

PASSWORDS

Password: “password”

The top 10 most common passwords:

- 123456.
- 123456789.
- qwerty.
- password.
- 111111.
- 12345678.
- abc123.
- 1234567.

What level of protection?

- Financial information (e.g. bank accounts)
- Device access (e.g. computer, smartphone)
- System access (e.g. WiFi)
- Identity information (risk of theft/fraud)
- Online shopping
- Subscription services
- Others?

Password considerations

- Complexity
 - Number and type of characters
- Re-use
 - Same password in multiple systems?
- Memory aids / hints
 - Write them in a notebook?
- Change them frequently?
- Provision for death or incapacity

Password tricks

- Initial letters of a memorable phrase
- Substitute figures for letters
- Insert special characters (if allowed)
- Depend on system features
 - e.g. multi-factor authentication
 - lock-out after three wrong attempts
 - forgotten password procedure
- Read Wikipedia on “Passwords”

Password managers



Our everyday tasks are increasingly being done online. That usually means having multiple accounts for various services, with lots of different passwords to manage.

We often cope by choosing weak, easy-to-remember passwords or by re-using the same favourite ones across lots of websites. That's not secure, as criminals can guess your passwords, or plunder them via [phishing attacks](#).

Password managers are marketed as the convenient, secure solution to these problems. Packages differ in terms of the features they offer, but they may:



- Securely store all your passwords for different accounts.
- Remember one password to access all websites and services.
- Share passwords and data with trusted friends and family.
- Securely store sensitive documents, such as your passport.

Password managers

Keeper	Bitwarden	Dashlane	Enpass
Intuitive Password	Kaspersky Password Manager	LastPass	1Password
Myki	Norton Password Manager	Pass	Pleasant Password Server
Avoid: KeePass			

Which? Recommends ...

Best free password managers

Name	Ease of use - desktop	Ease of use - mobile	Security	Score
	★★★★★	★★★★★	★★★★★	71%
<p>Name: LastPass</p> <p>LastPass is a secure vault for your passwords and private data. You can download it for free on your PC or Mac, Android or Apple iOS mobile device. You create an account with an email address and then set a strong master password – the only one you’ll need to remember. You can store unlimited passwords, either ones you’ve chosen or passwords created by the generator. LastPass works with all major web browsers. It detects when you want to log into one of your accounts and handles most log-in processes effectively. Although, it can struggle with ‘captchas’ and multi-page log-ins, such as Google. There’s online help if you get stuck, but it can’t be searched so be prepared to hunt for the answer you need. The security audit feature warns you about potentially weak passwords and checks your data against known breaches. All your password data is stored locally on your device to increase security. If you forget your master password, you can set a reminder hint or recover the account with a designated phone.</p>				
	★★★★★	★★★★★	★★★★★	70%
<p>Name: Dashlane</p> <p>Just like LastPass, you create a Dashlane account and set a master password, again stored locally on your device to increase security. You can use your own passwords or Dashlane can generate ones for you. With the free package, you’re limited to storing just 50. That should be enough for most people’s needs, but does put it behind LastPass Free. When accessing a webpage, Dashlane shows a list of your saved accounts and you click on the one you want to use. It works well, but sometimes struggles with captchas and multi-page log-ins. Dashlane automatically fills in stored personal information into online forms, but sometimes doesn’t detect the right field (the same feature is available on LastPass with the same limitation). We found Dashlane works well with Chrome and Internet Explorer, but not so well with Safari and Firefox (possibly due to recent changes to the browser). A security audit feature provides information on security breaches of websites you use and warns when you have weak passwords. Help is only available online, and, although useful, it’s hard to navigate.</p>				



Should I pay for a password manager?



You can also pay to upgrade to a premium package, but what do you get with paid password managers, and is it worth the extra cost?

Premium password managers tend to offer a range of extra features, so it's worth considering which you'll find useful before you decide.

- **Password sharing:** This is the primary draw of premium password managers. It enables you to share passwords and other data securely with family and trusted contacts. You can also often grant emergency access to your accounts if the need arises.
- **Unlimited password storage:** Some free password managers enable you to store unlimited passwords, but not all do. You're almost guaranteed this with a paid-for package.
- **Secure storage:** You can often store sensitive or private data in your password manager vault, such as a scan of your passport, to access when you need it. Some password managers offer 1GB or more storage on the paid package.
- **Multi-factor authentication:** With premium services, you can usually use additional multi-factor security, such as the physical Yubikey USB device or the Google Authenticator two-factor authentication (2FA) service.

Premium password managers

Name	Ease of use - desktop	Ease of use - mobile	Security	Score
	★★★★★	★★★★★	★★★★★	76%
	<p>Name: LastPass Premium Price: £18 per year / LastPass Family £36 per year You would go for LastPass Premium over LastPass Free if you want to share passwords and accounts securely with family or friends. For example, if you want to give your wi-fi password to your son or daughter, LastPass lets you do this securely. You can only share one password at a time, but if you upgrade to the family subscription, you can have another five people registered on your account, with shared folders you can all access. You can create a 'digital contingency plan' that gives emergency access (by default at 48 hours) to your data to family or friends in case you're unable to access them yourself. Alongside passwords, you can also save files securely, such as a scan of your passport, and share the data with other users. You get 1GB of storage in the premium version (secure storage is also available in the free account but you only get 50MB). With premium, you can also use extra multi-factor security, such as the physical Yubikey USB device or the Google Authenticator 2FA service.</p>			
	★★★★★	★★★★★	★★★★★	74%
	<p>Name: Dashlane Premium Price: €39.99 (£28.65) per year You have to sign up to a year's contract with Dashlane Premium and it's automatically set to renew unless you cancel it. Plus, Dashlane bugs you to buy premium subscriptions for friends and family as gifts. After that, you get the same core service as Dashlane free, but can store unlimited passwords in your vault. You can also sync your Dashlane account to various devices, including smartphones and tablets, to use wherever you go. You can store important information, such as passport details, securely in your Dashlane vault. Just like LastPass Premium, the service enables you to share passwords and notes securely with trusted contacts. Either grant them limited access or full rights to stored data (either way, they must be Dashlane users, too). You also get a virtual private network (VPN), essentially a secure internet connection to use while on often dicey public wi-fi. Alongside the core security audit, Dashlane monitors the 'dark web' and alerts you if any of your account details have been compromised. It supports security keys, such as Yubikey, and mobile 2FA services, such as Google Authenticator.</p>			

	★★★★★	★★★★★	★★★★★	64%
	<p>Name: 1Password Price: £33 per year As with all password managers, you create a master password for your 1Password database, and that's the only one you'll need to remember. The year-long contract is pricier than LastPass Premium, and will auto-renew if you don't cancel it. An unlimited number of passwords can be stored. On Android and iOS, the password generator can only be used when setting up a new entry. So, you would have to create an entry for Facebook in the database, get the password, and then set up your Facebook account, rather than 1Password doing this automatically. 1Password struggles with multi-page logins and captchas, but its automatic form filler works well. The online help is good for basic tasks, but needs to be more contextual and searchable. When you're travelling, you can activate 'travel mode' to remove any sensitive data from the vault in case your device is lost or stolen.</p>			
	★★★★★	★★★★★	★★★★★	64%
	<p>Name: Kaspersky Password Manager Price: £10.49 per year Antivirus software brand Kaspersky's password manager is also an encrypted vault safeguarded by a master password. Alongside unlimited passwords, you can securely store documents, such as passport scans. It's cheap compared with rival services and the annual contract doesn't automatically renew. It's easy to set up and there's a useful wizard that imports already-saved passwords from your browser. It makes you sign up for a Kaspersky account before you create your vault, and it's needlessly confusing to juggle that and the vault's master password. The password generator is good and automatically inputs into websites. Kaspersky offers detailed and easily searchable help and advice. However, the auto form filler is poor, you're better off just doing copy and paste, and the system isn't great to use on iOS and Android devices.</p>			

Audience participation

Questions

Password experience

Recommended managers