

How to keep your password strong memorable and safe

Most Importantly

TWO essential password rules to consider when creating a password

1. Length
2. Complexity

- Your password length should be at least 8 characters long
- Your password should use a combination of lower case letters, upper case letters, numbers, and special characters.

Passphrases

"Passphrases" are not only easy to remember but unique to you as well

- History buffs could take Ben Franklin's quote "Man will ultimately be governed by God or by tyrants" and make their *password* "MwubgbG0bt-BF"
- A classic rock fan would make their *password* "Sw33t-Home-Alabama" or "While-My-Guitar-Gently-W33ps"

Use a Password Manager

Strong passwords can be hard to remember and are confusing when dealing with multiple login locations across the web

Use password managers such as:

- **KeePaas:** <http://keepass.info/>
- **LastPaas:** <https://www.lastpass.com/>
- **1pass:** <https://1password.com/>

Change it Often

“Treat your password like your toothbrush,” said Clifford Stoll, U.S. Astronomer and author. “Don’t let anybody else use it, and get a new one every six months.”

While funny, this still holds true

Password Pitfalls to Avoid

- Never use a generic word like “Password” or a sequential number set like “12345.”
- Never use any information about yourself that can be found in the public record. This includes birthdays, anniversaries, license plate numbers, or home addresses
- It’s not a great idea to replace letters with numbers in a common dictionary word. Most botnets are keen to “l33tspeak” and will crack “P455w0rd” just as fast as the word “Password.”
- Never make your password the same as your username
- Never have the same password for two different sites
- Always play it close to the chest regarding your passwords. Never share your password with anyone, either verbally or electronically
- Please don't use the "remember password" option in your browser

Thank YOU !
for further support email to
email-support@iitr.ac.in