Cybersecurity: Passphrases

These tips will help you create complex passwords known as passphrases.

What is it?

Passwords are the first line of defense protecting your online accounts. Creating strong, unique passwords pays off, but you can take that idea one step further by developing passphrases.

A passphrase is a longer, more complex password that is easy to remember but hard to guess.

How can I build a passphrase?

Start with a phrase that means something to you. Try to avoid common phrases, like “The early bird gets the worm.”

This could be a song lyric or a sentence you know you’ll remember. For example:

- I live in Alberta

Then replace some of the letters and spaces with upper-case letters, numbers, special characters, or memorable shorthand:

- 1 |_!ve N *AB*

Just remember not to use our example.

Parts of a passphrase

When creating a passphrase, make sure it meets these guidelines:

- Use at least 12 characters to make your password harder to crack.
- Use a combination of lower- and upper-case letters, numbers, and special characters (ex: $ % & *_).
- Use spaces, if the platform allows it.
- Avoid using personal information, like your birthday or a pet’s name.
- Avoid using any single dictionary word or common phrases.
- Avoid using a pattern when replacing characters. For example, avoid replacing all As with 4s.

Avoid using an online password generator. Your information might be stored by the service that generates the password.

Be unique

Using a recycled password makes accessing your accounts easy, but it also leaves them vulnerable.

Did you know that stolen username and password combinations are bought and sold online after they are compromised in a security breach?

Cybercriminals know that most people use the same password on multiple accounts. In a common cyberattack know as a brute force, attackers will use these compromised credentials on other popular websites to try gaining access to your personal information.

Change it up

To help further protect your accounts, remember to update your password regularly. Consider changing your passphrase at least once a year, if the website or application experiences a breach, if malware is detected on your device, or after sharing it with someone—even if it’s someone you trust.

Keep it secret

Keep your passwords private for all accounts, including your email, social media, or online shopping profiles. Do not share them with anyone, including trusted friends or family members. Only an account owner or administrator should be able to access it.

Rather than write down your passwords, consider using a password manager to keep track.

Did you know?

Password crackers are software that use an algorithm to recover passwords using previously transmitted data that has been stored on a computer, even if it’s scrambled. Password crackers can test millions of passwords every second.

A simple 5-character password that only uses letters, like “CYBER”, can be cracked in less than 30 seconds.

A complex 12-character password that uses a combination of letters, numbers, and special characters, like “1 |_!ve N *AB*”, takes about 3,000 years to break.

CYBERSECURITY TIPS

Visit Alberta.ca/cybersecurity-in-alberta for more information.

Alberta