

# Create a strong Password and Evaluate its Strength

Password	Estimate To Crack
P@ssWord#42	51 seconds
Q7#x!R9mZ@pl	3 Years
jY4\$ev8*kL2@	3 Years
Blu3_Fox!Runs@Dawn_47	Centuries
st@r_Gal@xy_W1nter#99	Centuries

- Best Practices for Creating Strong Password

1. Length is King : Aim for at least 12-16 characters – longer password have exponentially more combination.
2. Mix Characters Type : Avoid Predictable Sustitution like P@ssword -attackers know these tricks.
3. Avoid Personal and Predictable Info : Don't include your name,birthdate,pet's name,favorite sports team, or any detail that could be found online.
4. Use passphrases for Memorability.
5. Make Every Password Unique.
6. Use a Password Manager.
7. Enable Two-Factor Authentication(2FA)

## 8. Change Password After a Breach.

- Research Common Password Attacks

1. Brute-Force Attack
2. Dictionary Attack
3. Credential Attack
4. Phishing Attack
5. Keylogging
6. Man-in-the-Middle Attack
7. Shoulder Surfing
8. Rainbow Table Attack

- How Password Complexity Affects Security

1. Length, Character Variety, Unpredictability, Avoiding Common Words.
2. A long, random, and varied password takes much longer to crack, greatly improving security against most password attacks.