

Help and resources

Questions about cyber security?

If you have any questions about the security of your University of Waterloo account, please call **ext. 41125** or email **soc@uwaterloo.ca**.

Get informed, stay safe

For more cyber security information, please visit **uwaterloo.ca/cyber-awareness**.

Don't get phished

Verify email senders

- **Review the display name:** it may show the suspicious email address, not an actual name.
- **Hover your cursor over the email display name:** you may need to hover over the envelope icon.
- **View the sender's contact card:** click the circle icon beside the sender's display name to view the sender's information.

Questions about other IT concerns?

Please contact the IST Service Desk by calling **ext. 44357** or email **helpdesk@uwaterloo.ca**.

DID YOU KNOW?

You can self-register for free information security courses on LEARN. Click on the 'Self Registration' tab from the top menu bar to enroll in:

- Information Security Awareness Training
- Information Security Awareness for Finance and Commerce
- Optional topics in Information Security Awareness



LOCK IT DOWN

Password Security
Best Practices and Guidelines

Before

changing your password

Password complexity requirements

All passwords must contain characters from **at least three** of the following five categories:

- English uppercase characters (A — Z)
- English lowercase characters (a — z)
- Base 10 digits (0 — 9)
- Non-alphanumeric (e.g. !, \$, #, or %)
- Unicode characters

The minimum password length is **8 characters**.

Passphrase

/'pas,frāz/, (noun):

a password that contains:

- at least 4 unique words
- some numbers and punctuation
- at least 15 characters in length

Example: *'Vision2020,whenthegeeseattack'*

PASSPHRASE TIP

This passphrase example has one upper-case letter, four numbers, and two punctuation characters. It's also memorable. While the use of dictionary words in a password is discouraged, **using words to form a passphrase of total length greater than 14 characters is acceptable.**

Change

your password

Change it up

When changing your password/passphrase, be sure to pick one that's very different than the one you are replacing. If your previous password/passphrase was compromised, **adding a single digit or character to it will not be enough to prevent your account from being compromised again.**

It is very important to **avoid reusing passwords between sites**. When you reuse passwords, a security breach at one site means your information is on risk at other sites where you used that same password.

To reset your password/passphrase, log in to **uwaterloo.ca/watiam** and select the 'Change Password' option from the Home page.

After

changing your password

Update your credentials on mobile

Most users access digital services at the University of Waterloo from more than one device (e.g. smartphone, laptop). To prevent getting locked out of your accounts, be sure to **update your devices with your new password as soon as possible** after making the change.

Two-factor authentication (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your University accounts. Verifying your identity using a second factor, like your mobile phone or tablet, prevents others from accessing your accounts, even if they know your password.

For more information about 2FA, please visit **uwaterloo.ca/two-factor-authentication**.

2FA TIP

When prompted to authenticate, click 'Cancel' and select 'Remember me for 30 days'.