

GLOSSARY

Vocabulary

This glossary has 10 terms. Every one of them is an answer in the guided notes word bank.

How Passwords Get Cracked

Term	What it means
Brute-force attack	Trying every possible combination of characters until one works.
Dictionary attack	Trying the most likely passwords first, from lists of real leaked passwords and common words.
Rate limiting	A cap on how many wrong guesses anyone can make at a sign-in page.
Hash	A one-way scramble of a password that can't be turned back into the password.
Salt	A random value added to a password before it's hashed, so two people with the same password get different hashes.
Offline cracking	Guessing passwords against a stolen file of hashes, with no sign-in page to limit the tries.
Composition rules	Rules that force a mix of characters, like a capital, a number and a symbol.
Blocklist	A list of passwords a site refuses because they're common or already leaked.
Passphrase	A password made of several random words.
Password manager	An app that creates, stores and fills in a different strong password for every account.