SIM card swap scam

Fraudsters are using SIM swapping and phone number porting to gain access to your email, social media and financial accounts. From there, they could gain direct access to your personal information, calendar, contacts, money, and then some. With some of your additional personal information fraudsters may attempt to gain access to your banking, 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 and mobile service to your mobile device. You may connect some 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 and 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. For example, publicly displaying your birthdate on websites or social media increases risk.
- 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 (avoid storing passwords in/on your Smartphone, unless they're encrypted).
- 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.
- Our Swan Valley Credit Union online banking/mobile app has "Alert" functionality. Please ensure you have Account Activity Alerts set up to notify you by both email and text message.

Am I Covered?

- Fraud is handled on a case-by-case basis. In general terms, members are protected for fraud beyond their reasonable control, provided they don't contribute to or benefit from the fraud, and they cooperate fully with the investigation
- As above, don't save your passwords online or in your smartphone (similar to how you protect your PIN for your debit card)