Stealing who you are

Description

The crime of identity fraud is increasing on an alarming scale, with personal information becoming more accessible via the dark web due to an increasing number of data breaches. More than ever before, it's important that we protect ourselves and our company from these cybercriminals.

What is identity theft?

Identity fraud is the unauthorised use of a person’s personal information by another person, obtained through various sources, including data breaches. It is then used to commit a crime or deceive or defraud that person or a third party to take advantage of the privileges that come with that identity.

What is a data breach?

A data breach is when unauthorised parties gain access to sensitive or confidential information which is:

- Theft of private or confidential data without the owner’s knowledge or permission;
- Release of confidential information into an unsecured environment;

- Unauthorised access or exposure of sensitive information; or
- A cybersecurity mishap where data falls into the wrong hands.

Medical data is among the most sensitive information shared with organisations. No organisation is 100% breach-proof, and to minimise the fallout, it is therefore important to understand what's at stake and what to do if your information is compromised.

Stranger danger

The following can fall into the hands of a stranger:


default watermark

- Personally identifiable information (PII), such as identification (ID) number, home address, email address, or birth date;
- Passwords to key medical, insurance and financial accounts;
- Medical history, including treatments and prescriptions; and
- Billing and payment information, including credit and debit card and bank account details.

What could happen

Possible results of a data breach include the following:

1. Someone can incur bills and debt on your credit card by:

- Opening new lines of credit;
- Accessing and draining your bank account funds;
- Impersonating you to obtain medical services or medication;
- Filing fraudulent tax returns to obtain rebates; and
- Blackmailing you by threatening to share confidential information on medical conditions and treatments.

2. Precautions you can take to protect your personal information:

- Always verify and authenticate any request for information, no matter how genuine it seems at first glance. This may mean that you must call the insurance company or your broker directly to verify the request. Remember the psychological manipulation effect – fraudsters make you feel important and respected to gain your trust.
- Never share identifiable information, policy numbers or claims numbers with strangers.
- Take extra caution when storing or disposing of insurance documents.
- Be cautious when clicking on links.

What to do following a data breach

1. Check notifications
2. Find out exactly what happened
3. Monitor your accounts
4. Report suspicious activity
5. Freeze your credit and cards
6. Change your passwords
7. Stay alert

Category

1. Our Knowledge Centre