Castle Trust

Protect yourself against identity theft

What is identity theft?

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to enable them to commit identity fraud. Identity theft can take place whether the fraud victim is alive, or deceased.

If you're a victim of identity theft, it can lead to fraud that can have a direct impact on your personal finances and could also make it difficult for you to obtain loans, credit cards or a mortgage until the matter is resolved.

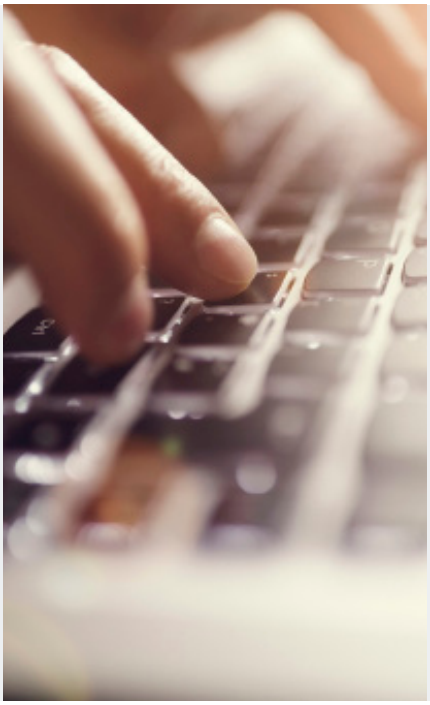
What is identity fraud?

Identity fraud is the use of a stolen identity for criminal activity, such as to obtain goods or services by deception.

Fraudsters could use your identity details to:

- Open bank accounts
- Obtain credit cards, loans and state benefits
- Order goods in your name
- Take over your existing accounts
- Take out mobile phone contracts
- Obtain genuine documents such as passports and driving licences in your name.

You may not become aware that you have been a victim of identity fraud until you receive bills or invoices for things you haven't ordered, or if you receive letters from debt collectors for debts that aren't yours.



What is phishing?

Fraudsters may try to trick you into revealing personal information by pretending to be from a legitimate source – this is known as 'phishing'. A phishing scam usually begins with an email (perhaps with a link to a fake website, or with a form attached), a text, or an unexpected call which looks or sounds like it's from a genuine business. The email or website might even have all the right logos or fonts on it. The scam might ask for personal details like usernames, passwords, PINs, or even ask directly for your bank account details. Alternatively, you may be encouraged to open a document attached to an email, which could in fact infect your computer with a virus.

Often, the approach is made under the premise of conducting routine maintenance, or to update your security details. A more dramatic approach (designed to frighten you into taking action) can be to tell you that you have already been the victim of fraud, and that the details are required to confirm that you are who you say you are, and to stop any further fraud taking place.

How can I spot a possible phishing scam?

Phishing isn't always easy to identify, but there are a number of clues to look out for, for example:

- Poor spelling or grammar – scams often originate overseas, where the scammers have weak English language skills
- Non-personal address – the scammer probably doesn't know you by name, so they might address you as 'Dear Sir/Madam' or similar, or something less formal such as 'Dear Friend'

- Unexpected email – try to think whether there is a good reason for this business to be contacting you
- Suspicious email address – some of the email addresses used in such scams clearly raise suspicion, because they look like a personal email address. Others, however, can look like they are from a genuine organisation, but there may be clues to indicate that isn't the case – perhaps a letter may be out of place, or a section of the email address (perhaps after the '@' symbol) looks inappropriate
- The website address that a link takes you to – check that it appears to be genuine, isn't unusually long, or has letters substituted by numbers (for example, a 3 instead of an E, or a 4 instead of an A)
- Requests to act quickly – you'll often be urged to take action immediately, perhaps on the premise that your account will otherwise be suspended, or to prevent any further fraud taking place against you (a double-bluff).

What should I do if I suspect a scam?

If you have any reason to suspect whether the contact is genuine – even if it just doesn't 'feel' right – proceed with caution.

Phone calls

- Don't disclose any personal or financial details to the person on the phone
- Don't tell them any password or login details
- Don't reveal your PIN number, or any of the numbers on your credit or debit card
- Tell the caller that you will contact their organisation directly instead, and hang up. Don't be afraid to be authoritative
- Wait a few minutes, and check that you have a dialling tone before you call any Helplines (sometimes the fraudulent caller may remain on the line).

Emails

- Don't reply to the email
- Don't open any attachments
- Don't click any links in the message
- Don't phone any numbers or visit any website address included in the message
- Delete the email from your Inbox, then delete it from your Deleted Items folder (sometimes called Trash).

Texts

- Don't reply to the text
- Don't click on any links in the message
- Don't phone any numbers or visit any website address included in the message
- Delete the text.

What should I do next?

If the contact claims to be from an organisation that you already have a financial relationship with, check previous correspondence you have received from them (a bank or credit card statement, for example), or look up their website address via a search engine such as Google or Yahoo, to find a genuine Helpline telephone number.

Call their Helpline, explain the contact you have received and ask them if it is genuine or not; they may be able to help you immediately, or may need to put you through to their fraud department to confirm whether the contact was genuine or not.

If you do not have a financial relationship with the organisation that has contacted you, there is more reason to be suspicious. Search for their website via a search engine such as Google or Yahoo, and contact their Helpline number.