

How Passwords Get Cracked

Guided Notes

Fill in the blanks as we go. Every answer is in the word bank.

Word bank brute-force attack · dictionary attack · rate limiting · hash · salt · offline cracking · composition rules · blocklist · passphrase · password manager

How do attackers break a password?

When attackers don't have your password, they guess it, and machines do the guessing.

Trying every possible combination until one works is a _____.

Trying the most likely passwords first, from lists of real leaked ones, is a _____.

A cap on how many wrong guesses anyone can make at the sign-in page is _____.

What does a careful site actually store?

A careful site never keeps your actual password.

A one-way scramble of a password that can't be turned back into it is a _____.

A random value added to each password before it's hashed is a _____, so two people with the same password get different hashes.

Guessing against a stolen file of hashes, with no limit on tries, is _____.

That's still guessing, so a long, uncommon password is very hard to crack.

What do the current rules say?

NIST, a U.S. government standards agency, rewrote its password rules in 2025.

Forced mixes, like a capital, a number and a symbol, are _____, and the current rules say sites shouldn't require them.

A list of passwords a site refuses because they're common or already leaked is a _____. The current rules also drop security questions, because the answers are easy to find or guess.

When a password is the only thing protecting an account, the rules say it should be at least 15 characters.

The rules also say sites shouldn't make you change a password on a schedule, only when there's a sign it leaked, so change it when a site tells you it was breached.

A site should let you use a password of 64 characters or more, so long passphrases fit.

What makes a password hard to crack?

Length does more work than symbols.

A password made of several random words is a _____.

An app that creates, stores and fills in a different strong password for every account is a _____.

Reusing a password means one leak can open every account that shares it.

REMEMBER

Attackers crack passwords by guessing, so long, uncommon passwords are the hardest to crack.