Digital Literacy by SPCO

Part 2

2025

Passwords

Online Security Course

What you'll learn by complete this 7 part course :

Part 1:

What is Online Security?

Part 2:

Creating Strong & Safe Passwords

Part 3:

Spotting Phishing & Fake Emails

Part 4:

Secure Browsing Habits

Part 5:

Protecting your Devices

Part 6:

Public Internet & Safe Internet Use

Why passwords matter?

Passwords are the **first line of defense** for your online accounts — like keys to your digital home. A weak password is like a rusty lock that anyone can break.

Hackers can easily guess passwords like:

- 123456
- password
- yourname2024

Once they have your password, they can access:

- Your **email**
- Your **bank accounts**
- Your **social media** — and pretend to be you

What makes a strong password?

A strong password is:

- **Long** (at least 12 characters)
- **Random** (not your birthday, pet's name, or "password123")
- **Unique** (don't reuse the same password on different sites)

✅ A good example: PurpleSun_48!HorseDuck

❌ Bad example: janet1995 or abc123

Pro Tip:

An easy way to create a password is to use **three random words** and a symbol or number.

🟢 TreeCoffee!Window94

This method is **easier to remember** than complex gibberish like T!%4d&y77.

Bonus: Use a password manager

Remembering 10 different passwords? That's hard.

A **password manager** is a secure app that:

- Stores all your passwords in one place
- Helps you generate strong ones
- Automatically fills them in when you log in

3 Password manager options

Google Passwords

Apple Passwords (Keychain)

Microsoft Authenticator

Tip: Never use the same password, if one gets stolen they all become vulnerable!

Real World Example:

Story: Malik used the same password for email & online shopping. When the site got hacked the scammers accessed his email and used it to reset other account passwords.

A password manager could've saved him a lot of stress.

Next Lesson

Spotting Phishing & Fake Emails