Advertisement

Most of us part with personal information far too easily! Due to the fast pace of life, we often just give out our information without even thinking about it. This provides fraudsters with opportunities to steal identities and commit fraud, which is why it is very important that you take responsibility for your own personal information, and manage it carefully.

WHY ALL THE FUSS?

Because being casual about sharing your personal information makes it easy for fraudsters to do the following:

- Attempt to acquire access to your retail or bank accounts.
- Defraud your insurance, medical aid or unemployment insurance fund.
- Impersonate you and do transactions using your bank account.

HOW DO THEY DO IT?

ID documents, passports, driver's licenses, salary slips, municipal bills, bank statements, till slips etc. all contain your personal information, which can be used to steal your identity, and your money. The digital age has provided us with many solutions, but has also created further opportunities for fraudsters to access personal information using clever tricks. Some of the ways they do this is by sending emails (phishing) or SMS's (smishing), purporting to be from trusted sources like your bank or other legitimate companies, in order to ask their victims for personal information such as passwords, ID numbers and bank card details. By responding, the victim is providing the fraudsters with the relevant information that enables them to commit the fraud.

Fraudsters are also experts when it comes to using social engineering techniques to obtain personal information. Vishing, which is "voice phishing", is where a fraudster phones you, posing as someone from a bank or a service provider, and manipulates you into sharing your confidential information with him or her over the phone.

PROTECT YOURSELF

With all these scams about, SABRIC provides you with tips to help you protect yourself:

- Don't carry unnecessary personal information in your wallet or purse.
- Don't disclose personal information such as passwords and PINs when asked to do so by anyone via telephone, email or SMS.
- Don't write down PINs and passwords and avoid obvious choices like birth dates and first names.
- When destroying personal information, either shred or burn it (do not just tear it and put it in a garbage or recycling bag).
- If you receive an OTP on your phone without having transacted yourself, it was likely prompted by a fraudster using your personal information. Do not provide the OTP telephonically to anybody. Contact your bank immediately to alert them to the possibility that your information may have been compromised.
- Don't use Internet Cafes or unsecure terminals (hotels, conference centres etc.) to do your banking.
- Should your ID or driver's license be lost or stolen report it to SAPS immediately.
- Use a separate email address for the internet which is not linked to your personal or business e-mail account.
- Make sure that your PC or mobile device is updated with the latest IOS updates and anti-virus/ malware software.
- Register for SMS notifications so that you are notified of any transaction on your bank account.
- Type in the URL (uniform resource locator or domain names) for your bank in the internet browser if you need to access your bank's webpage and never click on a link to access your bank's webpage.

Remember these tips and #SKELM

WISE UP. WATCH OUT.

SabricZA @Sabric SabricZA

WWW.sabric.CO.ZA

"FROM WHERE I'M SITTING I KNOW ALL ABOUT YOU"

#SKELM