



CHILTON PUBLIC LIBRARY  
CHILTON, WISCONSIN

# CHILTON PUBLIC LIBRARY

www.chiltonlibrary.org

## KEEP IT SECRET KEEP IT SAFE

### Creating & Managing Passwords



#### CREATING A STRONG PASSWORD

Passwords are needed for almost everything that you do online. From creating an account to browsing a catalog to viewing a 401K balance, a strong password helps protect your account from being accessed by unauthorized users.

- Never use personal information (name, username, birthday)
- Use a longer password (at least 6 characters)
- Try to use numbers, symbols, uppercase, lowercase - mix it up
- Don't use the same password
- Random passwords are the best.



#### Cybercriminals on the hunt.

64% of consumers with more than one password exposed kept reusing that password somewhere else.

Once a login name and password are exposed in a data breach, criminals will try that same combination many more times across the web, in a kind of attack called credential stuffing.

**Experts now say that you don't need to change your passwords on a regular basis. However, if it's exposed in a data breach, change it immediately.**

## Password Managers

A password manager is a program that stores, generates, and manages passwords.

Can generate a complex password for each of your online accounts. Then you access those password with a master password.



### 1Password

- Premium service
- Unlimited Devices
- Can share passwords (with Family)
- 365 day item history

LastPass

### LastPass

- Free or Premium service
- Main feature only available with Premium or Family (unlimited devices, share passwords)



### Dashlane

- Free or Premium service
- Main feature only available with Premium or Family (unlimited passwords, unlimited devices, share passwords)
- Bulk password change



### Keeper

- Free or Premium service
- Main feature only available with Premium or Family (unlimited passwords, unlimited devices, share passwords)
- À la carte features

## Multifactor authentication



Multifactor authentication increases security. A user presents two or more pieces factors for authentication.

Common types of authentication factors:

**Type 1: Knowledge** - Something you know, such as a password, or answer to a question

**Type 2: Possession** - Something you have, such as a security key or token

**Type 3: Inherence** - Something you are, such as a unique biometric or behavioral characteristic

Contact us


 920-849-4414

 [chiltonpubliclibrary@gmail.com](mailto:chiltonpubliclibrary@gmail.com)

## **References**

The Dummies Guide To Password Security - <https://edtimes.in/the-dummies-guide-to-password-security/>  
Internet Safety - Creating Strong Passwords - <https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/>  
Choosing and Protecting Passwords - <https://www.cisa.gov/uscert/ncas/tips/ST04-002>  
What are the Key Differences between 2FA and MFA? - <https://www.incognia.com/the-authentication-reference/what-are-the-key-differences-between-2fa-and-mfa#:~:text=MFA%20vs%202FA,all%20MFA%20is%20a%202FA.>

**Contact us**

 920-849-4414

 [chiltonpubliclibrary@gmail.com](mailto:chiltonpubliclibrary@gmail.com)