National Office for Identity Data
Ministry of the Interior and Kingdom Relations

Identity fraud

Don’t give scammers a chance

A safe ID

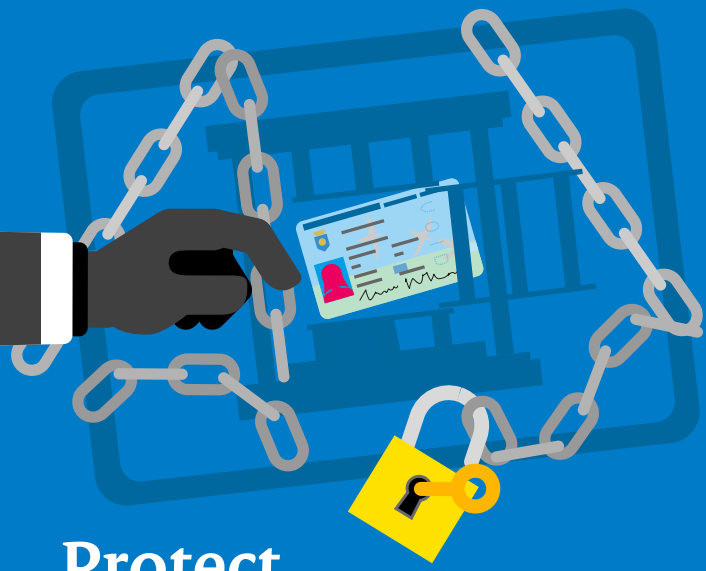
Borrowing money and disappearing off the face of the earth. Taking out a telephone subscription and running off with the latest smartphone.

Now imagine a fraudster doing this in your name. They disappear into thin air and you are left with the bill. We refer to this as ‘identity fraud’ and it can have drastic consequences.

How does it work? A fraudster gets hold of details of your identity, for example from a copy of your Caribbean Netherlands ID card (sédula), via an online advertisement, or by sending a ‘phishing mail’. The fraudster can then, for example, use these details to take out a loan in your name.

This flyer contains information on what you can do to prevent identity fraud.

Information on using your computer, tablets and telephone online safely can be found at
www.veiliginternetten.nl



Protect your personal data from thieves

- Keep your ID document in a safe place. If you have lost it, or if it has been stolen, notify the municipal civil affairs department [Burgerzaken] so that the document can be blocked and then apply for a new one.

- Take steps to make things even more difficult for hackers and protect your (online) accounts with a two-step verification. Then you will not only log in using your login name and password, but will use an extra access code which you receive, for example, in a text message.

- Always install the latest updates on your computer and telephone and use different passwords for online accounts. If you find it difficult to remember these passwords, you can use a password manager.

Do not share your personal data and documents with others

- Never send a copy of your identity document or bank card when buying and selling online.
- Learn how to recognise phishing! Phishing is not just something that is done by email, but also by telephone, text message or via WhatsApp. If you are asked to disclose your ID, bank or login details, you should be extra vigilant.
- Never disclose your personal data, login details, or PIN codes during a telephone call. Fraudsters will use ‘spoofing’ techniques to make it look as if they are using an existing telephone number of, for example, your bank, so you should make sure you are not fooled by the telephone number you see in your screen.
- If you are suspicious, call the person or organisation that is requesting the details and check whether the request is legitimate.

Make sure you do not simply give away your personal data

- Delete files and accounts from computers and telephones before you sell them or dispose of them.
- Be careful what you share on social media. Do not post any photos of your passport, sédula or driving licence.
- If you are obliged to issue someone with a copy of your ID document, make it unusable for fraudsters by writing down the date and purpose on the copy and cross out details which the recipient does not need. You should do this using the KopieID app.

Download the KopieID app from the Play Store or the App Store.

Do not make things too easy for criminals and be alert

The **Central Identity Theft Reporting Centre** [Centraal Meldpunt Identiteitsfraude] (CMI) provides tips and advice to prevent identity fraud and supports victims in order to stop data misuse and mitigate the consequences.

More information
www.rvig.nl/cmi

Victim of identity fraud?

- report the matter to the police
- notify the **Central Identity Theft Reporting Centre** (CMI) via www.rvig.nl/cmi