

Scams & online safety | Easy | 2 min read

How to create a strong password

A strong password is long, unique and hard to guess. It protects your accounts better than short passwords with clever symbols, and it is easier to remember than you might think.

What makes a password strong

- **Length:** aim for at least 12 characters. Longer is better.
- **Unique:** use a different password for every important account. If one site is breached, the others stay safe.
- **Not personal:** avoid names, birthdays, pets, football teams and anything on social media.
- **Not common:** avoid "password", "123456" and keyboard patterns like "qwerty".

An easy method

1. Pick three or four random words, such as "teapot river candle ladder".
2. Join them together, and add a number or symbol if the site asks for one.
3. Make sure it is not a phrase from a song or well-known saying.
4. Use this for your main email, and a different one elsewhere.

Keep passwords safe

- Use a password manager. Many phones and browsers have a built-in one, and they can make and remember passwords for you.
- If you write passwords down, keep the paper somewhere safe at home, not near the computer, and do not label it.
- Never share a password, including by email or text, even with someone who claims to be from your bank or from support.
- Turn on two-step sign-in so a stolen password is not enough.

Changing passwords

Only change a password through the official website or app, never via a link in an email or text. Change it at once if a site tells you it has been breached, if you used it on more than one site, or if you shared it.

When to get more help

Stop and ask for help if you are locked out, you cannot remember your main email password, you think someone has seen your password, or you are not sure how to set up a password manager. Do not reuse your old password. Tell us which accounts are affected.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.