you is easier to remember. | Niagara Falls Yellowstone National Park | N1ag4r4F@lls! Y3ll0wSt0ne.N@t.P@Rk |
| Ideas/Goals | Set a goal and use a passphrase to achieve it. | New York City 2020 Be a world traveler | N3wY0rkC!ty2020 B3@w0rldTr2vel3r |
| Movies | Use your favorite film, TV series, book or author to set a passphrase you will easily remember. | Terminator 2 Lord of the Rings | T3rmIn@t0rTWO Ush@llN0tP@\$\$! |
| Sayings/Quotes | Turn something you say out loud into a passphrase. Even if someone knows the saying, they won't know the spelling. | Keep Smiling Each to his own | K33pSm1lling! E@ch.2.his.OWn |

Account Lockout

When you unsuccessfully login to your account 5 times your access to the system is locked out for 60 minutes. After 60 minutes access is restored and login is available again for all devices.

A locked account may present with one or more of the following issues on and off campus.

- Error message at login "Referenced account is locked."
- Unable to access UNDA-WiFi and UNDA-AD wireless networks on university or BYO devices
- Emails not received on computer or BYOD
- Unable to log onto university applications and portals (Blackboard, Allocate, PeopleSoft)

If you are unsure of the cause of the account lockout, it is best practice to reset your password. If you are experiencing multiple accounts, please Contact IT Service Desk.

Please kindly contact your campus Service Desk if you require assistance.

Fremantle

08 9433 0777
8am – 5pm WAST

fremantle.it@nd.edu.au

Sydney

02 8204 4444
8am – 5pm AEST

sydney.it@nd.edu.au

Broome

08 9192 0632
8am – 4:30pm WAST

broome.it@nd.edu.au