Cybersecurity Digest

Bi-Weekly Digest by the CISO Section of Meghalaya Rural Bank

Volume 2 Issue 6 **Date: 16-06-2025**

SIM Swapping Fraud

Unauthorized SIM changes, sometimes called SIM swapping or SIM hijacking attacks, occur when a customer's phone number is transferred to a different SIM card or eSIM profile under the control of a criminal. If the SIM swap is successful, the criminal may intercept the customer's phone calls and text messages to receive one-time security codes from social media, banks, credit card companies, cryptocurrency exchanges, and other financial institutions, allowing them to potentially access those accounts and cause financial and reputational harm to the customer.

But, not all SIM changes are bad! Authorized SIM swaps may happen when you upgrade your device, or when you troubleshoot or replace a lost or stolen device.

Criminals typically use SIM swaps as a way to steal your phone number so they can access your bank or other financial accounts. They often start by gathering as much personal information about you as they can from social media, the Internet, the dark web, previously compromised accounts, and directly through phishing. They use this information to pretend they are you, in an effort to gain access to your account and transfer your mobile number to a different SIM card or eSIM under their control. Once they've "swapped" your SIM, calls and texts to your phone number route to the phone in the criminal's control. At that point, the criminals can use their phone to receive one-time security codes or calls that banks and other companies use to safeguard customer accounts. In some cases, you might not know this has even happened until your phone no longer works.

SIM Swap Scam—Causes

Understanding the underlying causes of SIM swap scams is crucial for identifying vulnerabilities and implementing effective preventive measures. Following are the causes of SIM swap scam:

Social engineering: Scammers use various techniques to deceive victims and mobile carrier employees into believing they are the legitimate owner of the phone number. This can involve phishing emails, calls, or text messages to collect personal information.

Data breaches: Large-scale data breaches can provide scammers with the necessary information to impersonate victims This data can include names, addresses, social security numbers, and phone numbers.

Insider threats: In some cases, scammers may bribe or coerce employees within mobile carrier companies to facilitate the SIM Swap.

Weak security practices: Mobile carriers sometimes have insufficient security protocols for verifying identity before transferring a number to a new SIM, making it easier for scammers to execute their schemes.

Signs you might be a victim of a SIM swap scam

- **Sudden loss of service:** If your phone suddenly loses service and displays " No Service" or "Emergency Calls Only", it could be a sign that your number has been transferred to another SIM.
- **Inability to make calls or send texts**: If you can no longer make calls or send texts, it might indicate that your SIM card has been deactivated.
- **Unusual account activity:** You might receive notifications of unusual login attempts or password changes from your email, bank, or social media accounts.
- **Receiving messages about SIM card changes**: If you receive notifications from your mobile carrier about SIM card changes that you did not initiate, this is a red flag.
- **Access denied to accounts:** If you are suddenly unable to access your bank accounts, email, or social media accounts despite entering the correct passwords, it could be a result of a SIM Swap.

How to protect yourself from SIM Swap Scams

Protecting yourself from SIM Swap scams involves strengthening account security, limiting the sharing of personal information, and staying vigilant for suspicious activities. We can reduce the risk of falling victim to this form of identity theft by taking the following proactive measures:

- **Enhance account security**: Use strong, unique passwords for all online accounts and change them regularly. Avoid using easily guessable information such as birthdays or common words.
- **Enable two-factor authentication (2FA):** Use 2FA methods that do not rely on SMS-based codes. Consider using the authenticator apps or hardware tokens instead.
- **Be wary of phishing attempts**: Do not click on links or download attachments from unknown or suspicious emails and messages. Verify the sender's identity before responding.
- **Monitor your accounts**: Regularly check your bank, email, and social media accounts for any suspicious activity. Set up alerts to notify you of any unauthorized transactions or changes.
- **Contact your mobile carrier:** Ask your mobile carrier to add a PIN or password to your account for an extra layer of security. Some carriers also offer the option to disable remote SIM swapping entirely.
- **Use identity protection services:** Consider using identity theft protection services that monitor your personal information and alert you to potential threat.
- **Report suspicious activity**: If you suspect you are a victim of a SIM swap scam, contact your mobile carrier immediately to restore your service and secure your accounts. Additionally, report the incident to your bank and other relevant institutions.