Password Safety

Passwords are vulnerable

Hackers have many ways to access our accounts and passwords. They can try using common passwords, using passwords leaked in data breaches, guessing password using public information, etc.

Good password tips

Don't reuse the same password on multiple sites. If you do, a leaked password puts all your accounts at risk.

Change your password when you know a website was breached.

Don't use names, birthdays, or other easy-to-guess info in your password.

Make long passwords. A passphrase (3-5 random words) is strong and easy to remember. E.g., dropkick-imitation-hence8birdseed

But how to remember all the different passwords?

Given the number of accounts we have, it is indeed difficult to remember all unique passwords to each account. Experts recommend:

- **Writing passwords down in safe place** (e.g., a notebook stored in a safe)
- **Using a password manager.** See the next page for more information.

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

Password Managers

What is a password manager?

A password manager is a program that generates **strong, unique passwords** and stores passwords for you. It can also **autofill stored passwords** when you log into accounts.

You need to **remember only one "master password"** to unlock your password manager -- make it strong!

Types of passwords managers

Password storage in system account, e.g., Apple iCloud Keychain

Password storage in browser (e.g., Chrome, Firefox, Edge)

Password manager apps (e.g., 1Password, LastPass, Dashlane)

Isn't it dangerous to put all eggs in one basket?

Intuitively, it is! But in reality password managers are quite safe:

All reputable online password managers **encrypt your credentials**. It means that even if there is a data breach, hackers can only get useless encrypted blobs without your master password.

Moreover,, the benefit of having unique and strong passwords for each account outweigh the risks of password managers being attacked.

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN