How to make strong PASSWORDS

Ministry of Justice

As you add characters to a password, the time it takes to crack the password increases exponentially.

Longer = better

A short password is very easy to crack in seconds, regardless of complexity. A long password is very hard to crack. It could take years.

Bad passwords?

- Are short and easy to guess
- Use formulas and patterns that lots of people use
- Confuse complexity with strength

Here are some examples:

1q2w3e4r   M0nkey364

UbiHjr!   Spring2022!

Why?

Computers can make billions of guesses a second.

Hackers use dictionary lists to collect common passwords. They add rules like add numbers or symbols at the end or substitute 'a' for '@' or '4' to guess more possibilities.

Strong Passwords

- Are long
- Use 3 or 4 random words to make a passphrase
- Put numbers or symbols between the random words, not at the end

Complexity is not strength

Length is strength

Here are some examples:

GreenDuck8Burger

Fortuneship6aeroplane!walnut