SIM Swapping

Fraudsters are using SIM swapping and phone number porting to gain access to your email, social media and financial accounts. From there, they gain direct access to your personal information, calendar, contacts, money, and then some. Fraudsters may empty your bank accounts, apply for credit in your good name, or impersonate you to defraud your entire contact list. In the meantime, you lose access to your mobile service, are typically locked out of all your accounts, and are left scrambling.

Here's how it works:

Your SIM card connects your phone number & mobile service to your mobile device. You connect dozens of your accounts to your mobile device through the use of applications. Most application logins are linked to your email address, phone number or both (if you setup two-factor authentication).

A fraudster will impersonate you to gain access to your mobile account and may claim that their phone has been lost or stolen. Your phone number will be linked to a new SIM & device that the fraudster controls.

The fraudster then downloads a series of the most popular and most attractive applications. They will select the 'Forgot Password' button on all applications. If an account is associated to your phone number or email address, the fraudster will receive a verification code. They will then use this code to confirm ownership of the account, create their own password and takeover the accounts.

Warning Signs – How to Protect Yourself

- Keep your personal information personal. It is as simple as not publishing your date of birth on social media.
- Do not answer phishing emails or text messages looking for you to confirm your password or update your account information.
- Use an offline password manager.
- Contact your phone provider and ask about additional security measures that may be available.
- If you lose mobile service on your device, contact your service provider immediately.

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1- 888-495-8501 or report online at www.antifraudcentre.ca.