Strong Passphrases

Good passphrases are the most important tool to protect any online account. It is important to create and maintain strong passphrases to help keep your personal data and UVic's data safe and secure. Use the following tips to help you practice good passphrase hygiene.

Regularly change your passphrase

Change your passphrase at least once a year. Good passphrases are the most important tool to protect any online account. When creating your passphrase, keep the following things in mind:

✓	✗
Choose a passphrase that is between 8 and 30 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. Many hackers maintain lists of common or known passphrases and try to use these to access accounts. Modern computing can brute force eight character passphrases in just six hours!
- 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 or 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 at www.uvic.ca/phishing.
- Verify emails received by going directly to the official website of the company and logging into your account to check the status or by contacting the sender through another method such as the telephone.

Who can I contact for assistance?

Contact University Systems Computer Help Desk for assistance with your NetLink ID, passphrase, or if you are unsure if an email is fraudulent.