What is a data breach?

 Prepared by Disability Equality Scotland

What is a data breach?

This guidance explains:

- what data breaches are
- how they can affect you
- what you should look out for after a data breach

A **data breach** happens when information held by an organisation is stolen or accessed without permission.

Then criminals can then use this information when creating **phishing** messages (like emails and texts) so that they look real.

Phishing is when criminals send emails pretending to be from a company you trust like Royal Mail, or from your bank.

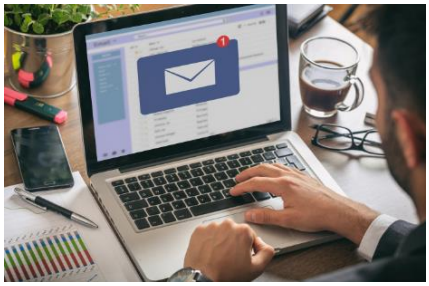
Phishing is used by criminals to trick you into telling them personal information like passwords or credit card numbers.

It looks like a message just for you.

The criminal will have sent out millions of **scam** messages.

A **scam** is a trick to get your money or personal information like your bank details.

How might you be affected?



In a typical scam, a criminal could send you a message pretending to be from an organisation that has had a data breach.

The message could ask you to log in and **verify** your account because **fraudulent** activity has taken place, or a similar message.

Verify means to agree that it is correct.

Fraudulent means it is false and trying to trick you.

Scam messages often have links to websites that the criminal wants you to click on.

The websites:

- steal any passwords you type in
- put viruses onto your computer

If the information stolen during the breach includes phone numbers, you might receive a **suspicious** phone call.

Suspicious means something does not look or sound right.

The phone call could ask you for:

- personal information like bank details or passwords
- access to your computer

What to do if you are a customer of an organisation that has had a data breach

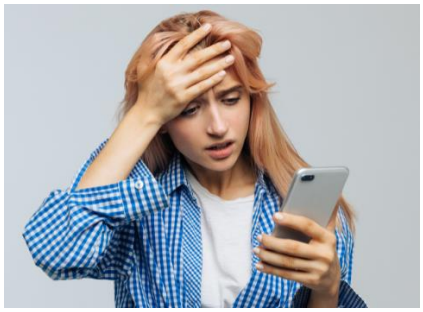
- **contact the organisation using their official website or social media to find out if you have been affected**

Do not use the links or contact details in any messages you have been sent.

The organisation should be able to tell you:

- if a data breach has happened
- how you are affected
- what you need to do

You can also phone the organisation but they are not likely to answer the call if there has been a data breach.



- **look out for suspicious messages which may be sent some time after the breach is made public**

Remember, your bank will never ask you to supply personal information.

Things to look out for include:

- emails full of **tech speak**

This means technical information that is difficult to understand

- official-sounding messages about:
    - resetting passwords
    - getting **compensation** - **t**his means money awarded for a loss or injury
    - scanning devices
    - missed deliveries

- being encouraged to do something straight away

- **if you get a suspicious message that includes a password you have used in the past do not panic**

If this is a password that you still use, you should change it as soon as you can.

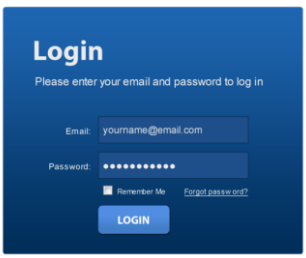
If any of your other accounts use the same password, you should change them as well.

For advice on creating strong passwords, visit www.cyberaware.gov.uk

- **check your online accounts to check if there has been activity you have not agreed to**

Things to look out for include:

- not being able to log into your accounts
- changes to your security settings
- messages or notifications sent from your account that you do not recognise



- logins or attempted logins from strange locations or at unusual times

If you think your account has been accessed, look at the NCSC guidance on recovering a hacked account.

- **check if your details have appeared in any other data breaches by using the website: https://haveibeenpwned.com**

You might find support in your own antivirus tools or password manager.

How to report suspicious messages

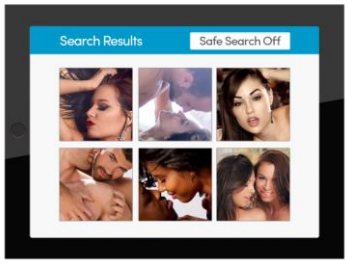
- if it is an email, forward it to the NCSC's Suspicious Email Reporting Service at report@phishing.gov.uk

- if it is a text message, forward it to 7726

This a free service.

- If it is a suspicious call or a call that you do not want, hang up and contact your phone provider

- if you have been a victim of a **sextortion** scam, report it to your local police by calling 101



Sextortion is when someone threatens to publish sexual information, photos or videos about someone.

They do this to get money or to make the victim do something they do not want to.

If you have lost money

If you have lost money:

- tell your bank
- report it to Police Scotland by calling 101

 Prepared by Disability Equality Scotland