In today's digital world, almost everything online is protected by a password or passkey. Your email, banking, social media accounts, medical portals, etc. all require login information. Without a way for your loved ones to access those accounts after you are gone, your important files can be lost forever.

A password manager stores your passwords securely, helps you create strong and unique passwords for every account, and then you only have to remember the master password to unlock your password manager. A good password manager also gives you a way to plan ahead so your trusted contacts can access what they need after your death.

University of Manitoba

Latulipe Research Group
Human-Computer Interaction Lab
Department of Computer Science
University of Manitoba
hci.cs.umanitoba.ca
celinelatulipe.net

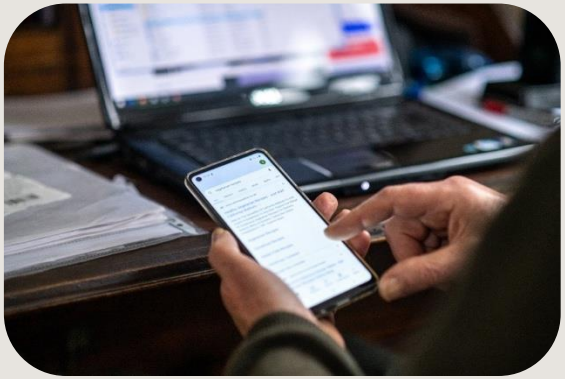
Password Managers

Digital Legacy Planning

Version 1

What is a password manager?

A password manager is a tool that stores your login credentials in an encrypted location called a **vault**. Instead of remembering every password you've created, you only need to remember **one master password** to unlock the vault.



Most password managers have features such as:

- Generating strong passwords
- Storing secure notes
- Saving payment information
- Syncing across devices, making it accessible on your phone, computer, and tablet

When a person passes away, their loved ones are often left guessing which accounts exist. Without this information, they can lose access to:

1. **Family photos** and **important documents** stored in cloud services
2. **Financial accounts**, on banking, investment, or retirement platforms
3. **Social media accounts**
4. **Subscriptions** that may continue to renew
5. **Health and medical portals** that contain diagnoses, prescription info and test results

A password manager gives your loved ones a single place to find everything they need, provided you have set it up properly and shared access with a trusted person.

Setting Up a Password Manager

1. **Choose a password manager**. Not all password managers have the same features, and some require a paid subscription. Some good password managers that support setting up an emergency contact are: LastPass, NordPass, ProtonPass, and Bitwarden.

2. **Create your vault** by setting up your account and adding your login credentials. Whenever you sign in to a new digital account, you'll be prompted to add the credentials to your password manager.

3. **Add notes** in the password manager to record important details, which can include email recovery codes, or instructions for specific accounts.

4. Set up **Emergency or Legacy Access** by adding a trusted person as your emergency contact. Your vault contains sensitive information. Choose your emergency contact carefully.

5. **Tell your emergency contact** that the password manager exists and where to find information about it.