

What is identity theft?

 [Print this guide](#)

Criminals commit identity theft by stealing your personal information – that is, your name, address, date of birth, bank account numbers, passwords and so on – and then pretend to be you. This is fraud.

It's usually done for financial gain – for example, your bank account can be accessed and your money stolen or someone can make purchases or apply for credit in your name. When using the internet, it's very important to take precautions to protect your identity details.



How to spot scam emails, texts or social media messages

Online fraudsters can mimic the company details and emails from trusted companies to hide their identity, so be vigilant! Scam messages will often imply a sense of urgency for you to act quickly. This might be to call a number included on a text message, a request for personal information, or banking details and security credentials.

Scam messages even encourage you to open links or attachments. This will open a fake website where you will be asked to login to your PayPal account for example. The fraudsters then use these details to access your account and steal your money.

Other types of identity fraud include:





- Tax rebate fraud
- Benefit fraud
- Telecommunications fraud
- Pension scams
- Driver's Licence fraud
- Change of Address fraud
- Romance fraud scams
- PPI refund scams.

For more information about identity theft visit [Action Fraud](#).

We recommend that you read our guide on [How to protect yourself from identity theft](#).

This guide was updated January 2023

Next steps

-  [What is phishing?](#)
-  [A guide to internet security](#)
-  [Email safety tips](#)
-  [Email safety tips](#)

▶ [How to stay safe online](#)

▶ [How to protect yourself from identity theft](#)

How do digital skills change lives?

Find out about Digital Inclusion
