A strong password is not enough: why reuse is the real risk

Generating a long random password is the easy half of the job. The half that actually gets people breached is using the same password in more than one place. Here is what makes a password strong in 2026, why reuse is the risk that matters, and how a password manager closes the gap a generator alone cannot.

Published 2026-06-30 · A Mue guide

There is a lot of advice about making a password strong: more characters, more symbols, a number and a capital. Most of it is right, and most of it solves the easy half of the problem. A generator can hand you a 16-character random string in a second. The half that actually gets people breached is quieter: using that password, or a close cousin of it, in more than one place. This is what makes a password strong in 2026, why reuse is the risk that matters, and what closes the gap that a generator on its own leaves open.

What actually makes a password strong

Strength is about how many guesses an attacker would need, and that is driven first by length, then by how many character types are in play. The standard way to measure it is entropy, in bits: each extra bit doubles the number of possible passwords. A 16-character password drawn from the full set of upper and lower case letters, digits and symbols carries more than 90 bits of entropy, which is enough that brute-forcing it is not a realistic attack.

This matches where official guidance has landed. Since its 2017 revision, US NIST guidance (SP 800-63B) has pushed length over forced complexity:

- Favour length. A low minimum is allowed, but long passwords are what actually move the needle, so aim for 16 characters or more.
- Drop the composition rules. Mandatory upper-plus-symbol-plus-digit recipes push people toward predictable patterns like Password1! rather than genuine randomness.
- Stop forcing periodic rotation. Changing a password on a fixed schedule mostly produces weak variations; change it on a real signal instead, such as a breach.
- Screen against known-breached passwords, because a password that is technically strong but already in a breach dump is worthless.

A good generator gives you all of this for free: it is random by construction, has no predictable pattern, and you can set the length as high as you like.

The real risk is not weakness, it is reuse

Here is the part the strength meter cannot see. The most common way ordinary accounts get taken over is not someone brute-forcing a strong password. It is credential stuffing: attackers

take the email-and-password pairs leaked from one breached site and replay them, automatically, against hundreds of other sites. If you used the same password on your email, your shop, and that forum that got breached two years ago, then one leak quietly unlocks all three.

The scale of available material is the problem. Have I Been Pwned, the public breach-tracking service, holds hundreds of millions of unique passwords seen in real breaches, each tied to addresses that get tried again and again. Against that backdrop, the strength of any single password barely matters if it is shared across accounts. A unique password per site is what breaks the chain: a leak from one place unlocks exactly one place.

Why a generator alone does not close the gap

So the real instruction is not just make it strong, it is make a different strong one for every account. And that is where a generator on its own runs out of road. Nobody can memorise dozens of 16-character random strings. Faced with that, people do the human thing: they reuse one good password everywhere, or they build a pattern (the same base with the site name bolted on) that an attacker who sees two of your leaked passwords can guess. Either way the uniqueness, the part that actually protects you, quietly collapses. A generator without somewhere to keep its output just moves the problem one step down the road.

What a password manager actually does

A password manager is the piece that makes per-site uniqueness practical. It generates a fresh random password when you sign up, stores it in an encrypted vault, and fills it in for you on the right site, so you never type or even see most of your passwords. You memorise exactly one thing, the master password to the vault, and that one you make a long passphrase. Most managers also warn you when a stored password turns up in a known breach, which turns the screening NIST recommends into something automatic. The free tier of a reputable manager covers this for the vast majority of people.

So use the generator below for the strong, random part, and pair it with a manager so every account gets its own. That combination, not any single clever password, is what keeps one breach from becoming five.

Frequently asked questions

How long should a password be in 2026?

Length is the single biggest lever, so aim for 16 characters or more for anything you care about. A 16-character password drawn from upper and lower case, digits and symbols carries well over 90 bits of entropy, which puts a pure brute-force guess out of practical reach. Since its 2017 revision, US NIST guidance (SP 800-63B) has emphasised length over forced complexity: it sets a low minimum but lets you go long, and longer is what actually helps. The catch is that length only protects you if the password is also unique to that one site.

Is a browser password generator safe to use?

Yes, when it runs entirely in your browser. Our generator uses the browser cryptographic random number generator (crypto.getRandomValues), the same class of randomness used for security keys, and nothing is sent to a server, logged, or stored. Reload the page and the password is gone. The thing a generator on its own cannot do is remember the password for you, which is where a password manager comes in.

Do I still need to change my passwords every few months?
No, not on a fixed schedule. Current NIST guidance dropped mandatory periodic rotation because it pushed people toward weak, predictable variations like adding a 1 or a 2 to the end. The modern advice is to use a long, unique password per site and change it only when you have a reason: a breach notification, a shared or reused password, or any sign the account was accessed. Rotation for its own sake adds friction without adding much security.

Is a free password manager good enough?
For most people, yes. Bitwarden is open source and its free tier stores an unlimited number of passwords and syncs across your devices, which covers what the vast majority of individuals need. The paid managers earn their fee on polish and extras: smoother family sharing, travel and breach-monitoring features, and tighter ecosystem integration. Start free, and upgrade only if you hit a specific need, not because the free option is somehow unsafe.

Are passphrases better than random passwords?
They serve a different purpose. A long random passphrase of several unrelated words can carry as much entropy as a shorter symbol-heavy string and is far easier to type and remember, which makes it the right choice for the one or two passwords you genuinely must memorise, above all the master password to your manager. For every other login, you do not need to remember anything, so a fully random 16-plus character string from a generator is the simpler strong default.

Generate a strong, unique password in your browser

Free, no signup: agent.mue.app/tools/password-generator

agent.mue.app/articles/a-strong-password-is-not-enough