SIM Card Takeover

Scheme

A SIM card connects your phone number and mobile service to your mobile device. A criminal's objective in the SIM card takeover scam is to gain control of your mobile services by linking it to a new SIM card, which is in a device that they have control over. Once a SIM card swap has occurred, criminals receive all incoming SMS text messages and phone calls sent to your phone number. From there they can download various popular apps, including online banking apps, and reset passwords by selecting the "forgot password" option. When a request to reset password is made, many apps send an SMS one-time verification code to the cellphone number on file to verify ID. In this scheme, the criminal receives this one-time code and can use it to gain access to the account and transfer out funds.

Credit Union Experience

- Canadian credit unions have been the subject of SMShing campaigns where victims are directed to spoofed websites and credentials harvested.
- In addition to credentials, members have been asked to input DOB, SIN, and answers to security questions etc.
- Through the SMShing attack, the hacker uses the harvested information to socially engineer the member's telecommunications company and have the member's number ported to a new phone and SIM card.
    - Hacker then quickly completes fraudulent transfers.
- In some instances, credit unions were notified by Interac that there was suspicious e-transfer activity.
- When credit unions called the members (from information they had on file), the staff were advised by the person on the other end that these transactions were legitimate.
    - In fact, these transactions were not legitimate, as staff were talking directly to the hackers.

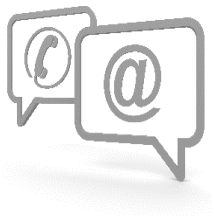
www.eagleriverCU.com

8 Branch Rd PO Box 29
L'Anse au Loup, NL A0K 3L0

Tel: (709) 927-5524
Fax: (709) 927-5018

How can members protect themselves?

- Avoid publishing personal information on social media (e.g. date of birth, telephone number, postal code, spouse's name etc.).
- Advise members that your credit union will never contact them in an unsolicited manner and ask for personally identifiable information (PII).
- Educate members on SMShing scams.
- Members should be encouraged to increase the security around their telecommunications account.
    - Add a PIN to account.
    - Add a secret word to account.
    - Some telco providers offer voice authentication as a security option. This option should be leveraged where possible.
    - Ensure your account is not validated by simply providing postal code and DOB (this is the default for some providers).
    - Turn on instant SMS and email notifications of account changes.
- Use an offline password manager.



For more information, please contact Eagle River Credit Union at:
1-877-377-3728