

Passwords and passphrases

A walkthrough of PrivacySafe Bot

THE QUESTION

What makes a secret hard to guess, and why do the rules keep changing?

THE PROMISE

You will watch a real generator and see the math behind strength.

OUR JOB

Learn what makes a secret strong, then build habits you can keep.

Length

Randomness

Uniqueness

Protection

How passwords get **guessed**

Common passwords first

Attackers try lists of popular and leaked passwords before anything else.

Reuse

One leaked password is tried on many sites. This is credential stuffing.

Offline guessing

After a breach, stolen password hashes can be guessed on the attacker's own machines.

Phishing

A fake page tricks you into typing it. There is no guessing at all.

- Online guessing is slowed by lockouts and limits
- Offline guessing is limited only by the attacker's hardware
- Strong secrets help most against guessing
- Unique secrets and a second factor help against the rest

Strength stops guessing. It does not stop phishing. That is why we also use unique passwords and a second factor.

Strength is a count of guesses

SECRET	STRENGTH
8 random lowercase letters	about 38 bits
16 random lowercase letters	about 75 bits
16 random letters, numbers and symbols	about 101 bits
3 random words	about 39 bits
4 random words	about 52 bits
6 random words	about 78 bits
8 random words	about 103 bits

THE RULE OF THUMB

$\text{bits} = \text{length} \times \log_2(\text{pool})$

The pool is the number of possible choices for each position: 26 letters, or a list of 7,776 words.

EVERY EXTRA BIT

doubles the number of guesses an attacker needs.

These numbers only hold for random choices. A pattern you invented, like P@ssw0rd, is much weaker than the math says.

What to watch for **in the video**

Password tab

- The length slider
- Four character sets
- The strength readout and its tier
- The bits estimate for each choice

Passphrase tab

- The word count slider
- The delimiter between words
- How the bits change with each word
- Where the tool says it runs

Predict: how many random words make a passphrase as strong as 16 random lowercase letters?

Write down a number. The video will show both.