

SHARE THIS AROUND

Choosing and using passwords

Most advice about passwords is out of date. The rules that actually matter are simpler than you have probably been told, and there are fewer of them.

WEAK, DESPITE LOOKING CLEVER

P@ssw0rd1!

Short, and the substitutions are the first thing any attacking tool tries. Broken in seconds.

STRONG, AND EASIER TO TYPE

otter-cinema-rope

Three unrelated words. Long enough to be impractical to crack, and you will remember it.

SIX RULES THAT MATTER

01

Length beats complexity

Three or four unrelated words is stronger than a short password full of symbols. If you must add a number or symbol, add it to something already long.

02

Never use the same one twice

This is the most important rule on the page. When any website is breached, attackers try those details everywhere else. Reuse is how one leak becomes five compromised accounts.

03

Your work password is only for work

Never on a shopping site, a forum or a personal service. You cannot control how well those protect it.

04

Nothing guessable about you

Pet names, children, birthdays, the football team on your desk mug, the company name plus a year. All of it is public, or nearly.

05

Never share one – ever

Not by email, not on a note, not “just while I’m off”. If someone needs access, they need their own. Shared passwords also mean nobody can prove who did what.

06

Change it when there is a reason, not on a schedule

Forced monthly changes just produce Summer2026 then Autumn2026, which is worse. Change it if it may have been exposed, if you have reused it, or if you are asked to.

Use a password manager

Nobody can remember thirty different long passwords, and nobody should try. A password manager stores them all behind one strong password that you do remember – and fills them in for you, which is quicker than typing.

It also spots fakes

A manager will not offer to fill in your details on a lookalike site, because the address does not match. That alone catches many phishing pages.

And it shares properly

Where a genuinely shared account exists, a manager shares access without anyone knowing or emailing the password.

WHAT NOT TO USE INSTEAD

A notebook in a drawer

The browser's built-in saving on a shared PC

Emailing them to yourself

A spreadsheet called passwords

A note on your phone

The same password with a different number

If a password may be exposed

1. Change it now, and change it anywhere else you have used it.
2. Tell whoever handles your IT, even if you are not certain. Nobody minds a false alarm.
3. Approve no sign-in prompts you did not start yourself.
4. Watch for unusual emails in your sent items or unexpected replies.

One last thing. A password on its own is never enough. Multi-factor authentication is what protects an account when a password does get out – and it is the reason a stolen password often causes no harm at all.

FILL THIS IN BEFORE SHARING

OUR PASSWORD MANAGER IS

REPORT CONCERNS TO