Criteria/Brand	NordPass	Dashlane	ProtonPass	Keeper	1Password	Zoho Vault	Roboform	Bitwarden	Sticky password	Total password
Starting price (USD per month)	$1.49	$4.99	$1.99	$2.92	$2.99	$1.00	$1.99	less than $1	$19.99 for 1 year	$1.99
Active Discount Coupon. Found on the Internet	53% OFF with coupon code: **passreddit**	Extra 10% off Premium memberships Coupon code: **SCAM**	No coupon	30% OFF your first year. Coupon code: **SMART30**	No coupon	No coupon	No coupon	No coupon	No coupon	80% introductory offer, and the annual cost after a trial is $119
Free version	yes	yes	yes	no	no	yes	yes	yes	yes	no
Average score:	**4.75**	**4.25**	**4.25**	4	4	3.75	3.5	3.5	3.25	3.25
Autosave & Autofill passwords	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Autofill personal data	yes	yes	yes	yes	yes	no	yes	yes	yes	no
Supports Passkeys	yes	yes	yes	yes	yes	yes	yes	yes	no	no
Data breach alert	yes	yes	yes	yes	yes	yes	yes	no	yes	yes
Email Masking feature	yes	no	yes	no	no	no	no	yes	no	no
Secure Notes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Multi-factor Authentication (MFA)	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Secure Credit Card	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Password generator	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Easy organization	yes	yes	yes	no	yes	yes	yes	yes	no	no
Attach files to items	yes	yes	no	yes	yes	yes	yes	yes	no	no
Biometrics	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Password health check	yes	yes	yes	no	yes	yes	yes	yes	yes	no
Devices	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Compatible for all devices	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Browser extension	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Password sync across all devices	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Password sharing (passkeys)	yes	yes	yes	yes	yes	yes	yes	yes	yes	no
Offline access	yes	yes	no	yes	yes	yes	yes	yes	no	no
Mobile access	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Desktop apps	yes	yes	yes	yes	yes	yes	yes	yes	yes	no
Emergency access	yes	no	no	yes	no	yes	yes	yes	yes	no
No storage limits	yes	no	yes	yes	no	yes	yes	yes	yes	yes
Family Plan (members)	6 members	10 members	no	5 members	5 members	min 5 members	5 members	6 members	no	no
Premium trial	30 days	14 days	yes	14 days	14 days	15 days	30 days	7 days	no	no
Subscription includes VPN	no	yes	yes	no	no	no	no	no	no	no
Options for businesses	yes	yes	yes	yes	yes	yes	yes	yes	yes	no
Money-back guarantee	yes	yes	yes	no	no	yes	yes	yes	yes	yes
24/7 support	yes	yes	yes	yes	yes	yes	yes	yes	no	yes
Encryption type	XChaCha20	Ad- vanced Encryption Standard (AES) 256-bit	256-bit AES-GCM	AES 256-Bit Encryption	AES-GCM-256	AES-256 encryption	AES-256 encryption	end-to-end AES-256 bit encryption, salted hashing, and PBKDF2 SHA-256	AES-256 encryption	AES-256 encryption

Criteria meaning:	
Autosave & Autofill passwords	Function that offers to save your credentials once you type them in and autofill them on different websites where login is required.
Autofill personal data	Software feature that automatically inserts previously entered personal information into web form fields (it includes name, email address, phone number, and work or home address).
Supports Passkeys	A passkey is a digital credential that is used as an authentication method for a website or application.
Data breach alert	Alert notifies if your passwords or credit card details have ever been leaked.
Email Masking feature	A feature allowing to create an email address that can be used to sign up for online services without revealing your true identity.
Secure Notes	You can store different notes, wifi passwords and other information together with your passwords.
Multi-factor Authentication (MFA)	Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource.
Secure Credit Card	You can securely store your credit cards and fill in their details on the go when shopping online.
Password generator	Service provides software that creates random passwords for its users.
Easy organization	You can organize your information on different folders.
Attach files to items	Service lets you securely add most important files to saved passwords, secure notes, personal info or credit cards.
Biometrics	Service use biological measurements or physical characteristics that can be used to identify individuals (example: Fingerprint or Face ID).
Password health check	Service scans all passwords stored in your vault and checks how vulnerable they are.
Devices	Service can be used with unlimited devices of your choice.
Compatible for all devices	Available for all devices including macOS, Windows, Linux and etc.
Browser extension	Service is available to add to your core browser.
Password sync across all devices	You can stay logged in on an unlimited number of devices.
Password sharing	You can share your passwords with other people.
Offline access	Service is available even when you aren't connected to your network and don't have access to the Internet.
Mobile access	Service has a mobile app and can be used on iOS and Android devices.
Desktop apps	Service has a desktop app for more convenient use.
Emergency access	Service provides one-time access to your vault to another user in the event of an emergency or crisis.
No storage limits	Service lets you store as many information as you want with no limits.
Family Plan (members)	The service allows to add addtional members to stora and share password data.
Premium trial	The amount of days that free trial is available for premium accounts.
Money-back guarantee	X days guarantee that, if a buyer is not satisfied with service, a refund will be made.

24/7 support	Service is providing support 24 hours a day, and 7 days a week.

Privacy Features/ Score (0-5)	NordPass	Dashlane	ProtonPass	Keeper	1Password	Zoho Vault	Roboform	Bitwarden	Sticky password	Total password
Multi-factor Authentication (MFA)	5	3	4	3	3	5	3	5	3	3
Biometrics	4	4	3	4	5	3	5	4	4	3
Data breach alert	5	5	5	4	4	4	3	0	3	4
Encryption	5	5	5	5	4	3	3	5	3	3
Average score:	4.75	4.25	4.25	4	4	3.75	3.5	3.5	3.25	3.25

Privacy Features - How scores are given for each criteria (0-5)	
Multi-factor Authentication (MFA)	5 - if the service is using more than two authentication factors. 3 - if service is using 2FA. 0 - if service doesn't have authentication factors.
Biometrics	5 - if the service has 3 or more biometrics (Facial recognition, Fingerprint scanning, Iris and Intelligent scan). 4 - if service has at least 2 biometrics. 3- if service has at least 1 biometrics. 0 - if service doesn't have any of them.
Data breach alert	5 - if service automatically scans leaded databases, looks into possible breaches for not only passwords on all browsers but also email addresses or credit cards and notifies you immediately if that happens. 4- if service automatically scans leaded databases, looks into possible breaches for passwords/emails on all browsers, but nothing is mentioned about other information safety (example: credit cards). 3- if service automatically scans leaded databases, looks into possible breaches for passwords/emails, but nothing is mentioned about other information safety. Moreover, not all browsers have this function. 0- going to those, who don't have this feature at all.
Encryption	5 - if service uses secure and up-to-date encryption algorithms. 4-3- If service uses standard encryption with additional safety features. 0 - if service uses encryption with weak and outdated standards.