SIMProject launched to protect Mobile numbers from being Hijacked

By Mikayla Fanto

Macquarie University has launched a research project focusing on the protection of mobile phones from unauthorised access to personal information.

The Australian Communications Consumer Action Network said one in five people in Australia will have their identities stolen or compromised in their lifetime. The criminals first get access to some personal information (date of birth, your address, mobile number, bank customer number, etc.), e.g. through mail theft or extracting information from social media. Then they use this information to take over your mobile number by pretending to be you and either conducting an unauthorized port or a SIM swap:

- For an unauthorised port, the criminal contacts a new Telecommunications company and pretends to be you (with the information they have gathered). They set up an account and then have your number ported to the new provider.
- For a SIM swap, the criminals purchase a SIM card, contact your current telecommunication provider pretending to be you. Then they request to have your number transferred to the new SIM card.

The criminal then has your mobile number and all messages (e.g. password reset links and confirmations, etc.) and calls go to them. This allows them to hack into your email accounts, bank accounts (if they have your bank customer number and do a password reset – that is typically confirmed via a OTP (one-time password) sent to you via SMS.

Researchers are working together at Macquarie University to raise awareness for their Antiport project.

Antiport aims to increase awareness of unauthorised mobile number porting and to help consumers protect their identities.

The team conducted workshops revealing many Australian's are susceptible to these attacks because they are not aware of the risks of mobile number porting.

Research Fellow at the Centre for Risk Analytics Dr Fabiola Barba Ponce said unauthorised mobile porting can have life-altering consequences.

"Victims can suffer increased levels of stress and anxiety, sleeping disorders and emotional responses such as anger and paranoia. In extreme cases, there have been signs of post-traumatic stress disorder," she said.

"Those who fall victim to identity theft during the uncertain times we currently live in have the potential to further exacerbate these symptoms and cause even more stress."
Dr John Selby said two-factor authentication by SMS can be attacked by identity thieves.

"Sophisticated criminals who gain access to a management layer of a mobile phone network known as Signalling System No.7 can intercept and read SMS two-factor authentication messages sent by businesses or financial service providers without having to do an unauthorised mobile phone port," he said.

Dr Selby said SMS messages are being sent in plain text (without encryption) over the mobile phone networks.

"As long as two-factor authentication with the use of mobile phones is the industry standard for resetting passwords for bank and superannuation accounts, email and social media accounts, criminals will still see huge benefits in fraudulent mobile number porting as they can gain quick and direct access to valuable parts of their victims' digital life for a period of time."

Professor Stefan Trueck said the AntiPort project will help reduce the number of victims of identity theft in the future.

"Recent prevention strategies assisting consumers to avoid poor choices and better protect their personal information have reduced the rate of these incidents by almost 30 per cent," he said.

Mr Trueck said the project will provide engaging tools such as an informational website, statistics and resources to help raise awareness of the problem and to help prevent future attacks.

"We believe the AntiPort project will help to reduce the number of Australians who fall victim to identity theft in the future."

For more information on the project and to gain further awareness, visit simprotect.com.au