Protecting yourself from phone porting and SIM card scams

ABC Everyday / By Patrick Wright

In April 2018, Stefan Trueck was driving home from the supermarket when he got a strange message on his phone.

"At 5:55pm, I got a text message from my telco. It said, 'Hi, received your port out request for this service,'" he says.

"By the time I tried to call them, my phone already went to SOS only. Before I could even react, my number was gone."

As it turned out, Stefan, a professor of business analytics at Macquarie Business School, was being scammed. Within an hour, criminals had reset his banking password and accessed his accounts.

"They had my customer ID [for online banking], and you can do a password reset if you have the customer ID and mobile number," he explains.

"It was really professional. I had daily limit of $10,000, so they sent $10,000. They bypassed that limit by opening another account inside my account, which you can do online, and then they transferred another $10,000."

Thankfully, Stefan quickly notified his bank and the transactions were reversed.

But the experience left a lasting impact. With the help of Macquarie University and the Ecstra Foundation, Professor Trueck set up SIMProtect, a series of online resources to help people avoid the scam.

"For me, it was relatively harmless. But they could have taken out a loan in my name, they could have reset all my passwords, they could have accessed my email accounts. So much harm can be done."

**How scammers are adapting to new laws**

Since Stefan was targeted in 2018, it's become harder for scammers to port phone numbers to new providers.
"If I want to change providers, before the [new] standard was put in place, I just had to give my name, my date of birth and my address," says Fiona Cameron, chair of ACMA's Scam Telecommunications Action Taskforce.

"We put a standard [in place] that said that's not enough.

"Now if I want to change my number, they will send me a four-digit PIN code, that will prove I have the device in my hand. It's upped the ante on the security that's required for changing telcos."

It's made it more difficult for scammers to transfer numbers to new providers, but they've found a new way to achieve a similar outcome.

IDCare, a not-for-profit organisation that supports victims of scams and identity theft, has received more than 850 reports of SIM card scams since the start of the year, with total losses of nearly $3 million.

David Lacey, IDCare's managing director, says nearly 80 per cent of new cases relate to SIM swapping — where scammers ask a victim's existing telco to switch the number to a new SIM.

"There is certainly a trend towards SIM swapping as opposed to intercarrier porting," he says.

"[That involves] a criminal going to the same telco and saying: 'I've lost my phone, I've lost my SIM card, can I get a new SIM and a new number', and the telco's compliant because they've got the relevant identity credentials to sail through the verification process."

Ms Cameron says this type of scam has been harder to stop.

"Remember there are a huge amount of retail service providers, certainly more than 300 in Australia, and some have better security provisions than others," she says.

Protecting yourself from SIM swapping and porting

To enable to SIM port or swap, scammers will need personal information, like your name, address, and date of birth.

In Stefan's case, scammers found this information by accessing his mail. In other cases, the scammers may be able to find the information online from social media accounts. Dr Lacey says scammers may also be able to find information online from data breaches by hackers.

The simple message from Stefan? Take extra precautions, such as setting up a password or PIN with your telco provider, and be very careful about sharing your personal details.

"Have as little personal information on social media as possible," he says.

"It's probably not a good idea to have your address, date of birth or telephone number on Instagram or LinkedIn."

Dr Lacey says many victims have their email accounts hacked.

"Almost in every case we see that trifecta of the email account, the bank account, and phone number," he says.

To protect your email and other online accounts, use strong passwords — ideally generated by a password manager — and never re-use old passwords.

The reason? If just one of your accounts has been hacked, it could put all your accounts using that password at risk.

"For many of the clients who say they have no idea how the scammers got their details, we can see their email accounts, usernames and passwords have been caught up in breaches and they haven't changed the email account password.

"[In those cases] the criminals have got into the email first to start harvesting data about that person."
On top of that, Dr Lacey recommends always using **two-factor authentication**, especially for important logins like your email. Consider using an authentication method other than a text message, such as a verification app or key.

To get around the increased restrictions on SIM porting, scammers may impersonate your telco to get the verification code.

Dr Lacey says these "**man-in-the-middle**" attacks are becoming more common.

"To port the number, for example, some telcos might require an authentication code. The criminal knows that. They also know the number of the person they're trying to exploit," he says.

"They'll arrange for that code to be sent via text, then the criminal will call the victim and impersonate the telco and say, 'Look, I noticed that there has been some unauthorised access on your account. We've sent you a verification code, can you confirm that to me?'"

To verify the request, you can always call back the telco yourself.

**What to do if you suspect you've been scammed**

- Immediately contact your telco provider
- Report the scam to your bank or financial institution, local police and ASIC
- You can also report the scam to the **ACCC's Scamwatch**. The ACCC can't help you recover your money or track down a scammer but your report may help prevent future scams
- Further information is available from **SIMProtect**, **IDCare** and **ACCAN**