One-way encryption (hashing) - What it is, why it matters, and how to use it safely

Gridinsoft Help Center

What it is

One-way encryption is the everyday name for cryptographic hashing. It turns readable data into a fixed-length digest that cannot be turned back into the original. Even if someone knows the algorithm, they cannot reverse it without guessing the original input.

Why it matters

Hashes let services store passwords safely without keeping the actual passwords. They also help verify file integrity and detect tampering. If a database leaks, strong hashing makes stolen digests hard to use.

How it works - quick tour

- You run data through a hash function and get a unique-looking digest.

- Good functions are preimage resistant: given a digest, it is impractical to find an input that makes it.

- They are collision resistant: it is impractical to find two different inputs with the same digest.

- For passwords, sites add a salt and use slow, memory-hard hashers so attackers cannot try guesses quickly.

Good uses

- Password storage: use Argon2, scrypt, bcrypt, or PBKDF2 with a unique salt per password.

- Integrity checks: verify downloads with SHA-256 digests.

- Digital signatures: hash first, then sign the hash for efficiency.

Common pitfalls

- Using fast hashes like MD5 or plain SHA-1/SHA-256 for passwords without a salt.

- Reusing salts or omitting them, which makes rainbow tables effective.

- Confusing hashing with encryption: encryption is reversible with a key, hashing is not.