



SAFE PASSWORDS





# SAFE PASSWORDS

Why we need passwords

Common password mistakes

Creating good passwords

Remembering passwords



# WHY WE NEED PASSWORDS

# What they do for us

- To protect information such as your address, date of birth, credit card details
- To be able to safely navigate and engage with the online world
- To protect others



# What could happen?

- Your email could be accessed
- They could open your social media accounts and make posts under your name
- They could buy goods online with your account

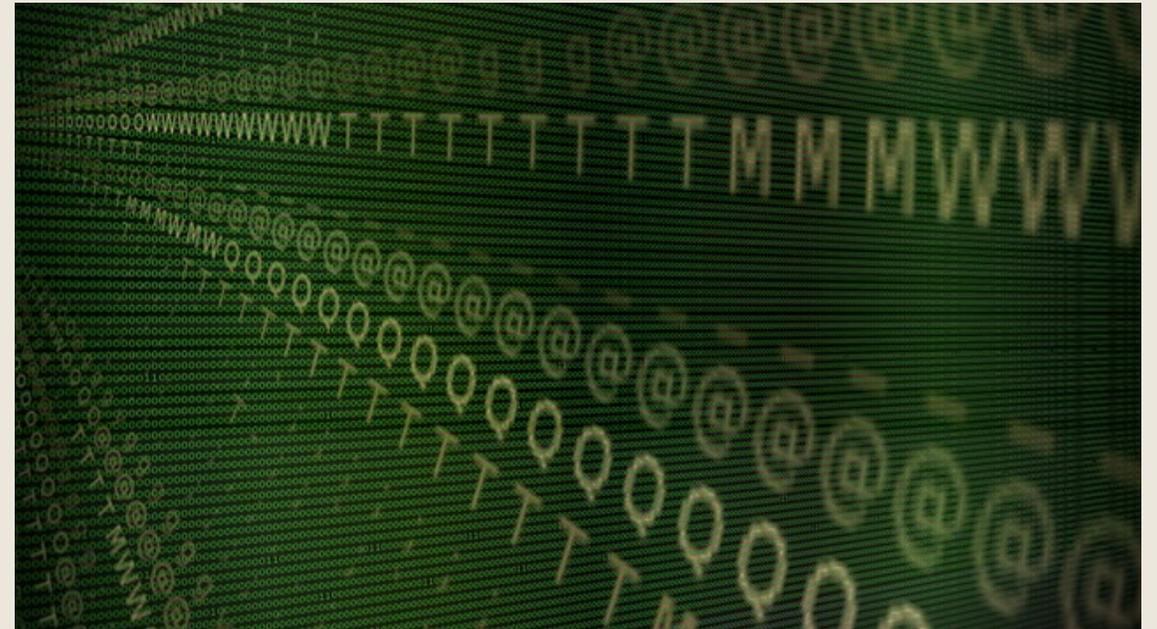


# ...but how?

Password guessing programs

Predicting human behaviours

Having knowledge of you



# That's why...

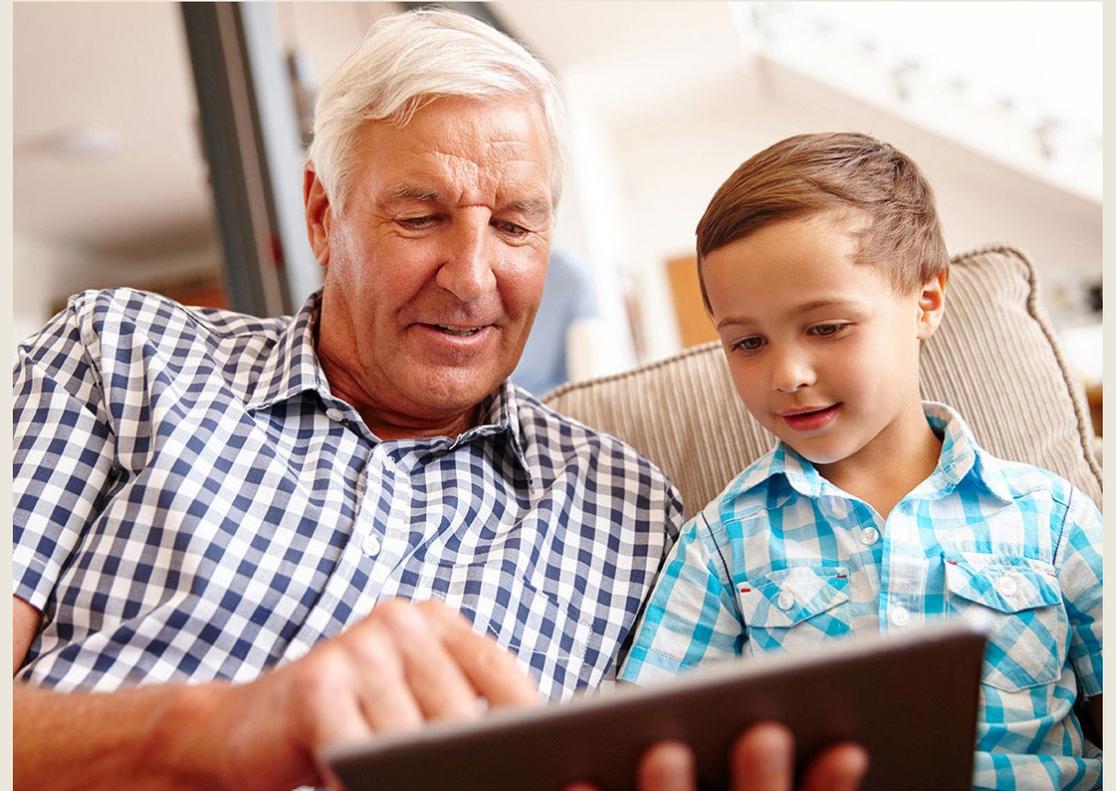
...we need passwords that can't be guessed. If you take away the easy guesses, your accounts will be better protected.



# That's it

Understanding why someone might want your passwords and how they can guess them is important.

It will make it much easier for you to understand how you can make a good password, one that can't be guessed.





# COMMON MISTAKES

# Avoid obvious passwords

The word Password

Common sequences like ABCD or 1234

QWERTY – the first 6 letters on your keyboard

Dictionary words like Friday, Obvious or Pizza



# Avoid using personal information

It is not recommended to use:

- Your name or date of birth
- Names of family members or pets
- The name of the street where you live

## Login example

Email Address

paul@gmail.com

Password

08071952



Continue

# Don't use one password everywhere

It may be hard to remember many passwords for different sites, but don't be tempted to have just one password for them all. If someone guesses that one password, they may be able to access all your online accounts, not just one.



# That's it...

You've just learnt all the things you shouldn't do...but what are the best ways to create strong, easy to remember passwords.

That's coming up next.





# CREATING A GOOD PASSWORD

# What makes a good password?

The best kind of password is one that looks like it's a jumble of **numbers, letters and symbols**. It uses both **capitals and lower case letters**.

Figit32!

12guRi

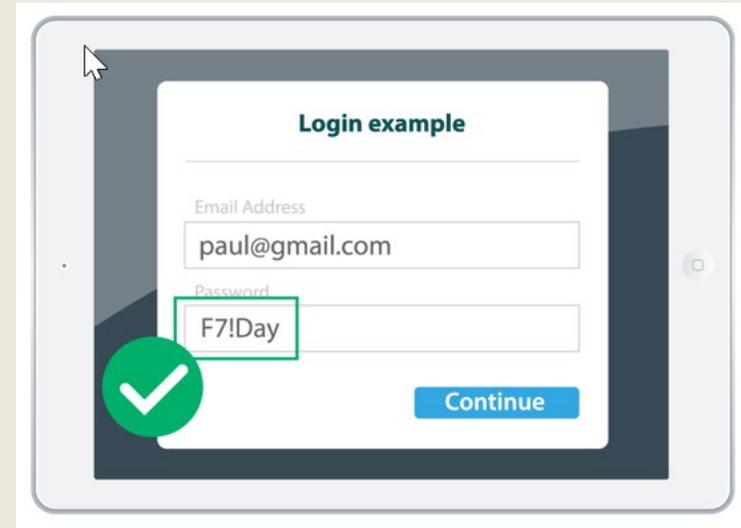
3br@T2



# Using substitutions

To make a password that's easy to remember, you can take a common word and substitute some letters with numbers, symbols or capital letters.

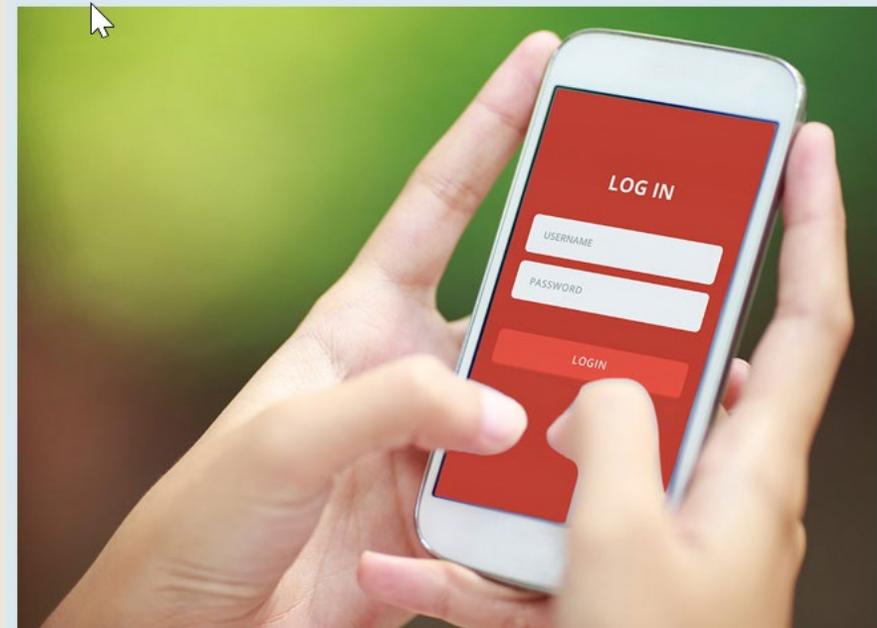
For example, it's easy to turn Friday into F7!Day



# Using substitutions

You do need to be careful with this method and make several substitutions. Some common substitutions are well known.

For example, if you change the word **forever** to **4ever**, or **house** to **h0use**, these are likely to be easily guessed.



# Using substitutions

Let's give it a go...

What can you turn from a word into a password?



# Using substitutions

Here are some other ideas...

First letters from:

- a song lyric,  
YcagwYw60
- Poem,  
TwM@t5BP
- well known phrase,  
Fbt\$0yP!

You can't always get what you want



There was movement at the station



Fly by the seat of your pants



# Using substitutions

Remember that creating unique passwords for each website is the best way to stay safe online.



# Creating a website password

Websites will make it as easy as possible for you to sign up and enter passwords.

- Many will hide what you are typing
- They often ask you to re-enter your password
- Sometimes your first attempt won't meet their security needs. They might ask you to use numbers, characters or have a minimum amount of characters.

The screenshot shows a registration page for 'ABC Shop'. At the top, there is a navigation bar with 'Shop By' and categories: DVD, Blu-ray, Books, Music, Magazines, Toys, and Clothing. The main heading is 'Register / Sign In'. There are two columns: 'New Customer' and 'Returning Customer'. The 'New Customer' section includes a message: 'First time shopping with the ABC? Create an account and make your shopping trip easier.' It has a 'My e-mail address' field with 'marion.kettle231@gmail.com' and a green checkmark. Below it is a 'Password' field with a pink border and a pink box around the text '••••••••'. Underneath the password field, it says 'Your password must include:' followed by '8 characters ✓', 'capital letters ✓', 'small letters ✓', and 'numbers ✓'. There is a checkbox for 'I accept the ABC Shop's Terms and Conditions' with a pink box around it. Below the checkbox is a small disclaimer: 'We will collect your Personal Information when you register with the ABC Shop. Information about how we use and disclose that information is available in the ABC Privacy Policy.' At the bottom of the 'New Customer' section is a green 'Continue >' button. The 'Returning Customer' section is partially visible on the right, showing 'Sign in with your', 'My e-mail address', 'Enter your email', 'Password', 'Enter your passw', and 'Forgot your passw'. At the bottom of the 'Returning Customer' section is a green 'Sign In' button.

# That's it...

You've learnt how easy it is to create strong passwords by converting something you know and changing it a little.

But how do you end up remembering all the passwords that you have to create?



The image features a light teal background with two dark blue L-shaped brackets. One bracket is positioned in the top-left corner, and the other is in the bottom-right corner. Centered between these brackets is the text "REMEMBERING PASSWORDS" in a dark blue, sans-serif font, arranged in two lines.

# REMEMBERING PASSWORDS

# How browsers can help

Browsers often ask if you would like your password remembered once you have entered it.

If you say yes, it will enter your details in automatically next time you visit that site.

When you agree to this, it will display your actual password as a line of asterisks or dots.

Password: \*\*\*\*\*



# When to say *NO* to the browser

If it is not your computer or device, or is one you share – you must say NO.

You don't want someone else's computer remembering your passwords.

When you select NO, the browser won't remember it this time.

When you select NEVER, the browser shouldn't ask you again when you revisit that site.



# True or false

Which statements do you think are true?

1. Web browsers can remember passwords for you.
2. You should always let a browser store your passwords for you on any computer you use.
3. If you don't want the browser to remember your password, you can say NO.



# Change your password

To be extra safe, it's good to change your password frequently and this is usually easy.

- Log in and make your way to the **My Account** page.
- Find the section on **Passwords**.
- Make your changes (remembering everything you have learnt). The website will confirm it has been updated.
- Use your new password next time you log in.



# Forgotten a password?

If you've forgotten your password, there is usually a **Forgotten Password** link or button when you try to login. Click on it, and you can arrange for the website to send you a new one by email.

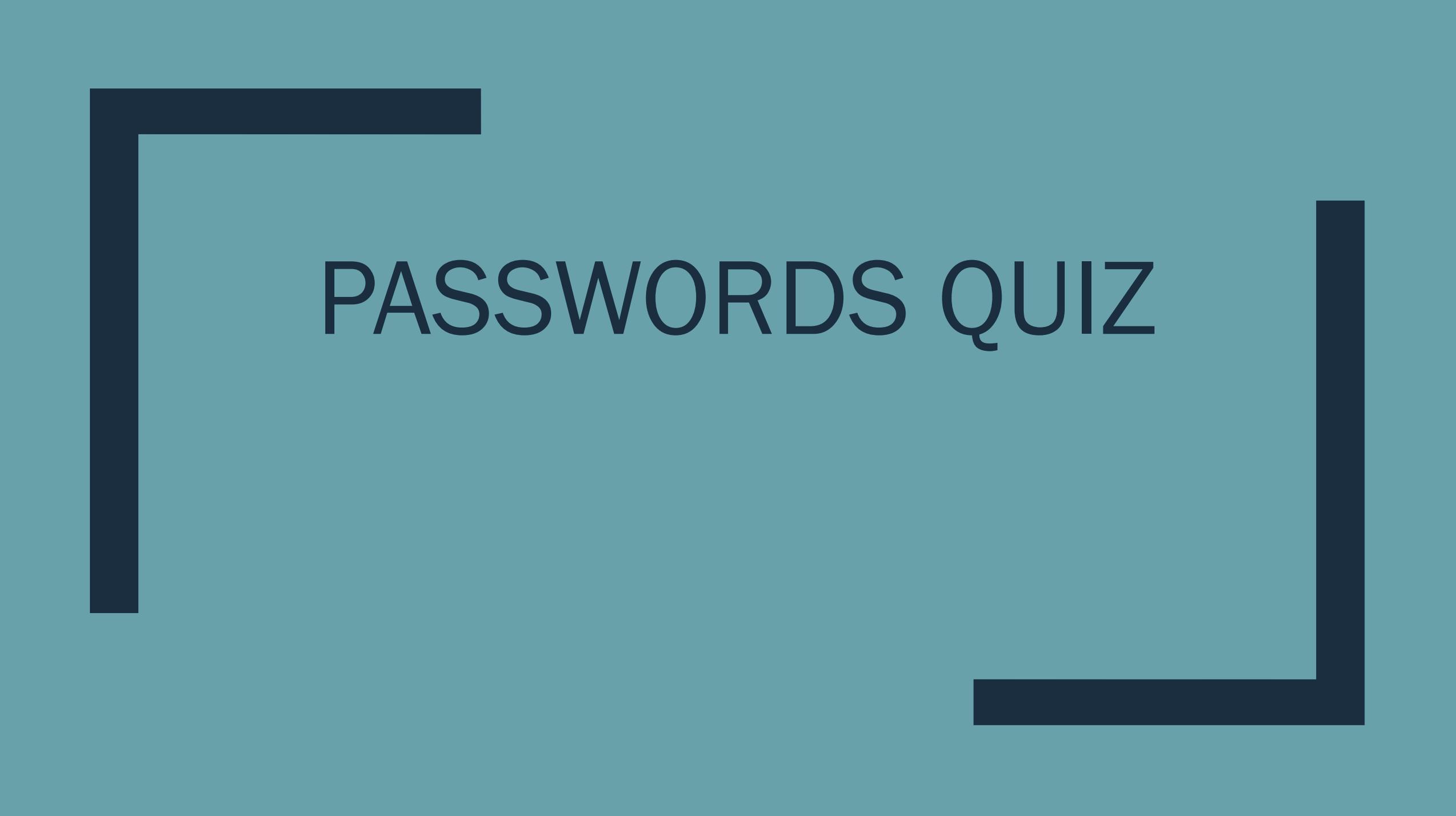
Then just follow the prompts.



# That's it...

You've learnt common password mistakes, how to create strong passwords, when to store them, and when to change them.





# PASSWORDS QUIZ

# PASSWORDS QUIZ

How are your password skills?

Here's a short quiz to test what you've learnt in the  
Passwords course.

There are three questions. Good luck!

# Question 1

Why shouldn't you use the same password for multiple sites?

- a. It will damage your computer's web browser program.
- b. If someone guesses your password, they may gain access to all of your online accounts, not just one.



# Question 1

Why shouldn't you use the same password for multiple sites?

- a. ~~It will damage your computer's web browser program.~~
- b. **If someone guesses your password, they may gain access to all of your online accounts, not just one.**

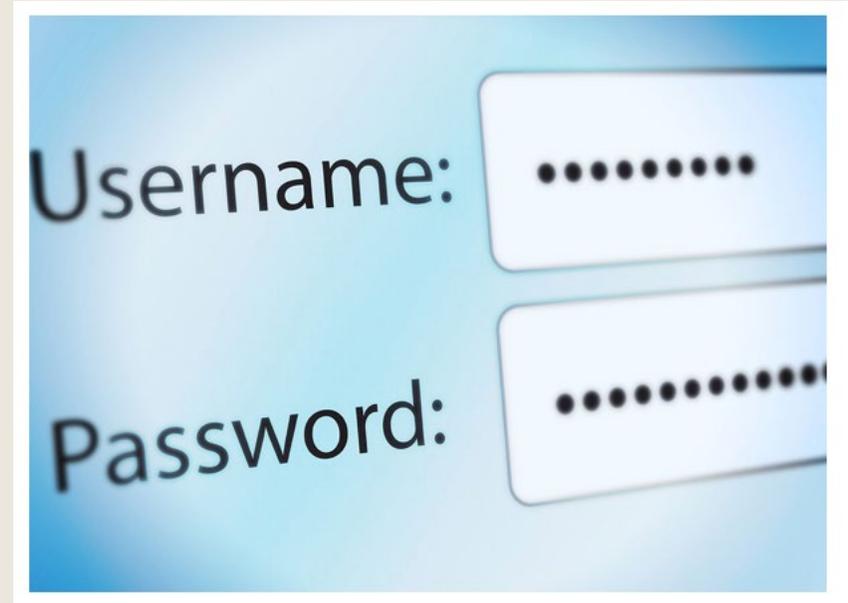
It's safest to have a different password for every website you use.



# Question 2

Which of the following do you think would make the best password?

- a. 1234567
- b. holiday
- c. B5fg73!



# Question 2

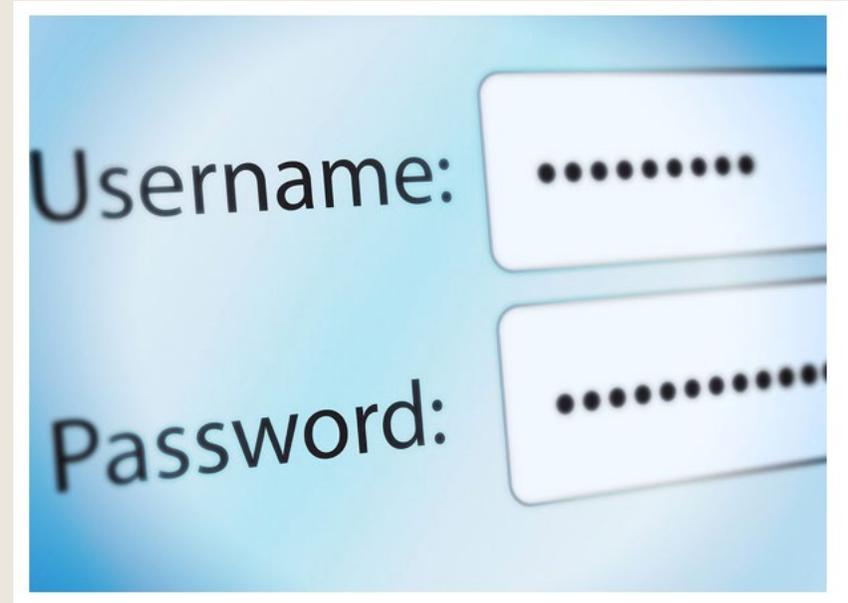
Which of the following do you think would make the best password?

a. ~~1234567~~

b. ~~holiday~~

c. **B5fg73!**

A mix of letters, numbers, capitals and symbols is a hard password to guess.



# Question 3

You're on a computer that other people have access to (like in a public library). The web browser asks if you'd like it to remember your password. Do you:

- a. Select YES
- b. Select NO or NEVER



# Question 3

You're on a computer that other people have access to (like in a public library). The web browser asks if you'd like it to remember your password. Do you:

a. ~~Select YES~~

b. **Select NO or NEVER**

If you're on a computer that other people have access to, you don't want it to remember your passwords.

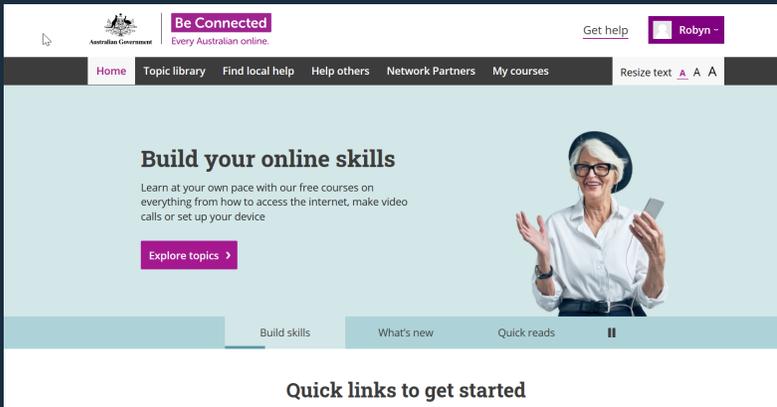


# Congratulations!

You should now have an understanding about why it's important to keep your personal details safe online, and be able to create passwords that people can't easily guess.

Remember, these lessons can save you from problems in the future!





# Like to know more about Be Connected?

Be Connected is an Australia wide initiative empowering all Australians to thrive in a digital world.

We have online learning resources as well as a Network of community partners - the Be Connected Network - who offer in-person support so you can develop your digital skills and confidence.

Find a local place for friendly help and advice, or join the Network to help others.

<https://beconnected.esafety.gov.au>

