

Recommended Password Managers

Cybersecurity starts with strong password protection. Update your passwords regularly and use unique, strong and complex passwords for every account that you maintain. Don't reuse your passwords between sites and systems.





Elements that make a strong password:

- 10-20 characters
- Combination of uppercase and lowercase letters
- Include numbers and symbols
- Don't choose obvious passwords (e.g. Password, 123456 & replacements like '@' instead of 'a')
- Don't choose passwords that can be found easily in the dictionary (any language)

Remembering multiple passwords can be challenging. We've got you covered!

Password Managers: It is unsafe to store passwords in unprotected documents such as Microsoft excel or word. Passwords managers help you generate unique and strong passwords and store them in a safe and secure environment.

Douglas College Information Security recommends the following password manager sites

Name	About	Link
 KeePass	KeePass is a free open source password manager which helps you manage your password in a secure way.	https://keepass.info/
 LastPass	LastPass is a secure password manager that comes in free and premium versions.	https://www.lastpass.com/password-manager
	1Password is a trusted and secure password manager that comes in paid version.	https://1password.com/
 dashlane	Dashlane is a secure and safe password manager that comes in free and paid versions.	https://www.dashlane.com/

Please note: These are external vendor sites and if you have any questions or concerns about the usage or access of these sites please contact the respective vendors directly.