1Password

Everything you need to know about 1Password's security model

A multi-layered security approach provides extraordinary protection

1Password is built differently: private by default, secure by design, and verified by experts. Every aspect of 1Password's security architecture is engineered to protect your business – even in the unlikely event of a breach.

Security isn't a feature. It’s our foundation.

1Password approaches security in a fundamentally different way than other password managers. Thanks to our unique architecture and dual-key encryption, even in the unlikely event that our systems were breached, your vault data would still be safe.

Dual-key encryption is unique to 1Password. Rather than relying on an account password alone, 1Password adds a second key, called the Secret Key, to strengthen encryption. The Secret Key is a 128-bit, random machine-generated key that is mathematically infeasible to crack.

Attackers would need both keys – **neither of which are accessible to 1Password** – to unlock your account. Without the keys to decrypt your data, if attackers were to breach our systems, any vault data they obtain would be effectively useless to them. They wouldn't be able to tell a bank login from a social media login.

Features	1Password	LastPass	Keeper	Bitwarden	Dashlane
Two-key derivation (account password + Secret Key) Instead of relying on an account password alone, 1Password uses unique dual-key encryption. Without both keys, no one can access your account – not even us.	✓	X	X	X	X
Secure Remote Password (SRP) SRP allows 1Password to authenticate your credentials without sending them over the network where they could be intercepted.	✓	X	X	X	X
Vault encryption Your data is guarded by tamper-proof protection on our servers – even in the unlikely event of a breach.	✓	✓	✓	✓	✓
URL encryption Prevent an attacker from knowing which websites you frequent, mitigating the risk of targeted phishing attempts.	✓	X	✓	✓	✓
Item title encryption Protect sensitive information within item titles so attackers wouldn't know a credit card from a cookie recipe.	✓	X	✓	✓	✓
Vault title encryption If your vault titles contain sensitive information, like your kids' names or confidential project titles, neither 1Password nor a potential attacker could read them.	✓	X	✓	✓	✓

1Password protects your data at every turn, at rest and in transit

Data you store in your 1Password vaults are **end-to-end encrypted**: not only your logins, secure notes, and payment cards, but also metadata like website URLs and vault names. Encrypting vaults in their entirety makes it much harder for potential attackers to glean any information from that metadata (such as the websites you've visited, which attackers can use in phishing attempts).

The Secure Remote Password (SRP) adds yet another layer of protection. Rather than sending your credentials over the network where they could be intercepted, 1Password uses SRP to authenticate, mitigating that risk. It also guarantees that your 1Password app is communicating with a genuine 1Password server, not an impostor trying to steal your data.

Strong security never rests

1Password also invests heavily in being good citizens of the security community. For example, we engage third-party security experts for regular audits, and we offer the industry's largest bug bounty program to help us discover and resolve vulnerabilities before they can be exploited by attackers.