Tech Safe BC

How to Create and Maintain Strong Passwords

Compiled by Tech Safe BC

Last Updated: January 27, 2026

Table of Contents:

If you would like to watch a simplified version of this document in a video form, click on this YouTube link.

Symbols and What They Mean in This Guide:

Course of action may be visible to your former or current partner.
You may want to consult with a staff of an anti-violence program in your community before removing your former or current partner's access.

Why Is It Important to Have a Strong Password?

When your accounts are compromised by a former or current partner, they can gather personal details about you such as your location, addresses, and any content you upload to your account. It is important to make sure all your passwords are secure and hard to guess. Consider using a password manager to store all your passwords, you can learn more about it below.

What Does a Weak Password Look Like?

Since passwords are often hard to remember, users tend to use simple passwords, or the same passwords on multiple services. This can make it easy for current/former partner to access your accounts if the passwords can be easily found.

A weak password is one that is easy to guess such as:

- Using common passwords, such as "password" or "ABC123"
- Using your own, children's or pet's names or any important dates
- Using the same password for all your accounts
- Answering backup questions with answers your former/current partner may be able to guess (e.g. your favourite colour or the name of your first pet)

Safety Tip:

If you think any of your accounts have weak passwords or may be compromised, consider consulting with a support worker before making the change. When you change a password, the email or phone numbers connected to those accounts will be notified. If your former or current partner has access to those contact methods, they could be notified and potentially increase your risk to violence. Always prioritize your safety and seek guidance if you're unsure.

What Does a Strong Password Look Like?

A strong password is a long and unique combination of random letters, numbers and symbols. The password should not involve any information about yourself, your children, or any pets.

It should be hard for your current/former partner to guess your password and should look like:

- Be at least 12 characters long
- Uses a mix of capital and lowercase letters or is all uppercase or all lowercase
- May use a combination of numbers and symbols (such as $, &, @)
- If you use words, they are unrelated to personal information about you, your children's or pet's names or any important dates
- Examples:
    - "Lem0m:C@mpu1er9"
    - "dr1nK&W1nd0.ws"
    - "orangesbearceilingproduce37"

The following website can help you test the strength of passwords:

https://password.kaspersky.com

What Are Password Managers and How Do They Work?

One of the safest options for generating and storing passwords is by using a password manager app as they encourage users to have safe password habits. Password managers can help you create unique and strong passwords, safely store your passwords with end-to-end encryption, and can help check if your passwords are compromised.

Password managers work by asking you to make a master password which gives you access to all the stored passwords in the manager. This will be a password you have to memorize to log into your manager.

When setting up a password manager on your device, it can look like:

- Making a master password and setting up your account
- Giving the password manager app permissions to autofill passwords in your device settings
- Setting the password manager app as the default password autofill source

After the set-up is completed, your phone will automatically suggest your password manager to help you create passwords and store them every time you make, or log into an account. Additionally, you will also have the feature to manually input passwords yourself in the app.

A secure password manager should be:

- End-to-end encrypted
- Have 2-factor authentication

- Help you create strong and unique passwords
- Makes it easy to manage your passwords across multiple devices

Most reliable options can be downloaded directly from Apple's App Store or Google Play Store.

What Are Ways to Remember Strong Passwords?

If you have trouble using password managers, you can use different tricks to remember your passwords. Remember to still include a mix of numbers and symbols to create a strong and unique password!

1. Write a sentence you will remember but modify the password by purposely making typos or changing certain terms.

You could make sentences related to your favorite colour, music artist, show, foods, common sayings, etc.

Example: Removing all vowels

> **Original sentence**: My Favourite Song Is 22 By Taylor Swift! 22/10/2012
>
> **Tip:** If you can't think of any numbers, you could add a random date such as the day that the song released, the day that the album released, or the day that the song hit top charts!

Secure password: MyFvteSngs22BTlrSwft!22/10/2012

Example: Purposely misspelling words

Original sentence: I Love Sushi And Pizza <3

Secure password: EyeLuvSh0esheAnPizah<3

Example: Changing certain letters that look like symbols/numbers into symbols/numbers

Original sentence: Always Look On The Bright Side Of Things

Secure password: @!way5-L00k-0n-Th3-Br1ght-S1de-0f-Th1ngs

2. Remember a specific keyboard typing pattern.

Example Password: 1290QwOpAsKlZxNm

This password was made by using the pattern of typing the first two and the last two letters/numbers of each row on the keyboard. Then, every other letter was capitalized to introduce variation and strength to the password. You can think of more patterns to generate unique and secure passwords.

3. Combine random words and list them in alphabetical order. Then, modify the password by adding symbols and numbers to make it unique.

Example Words: Airpod Flow Tiger Ukulele X-ray

Secure password: AirP0d-Flw-T1ger-kll+X-ray$

What Are Good Password Habits?

Maintaining good password habits can help keep all your accounts secure and prevent your passwords from being compromised in the future.

☐ Use different passwords for each account.

Each account should have its own unique password to ensure that one account compromise does not put other accounts at risk of being accessed.

☐ Enable 2-Factor Authentication on all your accounts.

This allows for an extra layer of security and makes it harder to have unauthorized logins. You can refer to What is 2-Factor Authentication (2FA)? to learn how to set it up and what it looks like.

☐ Avoid using password keychains from your browser such as Google Chrome or Edge.

The passwords can be easily accessible to your current/former partner as users tend to stay logged in on their browser even if it's not being used. Consider using a password manager to store your passwords instead.

☐ Use modified or false answers to security questions.

Someone who knows you can easily guess where you went to school or the name of your first pet. The answers to your security questions do not always have to be truthful. You can also consider using answers that are truthful to you but purposely have typos.

☐ Keep all your accounts separate.

Services like Facebook, Google, or TikTok may give you the option to sign into other accounts using an account you already have with them. This can pose a risk to your accounts as multiple accounts can be accessed when one account is compromised.

☐ Store your account passwords at a safe place.

If you prefer to write down your passwords, avoid storing them in an easy to access place such as on your computer monitor or the drawer next to your desk. Using a password manager app would be the safest option.

☐ Always remember to log out of your accounts, especially for public devices.

Avoid clicking “Remember Me” or “Keep Me Logged In” on devices you use to avoid unauthorized use of your accounts.

If you are experiencing tech abuse, you are not alone. Find support in your community by connecting with a BC Society of Transition Houses Member Program or check out our other safety resources at techsafebc.bcsth.ca.