How secure is my password manager?

Get the full interactive view at
https://bitwarden.com/ja-jp/resources/how-secure-is-my-password-
manager/

bitwarden

A password manager directly protects your digital identity by securely containing access to important accounts and sensitive information. The tool you select must have a foundation of strong encryption, trusted open development, and modern security practices.

Why password security matters

Every online account is a potential entry point for bad actors. With the growing number of services requiring authentication, and without the right tools, creating and remembering strong, unique passwords has become increasingly difficult. Password managers solve this by generating and managing secure credentials for each account.

A strong and unique password remains a key defense against unauthorized access. Using a password manager helps ensure that passwords are long, complex, randomly generated, and unique to each online account.

What makes a password manager secure?

Modern password managers rely on AES-256 encryption, a globally recognized standard also used by banks and government institutions. This level of encryption renders stored data unreadable without the proper credentials.

Trusted solutions also meet independent compliance standards such as SOC 2 and ISO 27001, which require routine audits, security controls, and ongoing assessments. These safeguards offer a clear, measurable way to answer: How secure is my password manager?

Some platforms also use internal tools to scan for weak or compromised passwords, helping users avoid common security pitfalls.

Understanding password strength

Password strength goes beyond complexity—it's about randomness. A strong and unique password typically includes:

- At least 12–14 characters or more.

- A mix of uppercase and lowercase letters, numbers, and special characters.

- No dictionary words, names, or identifiable patterns; therefore, random.

- Unique to the specific website or application, meaning it is only used once.

Avoid reusing passwords or relying on familiar combinations. Use a password strength checker to evaluate existing credentials and get guidance on where to improve.

Why open source enhances trust

Open source password managers allow independent researchers and security professionals to review the codebase continually. This transparency increases trust and ensures any potential vulnerabilities can be identified and addressed quickly.

Many open source tools offer options to process data locally, providing an extra degree of security and protection via self-hosting. For users asking "how secure is my password manager?" or "how hackable is my password?", open source platforms offer greater visibility and options into how your data is handled and protected.

Strategies that strengthen password security

Security improves when layered. These steps can significantly reduce exposure to attacks:

- **Enable two-factor authentication (2FA):** Adds a second verification step, such as a code from an app or a hardware security key.

- **Run password strength checks:** Identify reused, weak, or outdated passwords across accounts.

- **Use built-in security reports:** Prioritize password updates based on risk level.

- **Plan for account recovery:** Protect recovery methods and confirm they're up to date.

Each layer supports stronger defenses and helps answer the question: How secure is my password?

Protecting personal information

Password managers support privacy by safeguarding login credentials and keeping personal information secure. To further reduce risk:

- Avoid logging into accounts on public Wi-Fi.

- Use a VPN to encrypt internet traffic.

- Be cautious when entering sensitive data on shared or unknown devices.

- Enable 2FA on accounts whenever possible.

- Monitor activity across accounts and credit reports for unusual behavior.

Small habits go a long way in preventing unauthorized access and identity theft.

Staying ahead of online threats

Data breaches, phishing attacks, and password cracking methods like brute force are common tactics used by attackers. Secure passwords and modern password managers help defend against these threats.

Additional steps include:

- Keep software and devices up to date.

- Use 2FA across all major accounts.

- Avoid password reuse.

- Review your security settings regularly.

Combining these practices creates stronger resistance against evolving digital threats.

Quick actions to improve security

Get started with a few practical steps:

- Review password strength across your vault.

- Replace any reused or weak credentials.

- Set up and secure your account recovery options.

- Turn on two-factor authentication.

Each action builds another layer of defense.

How secure is your password manager?

The strength of a password manager depends on encryption, transparency, and layered security practices. Trusted open standards and transparent development increase confidence and reduce the risk of attack.

Password managers also serve teams and organizations by protecting shared credentials and securing sensitive business data.

Get started with Bitwarden

Strengthen your digital security with Bitwarden. Create a free account or start a 7-day trial of business plans to protect your team. Want to learn more? Join a live weekly demo and connect directly with the Bitwarden team.