Lead Scotland

How to spot a scam message

Easy Read

 Prepared by Disability Equality Scotland

This document tells you how to spot:

- scam emails
- scam text messages
- scam phone calls

Scam means a crime where someone is tricked into giving away their:

- personal information
- money

Scams are done by criminals so that they can get money.

About scams

Criminals might send you:

- a text
- an email
- a phone call
- a message on social media

They often pretend to be a person or an organisation that you trust.

These scam messages used to be easier to spot.

They often had lots of spelling mistakes and bad pictures.

But many scams are more clever now. They are hard to spot.

How to spot a scam

Scams often have these 5 things:

1. It says it’s from someone important

Scam messages often say they are from someone important.

It might be pretending to be from:

- your bank
- a doctor
- a solicitor or lawyer
- a government department

2. It says it is urgent

Urgent means it needs doing fast.

Scam messages often say you have only got a short time to reply.

It might say things like:

- ‘within 24 hours’
- ‘immediately’

Criminals often say there will be a fine to pay if you don’t do something. Or something else bad will happen.

3. It makes you feel a strong emotion

Scams often use words which:

- threaten you
- tease you

Scam messages often make you feel emotions like:

- panic
- fear
- hope
- curiosity

4. It offers something special

Scam messages often offer you something:

- special – like concert tickets
- needed – like money
- hoped for – like a medical cure
- exciting – like a good deal

Criminals hope that this will make people reply to the scam message quickly.

5. It is linked to what is going on in the news or in real life

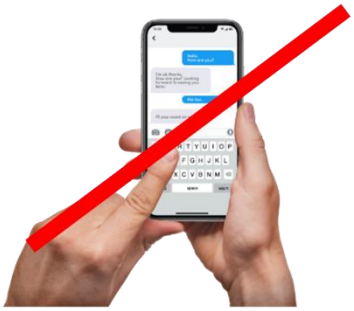
Scams are often linked to real life.

They might be linked to:

- something that has just happened in the news
- something happening in real life
- the time of the year – like the end of the tax year

How to check if a message is real

To check that a message is real and not a scam you must ask the organisation or person.



Don’t use the contact details from the scam message.

Find the real email address or phone number from their official website – and use it to ask the organisation if the message was from them or not.

Remember that important organisations – like your bank – will never ask you to put your personal information in an email.

How to be safer

Criminals look at places like:

- your Facebook pages
- your Twitter pages
- your Instagram pages
- other online information about you that can be found in a search

Decide what you want to put on these pages and what you want to stay private.

Use the privacy settings to decide:

- who can see your information
- who can’t your information