How secure is your password?

Your step-by-step guide to creating strong passwords

Passwords are still one of your first and most important lines of defence. But all too often, they're also the weakest. Whether you're building a policy from scratch or reviewing what you already have, our simple 10-step password policy toolkit can help you and your team create safer habits and reduce the risk of breaches.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

1

One password. One account

The golden rule–never reuse a password. It only takes one breach to open the door to every other system using the same login.

Action

- Create a different password for every account–especially for systems that hold sensitive business or customer data.
- Never use the same password for work and personal accounts.
- Avoid shared passwords for team logins where possible. Use access tools or role-based permissions instead.
- Start changing any old, reused passwords now.

2

Set clear standards for what 'strong' means

Don't assume your team knows what a good password looks like. Be specific.

Action

At a minimum, each password should include:

- 12 to 16 characters (or more).
- A mix of upper and lower case letters, numbers, and special characters.
- No names, guessable words, dates or patterns (including things like 'qwerty' or 'letmein').
- No personal links—birthdays, pet names, favourite bands or sports teams.
- No company-related terms like 'admin2024' or 'companyname123'.
- Use a reputable password manager.

And if anyone's asking, 'is my password strong?' – the answer's probably no.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

3

Embrace the 3-word rule

Three random words can create a password that's almost impossible to guess, like Dog-Coffee-Banana or CupFuzzyWorld

Action

- Make sure they're meaningful for the user so they'll also be memorable.
- Add a number or symbol to ramp up the difficulty for hackers.
- Don't fall into common traps:
  - o No famous phrases or quotes.
  - o No personal connections (e.g. DogName-Breed-Birthday).
  - o Avoid linked or themed words like 'BlueSkyThinking' or 'FastRedCar'.

4

Use password managers

A password manager is a secure tool that creates, stores, and fills in strong, unique passwords so you don't have to remember them all.

Action

At a minimum, each password should include:

- Choose a reliable password manager for your business and make sure everyone on your team knows how to use it.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

5

Use 2FA

Two-factor authentication (2FA) adds another layer of protection, and it's one of the easiest ways to boost your defences.

Action

- Make it mandatory for:
  - o Email accounts.
  - o Finance, HR, and payroll systems.
  - o Admin or superuser logins.
  - o Any platform storing sensitive customer or business data.
  - o Use authenticator apps over SMS wherever possible as. they're harder to intercept.

6

Train your team to spot password scams

Even the strongest password can be stolen through a well-crafted phishing email.

Action

- Include key info, such as:
  - o No one should ever share a password, even if asked by 'IT'–unless you've specifically reported a problem and know who you're talking to.
  - o How to check URLs and sender addresses before clicking links.
  - o How to look for warning signs like bad grammar, generic greetings, urgent demands, or strange sender addresses.
  - o Encourage a culture of asking—not assuming—when something looks off.
  - o Report anything suspicious immediately.
- Run controlled phishing tests to help your team get better at spotting scams.
- Check out our piece on free cybersecurity courses.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

7

Know what to do if a password is compromised

We're all human. If someone makes a mistake, quick action makes all the difference.

Action

If you suspect a breach:

- Change the affected password immediately.
- Review any accounts where it was reused (ideally none).
- Check for unauthorised access or changes.
- Report it to your IT lead or security contact.
- Let affected users, clients, or partners know, if necessary.
- Watch for any unusual activity on your accounts.
- Make sure you have a clear action plan for dealing with security incidents.

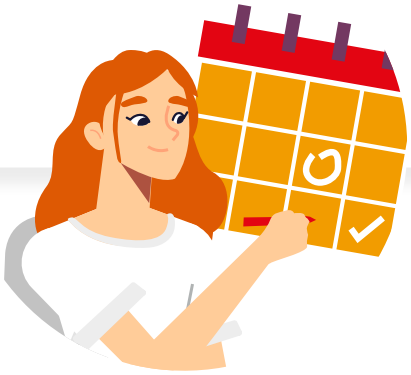
8

Review and rotate passwords regularly

Password reviews should be part of your regular cyber check-ups.

Action

- Review every six months or annually or after:
  - o Team members leave.
  - o Tools or platforms are retired.
  - o Access levels change through promotions or department switches.



Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

9

Set your expectations in writing

A clear, no-nonsense password policy helps everyone understand what's expected - and what's at risk if it's ignored.

Action

- Include key points, such as:
  - o Your minimum password requirements.
  - o Use of password managers.
  - o Required use of 2FA.
  - o Rules around password sharing.
  - o What to do in case of a breach.
  - o Where to go for help or training.
- Make sure everyone knows where to find it – quickly and easily.
- Align it to any other company policies like remote working or 'Bring your own device to work'.

10

Lead by example

Leadership sets the tone. If senior staff cut corners, others will follow. Strong passwords aren't IT's problem. They're everyone's responsibility.

Action

- Make it part and parcel of your workplace culture.
- Include password training in onboarding.
- Share updates or reminders in team comms.
- Avoid public shaming. Correct mistakes privately and reward good behaviour.
- Make security something you do–not something you dread.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business

Good password habits are a vital part of your overall cyber security. By following these practical steps, you'll help your team build a strong defence against cyber threats.

Want to make your digital world more secure?

Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone business