

WHY PASSWORDS MATTER

Your passwords protect almost everything you do online, from your email and online banking to your shopping accounts and photos. If a criminal gets hold of one, they can often use it to get into your other accounts, read your emails or reset your other passwords, and in some cases take money from you.

Most accounts aren't broken into by someone cleverly guessing a password. Criminals use computer programs that try millions of common passwords and patterns every second, and they use passwords stolen from one website to try to log in to others. A good password is one these programs can't work out, and that you only use in one place.

WHAT MAKES A PASSWORD STRONG?

- **It's long.** Length matters more than anything else. Three random words, such as Orange-Tractor-Pencil, are far harder to crack than a short jumble of characters.
- **It's unpredictable.** It avoids names, birthdays, pets, football teams, favourite places and anything else that could be found on social media.
- **It's only used once.** Every account should have its own password, so that if one website is hacked, your other accounts stay safe.

HOW TO USE THIS GUIDE

On the next page you'll find six made-up example passwords. Pick the one that's most like the passwords you use, then turn to page 3 to see how strong each example is and what to do next. Page 4 explains the safest places to keep your passwords.

PLEASE KEEP YOUR PASSWORDS PRIVATE

This guide uses made-up examples only. Please don't write your real passwords on it, and never share them with anyone, including us.

WHICH IS YOURS MOST LIKE?

These are made-up examples. Never share your real password with anyone. Pick the one most like yours, then see page 3 to find out how strong it is.

A

Rover1962

A name and a year

B

Orange-Tractor-Pencil

Three random words

C

Summer2024!

A word, a year and a symbol

D

Tq8#mVz2!pRk

Made up by a computer or password manager

E

Bluebell1 Bluebell2 Bluebell3

The same password with a number changed for each account

F

qwerty123

Simple and quick to type

HOW STRONG ARE THESE PASSWORDS?

A Rover1962 **WEAK**

Names and years are easy to guess, and are often on social media.

B Orange-Tractor-Pencil **STRONG**

Three random words, as recommended by the National Cyber Security Centre. Strong as long as it's only used for one account.

C Summer2024! **WEAK**

It has a capital letter, a number and a symbol, but it's one of the first patterns criminals try.

D Tq8#mVz2!pRk **VERY STRONG**

Impossible to guess, but also impossible to remember, so it needs keeping safely in a password manager or a well-organised password book.

E Bluebell1, 2, 3 **WEAK**

This counts as using the same password everywhere. If one account is leaked, criminals try the obvious changes on your other accounts.

F qwerty123 **VERY WEAK**

One of the most common passwords in the world. It can be guessed almost instantly.

Any password is weak if it's used on more than one account.

WHAT TO DO NEXT

1. Use a different password for every account. Start with your email, because it can be used to reset your other passwords.
2. Make strong passwords for free with our Password Creator at rothervalleyit.com/password-creator. Choose random words like B, or letters, numbers and symbols like D.
3. Keep them somewhere safe. Page 4 shows your options, from strongest to weakest.

WHERE TO KEEP YOUR PASSWORDS

Your options, from strongest to weakest.

1

STRONGEST

A reputable password manager, such as Bitwarden

Benefits: It remembers a different strong password for every account and fills them in for you. It works on your computer, phone and tablet, and Bitwarden has a free version.

Drawbacks: It takes a little time to set up. Everything is protected by one master password, so make it strong and don't lose it, because Bitwarden can't reset it for you.

2

GOOD

Your web browser's built-in password manager

Benefits: Already there and free in Google Chrome, Microsoft Edge and Apple Passwords on iPhone, iPad and Mac. It saves and fills in passwords, and most will warn you if one has been leaked.

Drawbacks: It works best when all your devices use the same company. Anyone who gets into your computer, or your Google, Apple or Microsoft account, could see your passwords.

3

OK

A password book kept safely at home

Benefits: Simple, no technology needed, and it can't be hacked over the internet.

Drawbacks: It can be lost, stolen or damaged, it isn't with you when you're out, and it needs updating by hand. Keep it out of sight, not next to the computer.

X

WEAKEST

Avoid: Sticky notes on or near the screen, a file called "passwords" on your computer or phone, emailing passwords to yourself, or using one password for everything.

EXTRA PROTECTION

Turn on two-step verification for your email, bank and password manager. A code is sent to your phone when you sign in, so a password alone isn't enough.