# Section 4:
# Online safety

## In this section:

- Learn about **passwords**.
- Find out more about **online scams**.
- Learn how to **stay safe online**.

## Online we share information

It is important for us to know:

- **What information** we are sharing
- **Who can see** this information

We want to keep our **personal information safe**.

# Safe websites

It is good to **check** the **websites** you use.

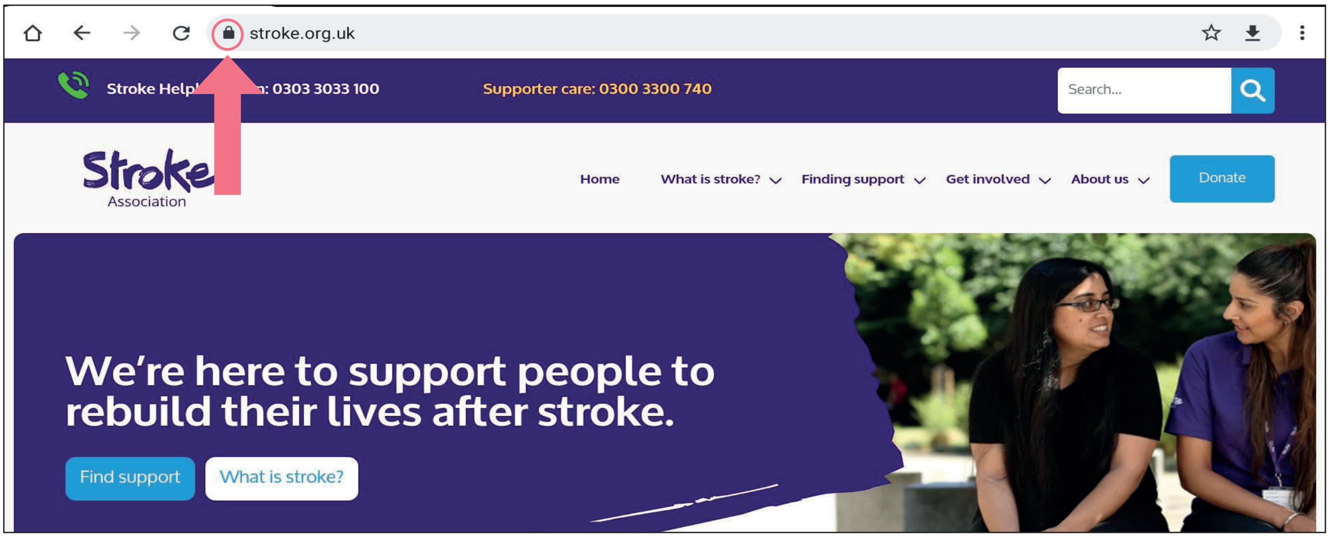
Look at the **top** of the **page** at the **address bar**.

The address should start with **HTTPS**.

It is important to see if there is an '**S**'.

The 'S' stands for **secure**.

There should be an **icon** of a **padlock**.



We're here to support people to rebuild their lives after stroke.

If there is **no padlock** or no 'S' the website is **not safe**.

**Do not use** the website or **share personal information**.

# Passwords

Passwords are a good way to **keep accounts safe**.

When you create an account it will ask you to **choose a password**.

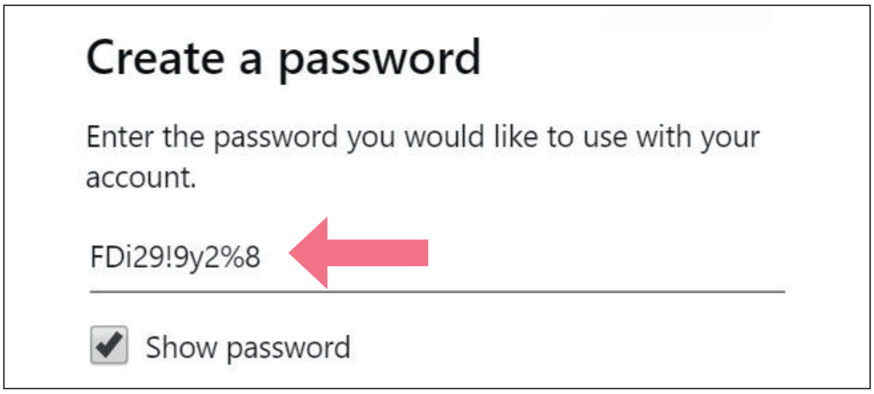
Your password must be **kept private**.

Some accounts have **rules** for passwords.

They might say **passwords need**:

- Numbers (123)
- Symbols (!$%)
- Uppercase letters (ABC)
- Lowercase letters (abc)
- At least 8 characters long

Using a **mix** of these make your **passwords harder** to guess.



Create a password

Enter the password you would like to use with your account.

FDi29!9y2%8

☑ Show password

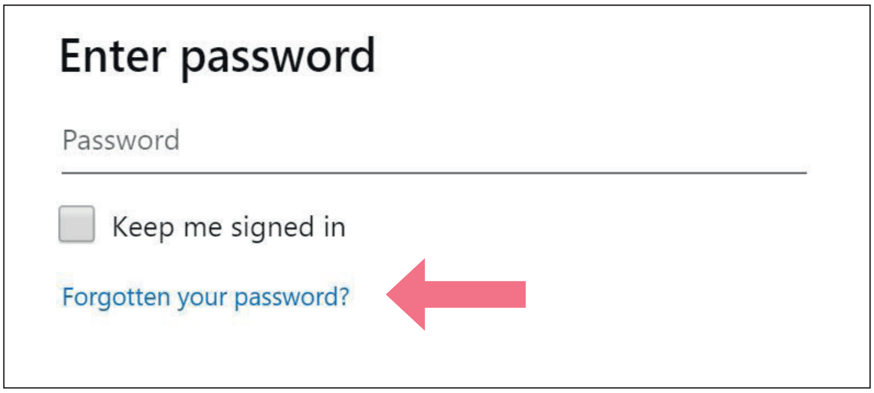
Try to **memorise** your password.

If you need to write it down **keep it** in a **safe** place, like a **locked drawer**.

It is good to **change** your passwords **every few months**.

If you **forget** your password do not worry.

**Click 'Forgot Password'** on the sign in page.



Enter password

Password

□ Keep me signed in

Forgotten your password?

The page will send an **email** to you with a **link**.

**Click** the **link** in the email.

Now you can **create** a **new password**.

## Online fraud, scams and crime

There are different types of **online scams**.

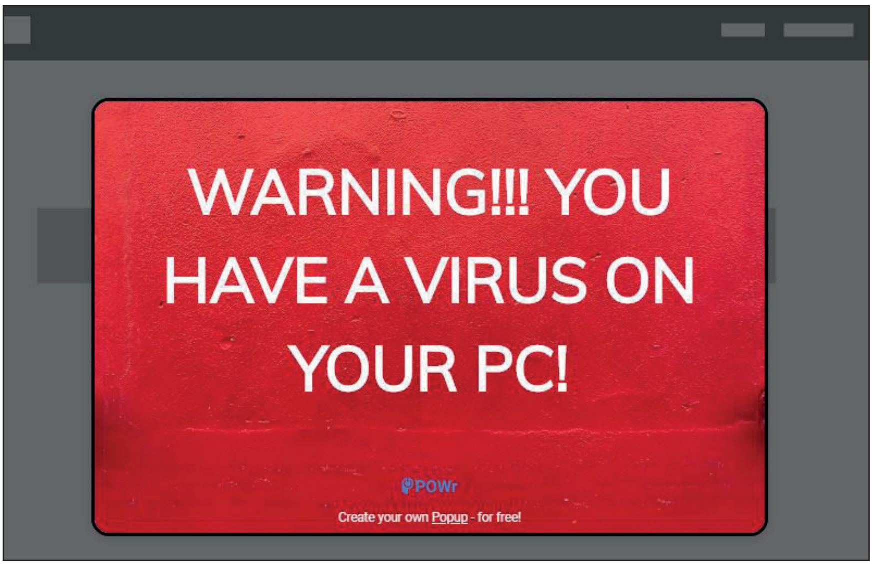
An **online scam** is when a person is given **false information**.

Scammers want your **personal information** or your **money**.

They may **try harm** your device with a **virus** or malware.

An **untrustworthy website** might:

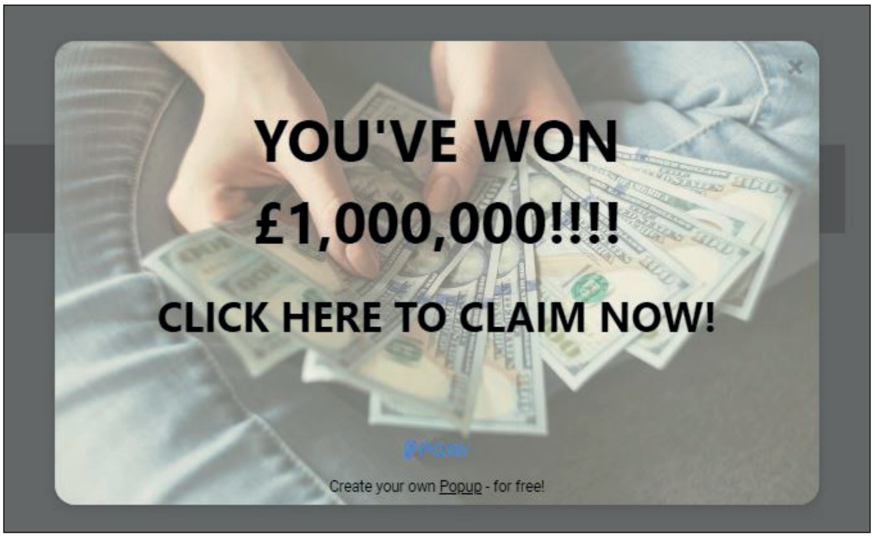
- Give you a **virus**
- Collect your **personal information** without your permission
    - Give **incorrect information** to get you to buy something
    - Trick you into **clicking on another link**



WARNING!!! YOU HAVE A VIRUS ON YOUR PC!

Some emails might have a **pop up message**.

- These messages might say you **won a competition** or have a **virus**.
- They can be **difficult to close**.
- If you are **unable to close** the pop up you can **press ALT + F4** on your keyboard.
- If you still cannot close the pop up then **restart your computer**.

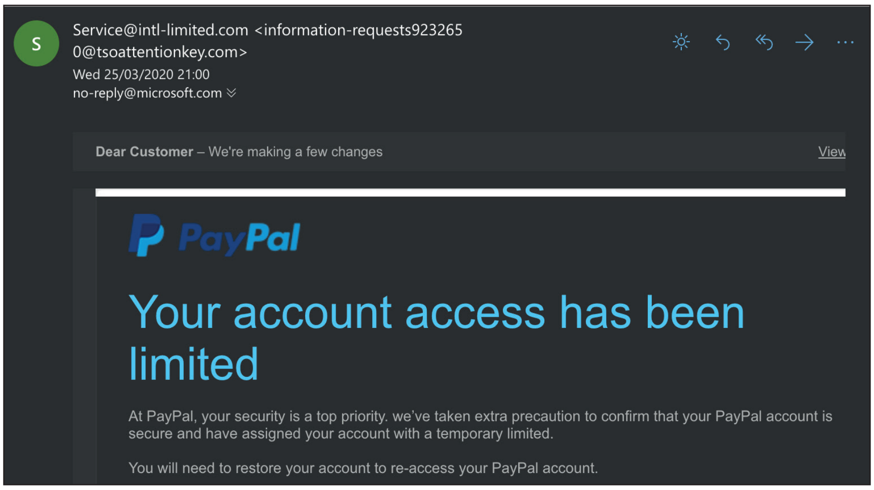


If you have an email account you might get **spam emails**.

A **spam email** is also known as junk mail.

A spam email might include **adverts**.

The email is usually sent to **lots** of **people**.



Service@intl-limited.com <information-requests923265
0@tsoattentionkey.com>
Wed 25/03/2020 21:00
no-reply@microsoft.com

**Dear Customer** – We're making a few changes View

PayPal

Your account access has been limited

At PayPal, your security is a top priority. we've taken extra precaution to confirm that your PayPal account is secure and have assigned your account with a temporary limited.

You will need to restore your account to re-access your PayPal account.

## Email scams

A **scam** email or website contains **false information**.

It might come from a **fake company**.

The email looks like it is from a **bank** or **government department**.

It might look like it is from **someone you know**.

It is called **phishing**.

If you are **worried** about a message from an email or website always **contact the organisation directly**.

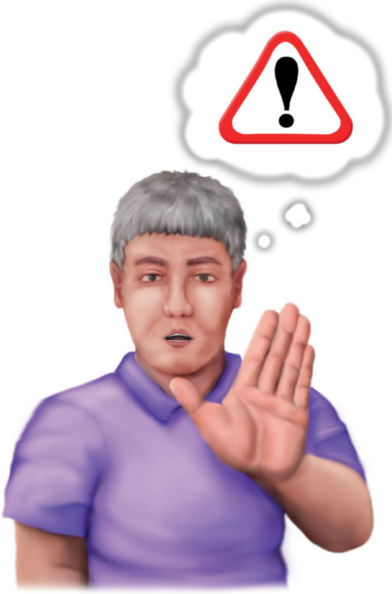
**Do not** use the **contact details** in the **email** you suspect.

In a **scam email** they may:

- ask you to **click** on a **link**
- phone a **fake number** or give **information**
- ask for **money**

**Questions** to ask when you think it might be a scam:

- Do I **know the person** or organisation?
- Does the email have the **correct logo**?
- Does the information **look professional**?
- Are there any spelling or grammar mistakes?
- Are they **making promises** that seem unreal?
- Are they **asking for money** or personal information?
- Are they pushing you to make a quick **decision**?



## How to stay safe online

Remember:

1. Do not give **personal information.**

2. **Do not reply** if you think an email comes from a scammer.

3. **Do not click** on **unknown links** or download items from unknown sites or emails.

4. **Delete spam emails** or mark them as spam.

5. If you are **unsure** always **contact** the person or organisation directly.

## Safety tips when using a shared device

Sometimes we might **share a device.**

For **example**, you might use a computer at a library.

1. **Do not let the computer remember you.**

   When **logging on** to an account you might see a box that says:

   - 'Remember my ID on this computer.'

   - 'Remember me.'

   - 'Store my password.'

   **Do not tick** this box. You **do not** want your **details saved** on a computer others use.

## 2. Sign out of your accounts

Remember to **sign out** of your **accounts** such as email and social media.

If you do not sign out, someone else using the device **could use your accounts**.

You can **log out** of most accounts the same way.

There will usually be '**sign out**' written in the **top right corner**.

**Click** on '**sign out**'.

## 3. Avoid banking and other confidential activities

A **public computer** might have a **virus** or **spyware**.

Limit banking or private activities for home or **personal devices.**