Hot issues

Fraudulent mobile number porting and identity theft

Recently ACCAN has heard increasing reports about fraudulent mobile number porting and identity theft.

What is a mobile number porting scam?

Fraudulent mobile number porting happens when a scammer uses your personal details to port your mobile number from one provider to another. Scammers can get access to your personal details, such as your date of birth, phone number and address, via your social media profiles.

Scammers then use your mobile number to gain access to email accounts and bank account details. Once your number has been ported, you no longer have access to it which means that any verification codes being sent to you by your bank for large money transfers will be sent to a scammer instead. This means they can authorise these transfers and steal money from you.

Earlier this year two telecommunications industry union officials fell victim to a number porting scam, which eventually resulted in one of the officials providing his bank account details to the scammer. Since then, ACCAN has received two additional first-hand accounts from victims of this type of fraud, with one victim having lost a substantial sum of money.

This is very concerning as these scams can be quite detrimental to consumers. The implications of fraudulent number porting for consumers can be very serious and include but are not limited to financial loss, negative credit ratings, and emotional stress. Once a consumer has had their identity stolen, it can be very difficult and time-consuming to reverse the effects.

In this blog post we have included information on how to tell if your number has been ported and tips on what you can do to protect yourself from number porting scams. ACCAN has also contacted relevant telecommunications industry bodies to discuss consumer protections against fraudulent number porting and identity theft.

How to tell your number has been ported

- A sign that your number has been ported is that your phone will show ‘SOS only’ where the reception bars usually appear.

What to do if you have been scammed

- Contact your mobile provider. They will be able to tell you whether your number has been ported. If it has been ported by a scammer, ask them to port it back.
- Contact your bank to see whether scammers have accessed your bank account. Let your bank know of any fraudulent transactions straight away.

- Change your passwords on your online accounts for social media, banking, emails and other important accounts.
- Scammers may try to steal personal information from your close contacts using your accounts. It is a good idea to let your family and close friends know to watch out for strange emails and messages sent from your account if you have been scammed.
- Report the scam to Scamwatch and the Australian Cybercrime Online Reporting Network (ACORN).
- For help with identity fraud, you can contact IDCare.

What can you do to protect yourself?

1. Ask your mobile provider and your bank to set up a secret pin number or password that only you know, to identify yourself when you call them or deal with them in person.
2. Check your social media profiles on Facebook, Twitter and LinkedIn to ensure your mobile number is hidden from public viewing (remember to check resumes and work documents that are available online). Also, find out if your mobile number is listed online anywhere and have it taken down. You can do this by Googling your mobile number. This may not be practical for small businesses that rely on social media and websites to attract business.
3. Remove your birthdate from public view on social media. Use a fake birthdate when you sign up. Do not use real personal information for security questions; make up a best friends name or mother’s maiden name. Remember a scammer can work out your birthdate from photos of birthday celebrations, or a happy birthday message from a friend.
4. Create strong passwords for your online accounts and use different passwords for different accounts. If you have lots of online accounts, consider using a password manager. More information on this is available in our tip sheet.
5. Wherever possible, use two step verification to login to your online accounts. Two step verification is when you are sent a verification code that needs to be entered before you can login to an account. The code is usually sent to a mobile number or email address.
6. Scammers can gain personal information about you by stealing your physical mail. Make sure you have a lock on your physical letter box, and keep your home street address offline. Google your address alongside your name to see if it is listed anywhere. For small businesses, it may not be desirable or practical to remove online addresses.
7. Be security conscious on Facebook and online generally. Do not list your family’s names online anywhere; if you have connected them in your Facebook profile hide or delete these links. Hide your friends list from public and friends’ view. If a scammer can see your friends list, they can then copy your Facebook profile to impersonate you, and then approach them using a fake profile. Never accept a friend request from someone you are already friends with on Facebook as it may be a fake profile.
8. Install anti-virus software on your computer, tablet and smartphone to ensure your devices are protected from hackers. Regularly run anti-virus scans. Ensure that the software for your anti-virus and operating system are up to date.

These tips first appeared in a blog post by the Cybersafety Lady. Check out the original blog post here.