Passwords: Choosing, using, storing and maintaining

What makes a good password?

A good password should, where possible (some sites restrict these options) be:

12 or more characters; with upper and lower case, numbers and symbols (where allowed).

Unambiguous Unusual Memorable Different to all your other passwords.

Are your passwords secure?

The most commonly used passwords (UK 2025) in order of frequency are:

Admin..123456 password 12345678 123456789 Password1 Password 12345 Lennon11 1234567890

Password123 Fortnite21 password1 qwerty123 qwerty 123qwe abc123 Strongman12 daday123

If you use passwords like this they are easy to crack. Password cracking mostly uses a "dictionary" based on passwords used around the world (and selected for your language). "Text-speak" or substituting numbers is s0 c0mm0n now that it's no benefit. Hackers may also use information collected about you from the public domain e.g. your facebook page - so don't use a family members (or pets) name, address, age or date!

Use a common strategy

One strategy often recommended is to use the first letter of words from a favourite poem or text.
ItbwtW, Iwlaac – can you guess them – would they be secure? (0.5 second to crack)

(clues – Genesis Wordsworth)

The more complex a password is – the more "entropy" it has – the more secure it will be.
Here is a good password: L8n-G3c?R4m,S3h (34 billion years)
It's not very memorable – would you write it down – or store it in a text file on your PC? So ..

Work out a strategy of your own for low security logins

– eg take a single short "seed" word "shed" , add letters (two) from the site (e.g. fa for facebook) a couple of numbers you will remember, and (if allowed) a symbol. Capitalise a couple and you get **sHEd19£fa**. Would you worry if it was going to take a powerful computer 3 weeks to crack your facebook password?
(**or sHEd19£ya for yahoo?) But update them with a new "seed" & symbol occasionally – eg bANk19$ya.**

How to create secure passwords that meet the above criteria

One good strategy to create a memorable password is to take two or three words that DONT go together -

E.g. focus tree;

focustree (2 minutes) now add numbers that have some significance to you (but NOT a birthdate etc)
focus17tree (1 month) - and add capitals (I've chosen to always use the second letter – first is too obvious)
fOcus17tRee (41 years)– and finally a symbol SOMEWHERE (here after the capital).
fO£cus17tR£ee (3 million years) *Password cracking time estimates from https://howsecureismypassword.net/*

All you need to remember is the two words, and the number, because everything else stays the same. You can use the "funny image" trick to help remember the words. For another password you use the same process but with different words fL£an42cA£stle (204m years) Using dictionary words reduces the "entropy" because a dictionary attack will find them. However splitting the words with symbols overcomes that objection (for now).

The "four words" password strategy once advocated (example: correct horse battery staple) fails because it reduces to 4 quick "dictionary searches".

Levels of security

When you have a LOT of logins to remember passwords for it becomes unmanageable. We need to reduce the level of complexity, and **my first step is to divide logins into three different security levels**.

1: Logins to financials – bank, PayPal, eBay, etc. need highest security; a unique, very secure password for each.

2: Logins to personal stuff – email, facebook, cloud storage such as Google drive etc. need good security.

3: Unimportant logins can share a small range of simple passwords from your strategy above as above – depending on the requirements of the site. But please don't just use your name, date of birth, etc. – That's ALL in the public domain.

Also don't use your "memorable information" that the important sites use to confirm your identity.

It's still too much to remember

Well, you should be able to remember the level 3 passwords – in their simple variations. However you need some way of storing them all – especially more complex passwords - securely. Write them down and stick them on the side of your monitor? Perhaps not. However it is reasonably safe to store them in a file on your computer, provided that the way they are stored is secure. Here are three ways to achieve this.

1: DONT let your browser store passwords: Unfortunately anyone who can log in to your computer can access all of them. Simple and very convenient. Be aware that the login password to your pc can be breached reasonably easily and quickly by anyone with access to it and sufficient skill.

Some browsers (eg Firefox) allow you to enter a master password before they will allow use of the stored passwords. The encryption used is known to be not very secure. For most domestic purposes (level 2 or 3 security logins) its fine. However as your browser is your point of contact with the web, it's also a common target for hackers, so perhaps not the best place to save more important passwords.

2: Create your passwords in a document and copy/paste to use them. The document needs to be secured by a complex master password and encrypted securely**. This is the system I use myself**. For example Libre Office Writer allows password protection of a document and very secure AES256 encryption as used by governments etc. You can store multiple copies of the file to prevent its loss, even give them away; only someone who has access to the master password would be able to use it. It goes without saying (I hope) that if you lose THAT password you will have REAL problems. And if you keep it written down you need to be VERY careful.

3: Use a password manager. KeePass is FREE, open source, available for many different platforms (PC, Apple, Android etc. and very secure. It will generate secure passwords for you, remember them, and apply them to a site login. It's not as convenient as the browser password manager, but by far the most secure way to store your passwords. Just don't forget the master password.

What happens if the device you have this program (and the password database) installed on breaks? Or if you are using a different device - a tablet or phone? I'm not happy with this system.

Maintaining passwords

You should consider changing your password strategy – especially if you have any concerns about a password breach. If your facebook login was compromised (**sHEd19£fa)** how long would it take AI to work out a password for yahoo? The "seed" strategy makes maintaining your passwords easy.

Important Logins (such as financials)

These should not rely on a single authentication, and ideally should not rely solely on characters typed in on your keyboard. Why not? because a keylogger virus would capture all your login information!

Here are some examples of strategies commonly used.

Lloyds Bank – user code (8ch), password (10ch), memorable (3 ch from 10 via drop down)

Santander – Personal Id (confirmed with chosen image and text) if the website does not respond with the correct image do not proceed! THEN passcode (8 ch) and registration number (5 digits)

Binance (cryptocurrency exchange) – previously confirmed email address, long password (upper and lower case, numbers and symbols); Two factor authentication (2fa) via one-time passcode sent to phone.

Often if the site does not recognise the device you are using, a further authentication (2fa) will be required.

Two factor authentication (2fa)

For high levels of security an online log-on via a pc, tablet etc is not sufficient. A common strategy is for the login to require a one-time passcode sent as a text to your phone, which you then enter on the PC. Another example of 2fa is the chip & pin system used on credit cards.

Authenticator app

Some sites support the use of an "authenticator app" that resides on your device (pc, phone etc.). The app generates a short lived "one time passcode" you enter on the sites screen.

Further authentication (only if you REALLY need high security)

USB keys

Makers such as Yubi sell keys that plug in to a usb port to provide a second level of security for your data.

Biometric security

Many phones and laptops offer fingerprint, face or voice recognition for security. You can buy a USB fingerprint reader for a pc or laptop for around £20.

What if it breaks?

I would not be happy relying on a single device to allow access to my online activities. I have several copies of my password file on different devices, and including my google drive, so I can access my online services from any of them – and if one breaks, or I can't access it, I'll use another with no issues.

You WILL need to use the program with which they were created; that's why I use Libre Office, its free and runs on any PC, even as a "portable application" which does not need installing. AndrOpenOffice which runs on android tablets can also open these files (with the password)

This has proved invaluable when I have needed to perform transactions or access personal data while on holiday.

Unambiguous username, password, memorables

To log on to a site (eg internet banking) you will usually need your

Username password and memorable information.

All of these need to be EXACTLY right. So to make life easy

DON'T CAPITALIZE. DON'T PUNCTUATE.

if your password is bradford Bradford is WRONG.
So is bradford, brad ford bradf0rd bradf0rd. bradford. Can you see why?

What is the right password here? brAdford23; *see below

DON'T USE CHARACTERS YOU CAN CONFUSE. I l ! | L 1 o O 0

What symbols are allowed?

It depends on the site. Most commonly allowed symbols are

! @ # $ Generally all the ones above your number keys ! " £ $ % ^ & * ( )

But NOT | \ / > < because they can be used to hack into email systems.

Username:

where possible always use the same one e.g. jennyagutter avoid spaces

sometimes your username will be your email address.

Passwords

most sites require you to use a password that has at least three of the following:

- CAPITALS: don't capitalize, never put the capital at the start of the word.
- miniscules: (i.e lower case) use these as much as you can
- numbers: keep them together
- symbols: use the same one(s) , in consistent place/s. Not at the end.
  e.g. bradFord%52

Recovery

Sites always have a process to recover your account if you enter the wrong details.
Often it uses your email address and phone number. So they need to be exactly right.

your email address is ALWAYS lower case (no capitals); sometimes it will have a dot

e.g. jennyagutter@bbc.co.uk or jenny.agutter@bbc.co.uk

*** brAdford23; yes, the semicolon was supposed to be part of the password. But its confusing. if you use brAdford%23 or brAdford!23 you won't get it wrong.