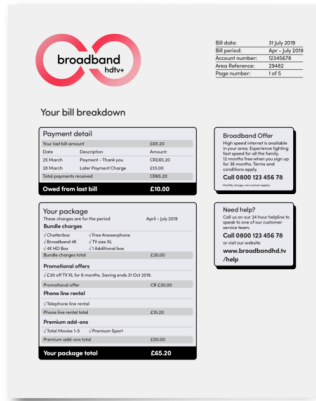


Invoice and mandate fraud



Easy Read

What invoices and mandates are



Invoices are paperwork or emails sent by an organisation to ask you to pay them money for something you have agreed.



A **mandate** is an agreement from you telling your bank to make a payment for you.

What invoice and mandate fraud is



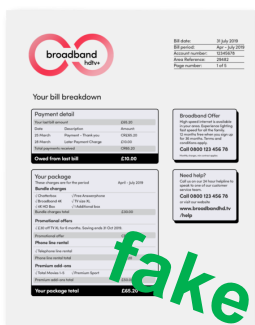
In this document **criminals** are people who tell lies to steal money from other people.



Criminals often pretend to be from an organisation you trust.



They send you different bank details and trick you into paying your money to them instead of to the organisation.



This is called invoice and mandate fraud.

Criminals can pretend to be



- your builder
- a tradesperson, like a plumber or electrician
- from another organisation that you trust
- your **solicitor**



A **solicitor** is a law expert.

Solicitors give advice about things like buying a home or complaining about a service.



Criminals might try

- getting into your emails
- getting into your trusted organisation's emails
- pretending to be someone else

How to notice invoice and mandate fraud



You might get information from an organisation you trust, telling you that they have changed their bank account details.



They might send you the new bank account details.



But this is not true.

They are criminals and if you use the new bank details you will lose your money.



You might get extra invoices or copies of invoices, asking you to pay again.



But this is not true.

They are criminals and if you pay the invoices you will lose your money.

What to do if fraud has happened to you



If you think invoice or mandate fraud has happened to you, 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**



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

More information about keeping your money safe



If you are paying an organisation for the first time, just pay a small amount of money first.

Then ask the organisation to check they have got the small amount.

If they have, then pay the rest.



Get in touch with the real organisation and check the bank details you have are right.



If you get information telling you an organisation has changed their bank details, get in touch with the organisation the way you know is real, and check with them.

Organisations do not often change their bank details.



Be careful using social media, like Facebook, Instagram or X.

If you post clues about your life there, criminals may be able to guess what kind of big money choices you are making.

