

Use strong passwords or passphrases



When you use simple passwords or passphrases, or if you reuse the same one for multiple accounts, they are easy for cybercriminals to guess. It's like locking your front door and leaving the key in the lock. Use long, unique passwords or passphrases to protect your data, money, and identity.

WHAT YOU CAN DO

Create long, unique passwords or passphrases

- Strong **passwords** rely on length and character types.
- Strong **passphrases** rely on five to seven unassociated words.



Use a password manager

A password manager can generate, store, and autofill unique passwords for all your accounts – on your computer and mobile device.

SECURITY DO'S AND DON'TS



- › **Do** check if your email address was in a data breach at haveibeenpwned.com, and if it was, change your password.



- › **Do** turn on multi-factor authentication whenever possible for email, social media, health, and financial accounts.



- › **Don't** share your passwords or passphrases with anyone.



- › **Don't** save passwords or passphrases in a file on your computer, or in your browser.

STRONGER IS SAFER

Make them long

- Use a minimum of 14 characters. The longer they are, the stronger they are.

Make them unique

- Use a different password or passphrase for every online account you have.

Make them complex

- Select random words and numbers.
- Use special characters such as \$, %, &
- Substitute letters with numbers or special characters:
 - 3 for an E
 - Z or \$ for an S
 - @ for an A