Keeping Your Account Secure

Strong passphrases and multi-factor authentication (MFA) are the most important tools to keep your online accounts secure. Protecting your accounts keeps your personal data and UVic's data safe and secure. Use the following tips to help you practice good security hygiene.

Set a strong passphrase

Good passphrases are the first line of defense to protect any online account. When creating your passphrase, keep the following things in mind:

✓	✗
Choose a passphrase that is between 12 and 128 characters long	Don't repeat numbers or use sequential keyboard characters in your passphrase (i.e., 111, qwerty)
Include at least two of the following: lowercase, uppercase, digits, or special characters (e.g., $, _, #)	Don't include any personal information in your passphrase (e.g., first name, last name, birth date)

* You should never write down or store your passphrase in plain text on your computer.*

Don't reuse passphrases

- Never reuse your old or short passphrases. Cybercriminals may maintain or access lists of common or known passphrases and try to use these to access accounts. Modern computing can brute force eight character passphrases in just 2 minutes!
- Use a different passphrase for each service you use. Once a hacker finds the passphrase for one service, they could access them all.

Keep your passphrase secure

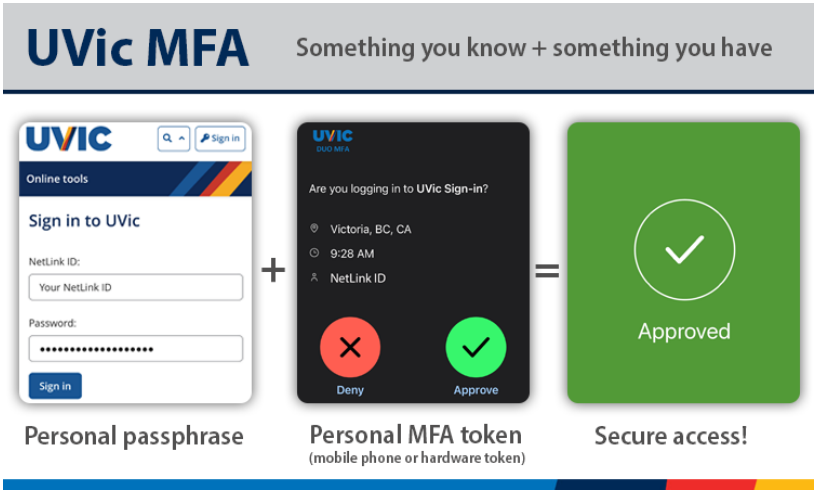
- Use a passphrase manager such as KeePass to remember unique passphrases. A passphrase manager enters the username/passphrase combinations required to access different resources and stores them in an encrypted, passphrase protected file. For more information, review the UVic Systems page on Secure Passphrase Storage.
- Never share your NetLink ID and passphrase with anyone, for any reason, no matter what.
- Phishing is a common scam where a malicious person attempts to trick you into providing your username and passphrase by pretending to represent a legitimate contact such as a bank, utility company, or UVic. Learn to spot the signs of phishing and how to avoid these scams by completing the University Systems Phishing Awareness training.
- Verify emails received by using known good contact information for the sender or company to verify the authenticity of a message. If it sounds too good to be true, it probably is!

In 2022, University Systems started to offer an additional layer of security for UVic NetLink IDs designed to protect your account, your information, and access to university information resources. UVic MFA is required for all critical systems as of May 15, 2022.

What is UVic MFA?

UVic MFA strengthens NetLink account security by requiring a second factor when you login to online services. The first factor we use is a *passphrase* – something you know. The second factor is something you have – such as a *device* in your possession. UVic MFA uses a quick, simple push system through a mobile app to verify you have the device.

More information and how to enrol is available at [UVic MFA].



Why do we need UVic MFA?

"MFA is a critical tool to protect your accounts and information by providing an additional layer of protection if someone gets a hold of your passphrase. This additional security prevents them from logging in as you—even if they have your passphrase. For this to work, everyone must enroll in UVic MFA."

Kevin Hall - President & Vice-Chancellor

UVic MFA helps us protect against attempts to steal information entrusted to our care, including financial data and student and employee records. Using UVic MFA, we can help to prevent:

- Criminals attempting to commit identity fraud
- Unauthorized access to your applications and personal information contained within
- Attempts to change your payroll or financial aid direct deposit settings without your knowledge

Tips and Tricks

Don't have your phone or internet access to sign in?

- Use Duo Mobile app offline to generate sign-in codes
- Use a Duo hardware token
- Generate bypass codes

Stop and think about any prompts from the Duo app.

Are you currently signing-in to a service?

If you receive a prompt that did not originate from your sign-in attempt, **deny the request**, change your passphrase, and contact the Computer Help Desk for assistance.

more tips at [MFA Common Questions]

For further information:

[Computer Help Desk website]

helpdesk@uvic.ca