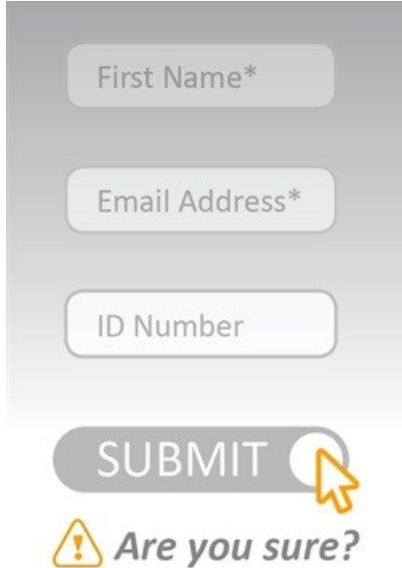


Identity theft: take care before you share

Identity theft and fraud is a widespread global phenomenon that has gained considerable momentum in South Africa in the last decade.



The internet and social media – combined with the naivety of the public in sharing personal information – have helped make the work of criminals easy.

By sharing their information on social media, clicking on unsafe links in emails, and by responding to phishing emails and phone calls, an increasing number of unsuspecting members of the public are becoming victims of identity fraud. By using stolen identities, criminals are able to steal money from bank accounts, apply for financing on vehicles in someone else's name, and all manner of fraud.

Using less technical means

Although the internet has helped perpetuate the scourge of identity theft, fraudsters are also known to use less technical means such as going through rubbish bins in search of important documents and mail such as credit card and insurance statements. Other more organised criminals hack into organisations' networks to access consumer files and information.

“To protect yourself from becoming a victim of ID fraud and/or theft you must be aware of the growing problem and act immediately if you notice any suspicious activity on your bank account or receive any strange phone calls or emails

requesting you to supply information or worse still, if you receive documentation about finance or insurance on vehicles you haven't bought, retail accounts that you have never applied for, or credit cards you don't have.

"Organisations are obliged by the Protection of Public Information Act (PoPIA) to implement measures to stop unauthorised access to, and protect, the information they store and process about their customers," says Charl Ueckermann, CEO at AVeS Cyber Security.

PoPIA rights

In terms of PoPIA, consumers have certain rights with regards to their personal information. It allows people to have control over when and how they choose to share personal information. For instance, they would need to give their consent before the information is shared. Furthermore, information should only be shared for a valid reason.

PoPIA obliges companies to be transparent and accountable about how they will use the personal information they collect and to notify their customers should their data be compromised. In addition, PoPIA obliges companies to provide their customers with access to their own information as well as the right to have their data removed or destroyed. Companies also need to put adequate measures and controls in place to track access and prevent unauthorised people, even within the same company, from accessing customer information. This means implementing strict processes and technologies to control access to data and prevent data losses and breaches. Failure to do this puts companies at risk of penalties.

"Be informed of your rights with regards to your information and how it is used by companies. If you feel that your queries in this regard are not answered satisfactorily, then don't hand over your data," warns Ueckermann.

Tips to protect yourself against identity theft

- Always keep your ID book, passport and drivers licence in a secure place.
- Before you disclose any personal information find out how it will be used. Make sure that the information will be kept confidential.
- When you are requested to fill in personal details on documents, ensure that the company you are dealing with is legitimate. Verify if the representative posing on behalf of the company does indeed work at the company in question.
- Keep a record of your accounts and follow up if statements do not arrive on time.
- Guard your mail against theft. Remove post from your letter box straight after it has been delivered. If you are going to be away from home, ask a neighbour to collect your post for you.
- If you move to a new place of residence, change your address on your accounts without delay.
- Do not use predictable passwords such as your date of birth or telephone number on your accounts or online.
- Carry only the amount of information that you will actually need in your handbag or wallet.
- Do not give out personal information on the phone, through the post or over the Internet unless you have initiated the contact or know whom you are dealing with.
- Keep items with personal information in a safe place. Tear or shred documents such as credit applications, bank statements and receipts before throwing them away.
- If you have service work done at your home or employ outside help, do not leave personal information lying around.
- If you live with housemates ensure that your personal information is kept safely.
- Give your ID only when absolutely necessary. Ask to use other types of identification when possible.
- Request a copy of your credit report from each of the major credit reporting agencies every year. Make sure it is accurate and includes only those transactions you have authorised.