

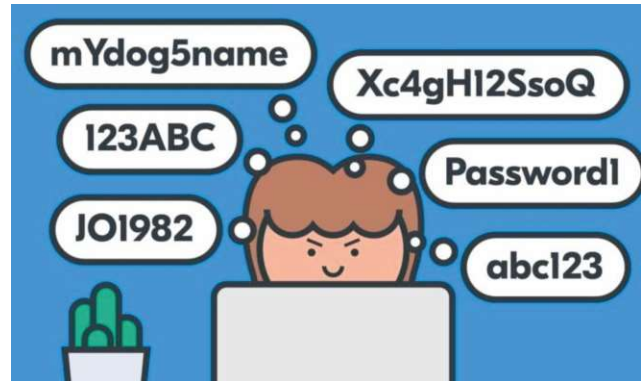
Chapter 3

ALL ABOUT PASSWORDS

Passwords !

You are growing up in a computer-rich world and knowing more about passwords is important.

As you grow, you are likely to increase your social media presence.



Knowing how to set a secure password and why it needs to be kept private are a vital part of staying safe in the cyber environment, not only on websites but also on home and school networks.

According to the **National Cyber Security Centre (NCSC)**, the top five passwords used are

- 123456,
- 123456789,
- qwerty,
- password and
- 1111111.

Have you ever used such easy and prone to hack passwords. Tick below

- ☐ Yes
- ☐ No

Clearly, today in a world where hackers are getting better at breaking into computer systems, it is clear that you have much to learn and do to stay safe.

Lets Know Password !



What is a Password?

It's a secret word or phrase (*****) that helps you get onto a computer, email, game, website or device.

Why do you need to have Strong Password?

It stops other people getting into your accounts online, accessing your personal information, and other stuff that you have in there.

Is it a good idea to put your personal information into your password, like your name, age, favourite sports person?

No, it's not a good idea, because that information is easy for others (even your friends) to guess.

What does a strong password look like?

- It can be a word, a phrase, or a sentence.
- It's long and has capital letters, small letters, numbers, and special characters like !@#\$% and so on.
- They're easy for you to remember but not easy for others to guess!

Examples of a strong password?

✖ Weak Passwords	✔ Strong Passwords
Mydog	MyDogLoves1Treat#Daily
Laura25	L@ura.\$Hops247
roblox	pl@yRoblox41hour
thanks123	A1way\$aYthank.u
disneyplus	watCHd1sney+Plu\$

What could happen if you share your passwords with other people, perhaps your friends?

They could pretend to be you, use your account, change your profile, change your privacy settings, and perhaps share/post or comment online. This then looks as if you did those things.

What are three strong password skills?

- ✓ Use different passwords on every app and game that you use.
- ✓ Don't share them. (It's okay to share your passwords with parents/guardians.)
- ✓ Change them often.

Where can you store your passwords in case you forget them?

- Many devices have '**autofill passwords**' –
 - it asks if you would like for your password to be stored for the next time you need to log on.
- **Tell a guardian or parent** who can keep them safe for you.
 - (This is also useful in case you forget)
- You could use a **Password Manager**
 - A Password Manager stores and manages your passwords for you.
 - To set this up, you would need a grown up to help you. This is useful if you have many passwords.

Setup Secure Password

Where are you using Computers or your email or your other social media accounts.

- At School
- At Home
- At relatives Home.
- At other public places.

Do you type your password at these places?

Yes

No

Word of Advice

Even in your school, you might require to log on to a network computer using your email ID.

Thus, you should be familiar with and setup

SECURE PASSWORD



6 – Rule Principle

A simple set of **six rules** for you to set up safe passwords is:

- ✓ To include numbers, letters and symbols in your password.
- ✓ To use at least one capital letter.
- ✓ To make it something you will remember but others won't think of.
- ✓ To make sure it has eight characters or more.
- ✓ To never use obvious names or dates like your nick name or birthday.
- ✓ To never write down or share your password. (You can share it with your parents or guardian)

Using above rules, create strong password

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____

2FA – Two Factor Authentication

Two-factor authentication adds an additional layer of security to the authentication process.

It does this by asking user to authenticate twice. Once by the password and second time by a different way.

This second way of authentication can be by

- SMS OTP (One Time Password),
- Secret Questions
- Choose right image
- And any other way.

2FA making it harder for attackers to gain access to a person's devices or online accounts because, even if the victim's password is hacked, a password alone is not enough to pass the authentication check.

Example of 2FA using OTP in an email access

Assume you want to access your email which has 2FA setting enabled. The general workflow will be as mentioned below.

1. Login to your Email Client Website (Like <https://www.mail.icodet.com>)
 - Mostly banking sites like <https://www.onlinesbi.com/> supports 2FA for additional security.
2. Click on Sign In option.
3. You are prompted to log in by the application or the website.
4. Enters what you know –
 - Usually, username and password.
 - Then, the site's server finds a match and recognizes you as the user.
5. The site then prompts you to initiate the second login step by asking you to enter OTP sent to your registered mobile number.
6. Then, the user enters a one-time code that was generated during step five.
7. After providing both factors, the user is authenticated and granted access to the application or website.