

PASSWORD MANAGEMENT

Helps to secure online accounts by ensuring that passwords are strong, unique, and safely stored, reducing the risk of unauthorized access and cyberattacks.



Password Security Principles



In today's digital world, information is power. Valuable data can be worth a fortune, and the loss of such information, or even control over it, can lead to significant consequences.

Cybercriminals can exploit access to our online accounts, impersonating us, stealing our information, and even embezzling funds. This includes sensitive data stored in apps like banking and payment platforms.





A study by Business Insider revealed a startling statistic:

10,000 of the most common passwords provide access to 98% of all accounts.

This means that a vast majority of individuals reuse passwords across multiple accounts, failing to implement adequate security measures.

Meaning that even seemingly insignificant accounts can harbor sensitive information that, without proper protection, can cause immense harm.





Treat your password LIKE YOUR THOOTHBRUSH



Pick a Good One

A good password is long, complex and unique. For example:
mo9fkq@B



Don't Share it With Others

A password is personal, no one should know it



Change From Time to Time

Even the best passwords might leak due to no fault of the user, changing your password prevents you from falling victim if your password is leaked

**The problem is remembering and managing so many passwords.
Enters: Password managers.**

Let's talk Password Managers



Password managers securely store all your passwords in an encrypted database, often referred to as a vault. The manager encrypts the vault's contents and protects it with a master password that only you know.

When logging into a secure site with a password stored in your password manager, you simply enter your master password, and the manager automatically fills in the correct password for that specific site. This allows you to set strong, unique passwords for every account without the burden of memorizing them all.



Choosing the Right Password Manager



An ideal password manager should be easy to use, reliable, and compatible with all your passwords.

Browser-based password managers, like those built into Chrome and Edge, offer a convenient way to store login credentials. However, they come with several drawbacks compared to dedicated password managers, such as being a single point of failure, having fewer features and most importantly being password dependent.

However, this is a valid choice for people who only use personal devices.

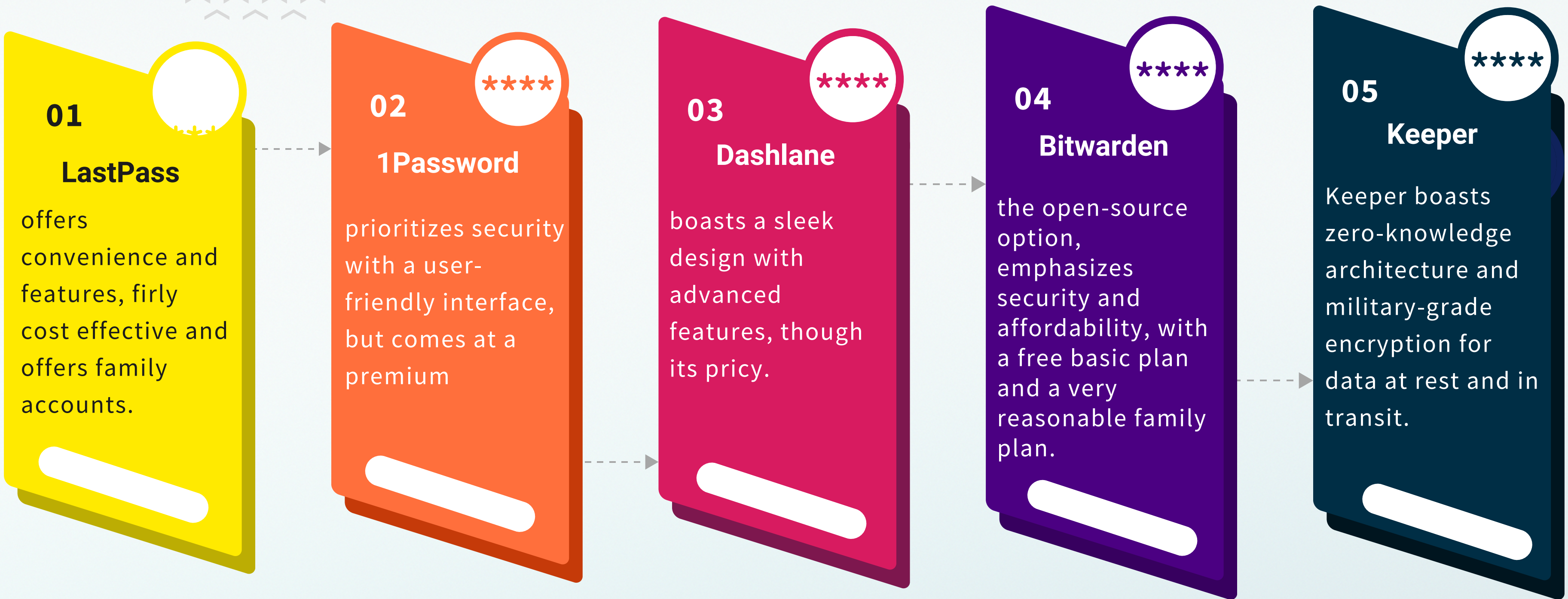


Reputable password managers employ military-grade encryption algorithms like AES 128/AES 256 to safeguard your data, even in the event of a data breach. If a software provider claims to have developed its own unique encryption solution, it's often a red flag indicating a potentially problematic service.

When selecting a manager, exercise caution with new or less-reviewed products. Cybercriminals may create fake password managers to steal your information.



Quick rundown of a few popular options:



Consider factors like ease of use, cross-platform compatibility, and desired features alongside security and cost when making your choice. Remember, the best password manager is the one that fits your budget, prioritizes security, and helps you manage your digital life effectively.





CYBER JOKE

I changed my password to
“incorrect” so whenever I forgot it
the system will tell me:

“YOUR PASSWORD IS INCORRECT”