Lead Scotland

Linking education and disability

Lead Scotland

Impersonation fraud

What to do when someone tricks you into believing they are someone else

Easy Read

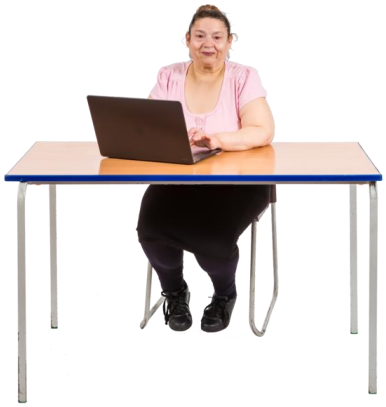
Easy Read made by Disability Equality Scotland

made with photosymbols®

What impersonation fraud is

Fraud is when someone tricks someone else into giving away things like their money.

Impersonation is when someone pretends they are someone else.



Impersonation fraud is when someone pretends to be from a trusted organisation like your bank.

They they trick you into giving away your private information or money.

In this document **criminals** are people who tell lies to steal information or money from other people.

These are the kinds of organisations that criminals pretend to be working for

- your bank
- the police
- a delivery company
- your water, gas or electricity company
- your phone company
- the government

Criminals might also pretend to be

- a friend of yours
- a family member

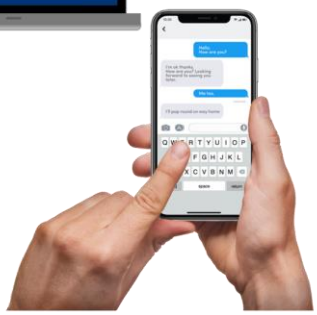
Types of impersonation fraud

You might get

- a letter

- a phone call
- a text

- an email



- a social media message

which looks like it is from an organisation or a person that you trust.

You might get a scam message saying your bank account is at risk.

The criminal might pretend to be bank staff and ask you to move your money to a ‘safe account’.

The criminal might pretend to work for the police.

They might tell you that your money needs to be moved so that it can be looked at by the police.

The criminal might pretend to be your friend or family member.

They might pretend they need help fast.

They might pretend they need money for

- an emergency
- to pay rent
- to get a flight home from another country

The criminal might try to send a **courier** to your collect your bank cards, cash, passwords, pin number or valuable things from your home or workplace.

A **courier** is a company that will deliver and collect things from houses and other addresses.

The criminal might tell you that your internet access has been **hacked**.

Hacked means that someone else has got into your system without permission.

The criminal might say that you can get some money, called compensation, because you were hacked.

When they pay the money into your account, they pay too much and ask you to pay some back.

While you are paying back, they get control of your bank account and take all your money.

How to notice impersonation fraud

Look out for messages that say you need to pay money or move money very quickly.

Look out for messages that make you feel panicky.

Look out for messages that offer you a kind of reward.

Or ones that say you will save your money from danger.

Look out for messages that tell you to move your money from your account into another account to keep it safe.

This is not true.

Look out for messages that say you can pay a fine by buying expensive goods or vouchers for someone else.

Look out for messages that say you have a **tax rebate**.

A **tax rebate** is when the government pays you back some money because you paid too much tax.

Look out for messages that say you have to pay a tax bill or a water or gas bill.

Look out for messages that say your money is part of a police investigation.

Look out for emails where the address that sent it is a little different from that person's usual address.

Remember that criminals can change their **Caller ID** to look exactly like someone you already know.

Caller ID is the name or words that show on your phone when someone phones you.

Look out for messages or calls that say if you don't do something quickly, you might get

- a fine
- arrested
- a criminal record

Look out for links to websites that look a bit odd.

They can be fake websites.

How to stay safe from impersonation fraud

If something does not feel right in a phone call, hang up.

Do not let anyone take **remote access** of your computer or phone if they have called you and you were not expecting their call.

Remote access means that you give someone else permission to control your computer or phone from anywhere else in the world.

Do not log in to your bank or money accounts when you are using **public WiFi**.

Public WiFi means internet access when you are in places like

- shops
- trains
- cafes
- airports

Remember that banks and the police will never ask you to move your money to a safer account.

Stop and think before you click on any links that ask you to make a payment or give your personal information.

Only give out your information to organisations who you were expecting to hear from.

What to do if you think this has happened to you

If you think you have been tricked, do these things

- contact your bank straight away.

  Use the phone number that you know to be right, from your statement or card

- tell Police Scotland by calling **101**

advice direct scotland

- phone Advice Direct Scotland on **0808 164 6000**

TAKE FIVE TO STOP FRAUD™