**PASSWORD STRENGTH EVALUATION**

| **PASSWORD** | **SCORE(100)** | **ESTIMATED TIME TO CRACK** | **FEEDBACK** |
| --- | --- | --- | --- |
| *AnGeL8094#* | **75** | **12 DAYS** | Consider using an even longer password (12+ characters) for maximum security.  Try a passphrase - several random words combined with numbers and symbols. |
| *@NGE|4!3#* | **60** | **1 DAY** | Mix uppercase and lowercase letters throughout your password.  Consider using an even longer password (12+ characters) for maximum security. |
| *AnGle@2o4%!~(8)* | **85** | **50 YEARS** | Try a passphrase - several random words combined with numbers and symbols. |
| *A$<>geL#2+”Dai$E04* | **95** | **70 YEARS** | Excellent password! Remember to use different passwords for different accounts. |

**TIPS LEARNED**

-Don’t reuse passwords across accounts

-Avoid names, birthdays, or common words

-Use a password manager to generate and store strong passwords

-Change passwords regularly

-Use passphrases

| **Attack Type** | **Description** |
| --- | --- |
| Brute Force | Tries all possible character combinations until it finds the correct one. |
| Dictionary Attack | Uses a list of common words/passwords (e.g., "password", "123456"). |
| Phishing | Tricks users into revealing their passwords. |
| Keylogging | Records keystrokes to capture passwords. |

**SUMMARY**

**-**Complex passwords significantly improve security.

-Longer passwords with random characters are harder to guess or crack via brute-force or dictionary attacks.

-Even a few extra characters or symbols can increase cracking time from seconds to centuries.