Identity fraud is increasing on an alarming scale.

Personal information has become more accessible via malicious sites on the internet due to the increasing number of data breaches in recent times. Another method commonly used by fraudsters to trick victims into disclosing personal information is called social engineering. It is a technique based on emotional manipulation and deceit into getting the victim to reveal confidential personal information.

By definition: **Identity fraud** is the **unauthorised use of a person's personal information** by another person, obtained through various sources, including data breaches, to commit a crime or deceive or defraud that person or a third party

Data breach is unauthorised parties gaining 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 it is therefore important to understand what's at stake and what to do, in the event that your information is compromised – to minimise the fallout.

The following can be in the hands of a stranger:

- Personally identifiable information (PII) – Identification 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.
- Fraudsters uses social media to gather personal information of potential victims.

Possible results of a data breach:

- Impersonate your identify to obtain medical services or medication;
- Changing of bank account details to intercept refunds due to you.
- You can be blackmailed by the fraudster who will threaten to share confidential information on medical conditions and treatments.

The insurance industry is consistently tracking emerging risks. As an industry, we have recently noticed a trend where fraudsters are targeting insurance companies using social engineering to obtain policyholder information. The fraudster poses as a member or broker to acquire personal information or to change contact details.

In 2020, the Experian credit bureau was hacked, which released information such as ID numbers, phone numbers and residential addresses of over 24 million South Africans.

For this reason, we need to make the assumption that our information could also be there and therefore adopt a zero-trust mindset by applying a healthy dose of scepticism.

Here are 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 have to call the medical aid, insurance company or your broker directly to verify the request.
- Never share identifiable information, policy numbers or claim numbers with strangers.
- Take extra caution when storing or disposing of any documents.
- Be cautious when clicking on links.

Anyone who is concerned that their ID number and personal data may have been compromised should request their free annual credit report and register with the Southern African Fraud Prevention Service (SAFPS), which provides protective registration for all consumers who have experienced identity fraud. The protective victim registration is a free service which is a step in the right direction to take precaution and safeguard your identity.

Steps to take following a data breach:

1. Check notifications

Read through the email carefully for any signs of a potential scam. Signs include spelling and grammatical mistakes and urgent requests for your personal information. Double check the email address of sender and don't click on embedded links.

2. Find out exactly what happened

Understand your risk exposure: Find out exactly what information has been compromised? Was the incident an accidental data exposure, or did malicious third parties' access and steal your data? What type of information may have been accessed? Was it encrypted? If your provider hasn't answered these questions adequately then call them to get the information you need to take the next steps. If it's still unclear, then plan for the worst.

3. Monitor your accounts

If malicious actors have accessed your Personal Identifiable Information (PII) and medical information, they may sell it to fraudsters or try to use it themselves. Either way, it pays to monitor for suspicious activity such as medical bills for care you didn't receive, or notifications saying you've reached your benefit limit. If financial information has been compromised, keep an eye on bank accounts and card transactions. Many organisations offer free credit monitoring, which notifies you when there are any updates or changes to your credit reports which could indicate fraud.

Make sure that your contact information is up to date and that you receive the medical aid claims notifications after visiting a doctor or pharmacy.

Make sure you receive notifications confirming any updates on your membership.

4. Report suspicious activity

It goes without saying that you should report any suspicious activity or billing errors immediately to the relevant provider. It is best to do so in writing as well as notifying your Scheme, insurer/provider via email/phone.

5. Freeze your credit and cards

Depending on what personal information has been stolen, you might want to activate a credit freeze. This will mean creditors cannot access your credit report and therefore won't be able to approve any new accounts in your name. That will prevent fraudsters running up debt in your name. Also consider freezing and/or having new bank cards issued. This can often be done simply via your banking app.

6. Change your passwords

If your log-ins have been compromised in a breach, then the relevant provider should automatically reset them. But if not, it might pay to do so manually anyway – for peace of mind. This will prevent account takeover attempts – especially if you enhance your security by way of two-factor authentication.

7. Stay alert

If fraudsters get hold of your personal and medical information, they may try to use it in follow-on phishing attacks. These could be launched via email, text, or even live phone calls. The aim is to use the stolen information to add legitimacy to requests for more personal information like financial details. Remain vigilant.

BE AWARE – REMAIN VIGILANT – REPORT SUSPICIOUS ACTIVITY

References:

https://www.welivesecurity.com/en/privacy/my-health-information-has-been-stolen-now-what/

https://www.fanews.co.za/article/fraud-crime/5/general/1094/identity-theft-on-the-rise-how-to-safeguard-yourself/39657