Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

SIM Swapping

SUMMARY

SIM swapping, also known as SIM hijacking, occurs when a fraudster transfers a victim's phone number to a new SIM card. Using personal information gathered through phishing or social media, the fraudster impersonates the victim and convinces the mobile provider to make the switch.

Once in control, the attacker can intercept messages and calls, including security codes, allowing access to online accounts, password resets, and financial information.

SIGNS OF SIM SWAPPING

If an accountholder reports account takeover fraud but insists they didn't share their information, they may be a SIM swap victim. Warning signs include:

- Inability to place calls, send texts, or access certain accounts
- Alerts about changed login credentials for banking, email, or social media
- Loss of signal or phones stuck in "roaming" mode
- Unexpected PIN messages from their mobile carrier

WHAT IS AT RISK?

- **Financial Access**
  - Online banking and investment accounts
  - Payment apps linked to the device
- **Digital Identity & Online Assets**
  - Social media accounts
  - Domain names and digital handles
- **Device Access & Stored Data**
  - Apps and locally stored information
  - Contacts
  - Security codes and messages
- **Personal Information**
  - Name, address, date of birth, and other PII

MITIGATING SIM SWAPPING ACCOUNT TAKEOVERS

- **Strengthen Authentication**
  - **Avoid SMS-based 2FA:** Opt for more secure methods:
    - Authenticator apps (e.g., Google Authenticator, Authy)
    - Biometric authentication (fingerprint or facial recognition)
    - Hardware security keys
  - **Risk-based authentication:** Use tools that monitor behavior and trigger extra verification when activity seems suspicious.
- **Enhance Verification Processes**
  - **Account changes:** Require multi-channel identity checks and out-of-band verification for changes to addresses or phone numbers, according to Medius.
  - **Transaction monitoring**: Flag unusual activity for further review.
  - **SIM swap detection:**
    - Use mobile carrier APIs to detect recent SIM swaps
    - Automatically flag affected accounts for added scrutiny
- **Educate and Empower Customers**
  - **Raise awareness:** Help customers understand SIM swapping risks and prevention.
  - **Promote SIM protections:** Encourage enabling SIM lock features from major carriers:
    - Sprint/T-Mobile
    - Verizon
    - US Cellular
    - AT&T
  - **Encourage strong security habits:**
    - Use unique, complex passwords
    - Enable MFA on all accounts
    - Stay alert for phishing attempts
  - **Freeze credit reports:** Recommend placing a freeze to prevent fraudulent loans or new accounts.

RISK MITIGATION RESOURCES

- Fraud in the News: Man Lost $21k in SIM Swap Scam
- Helpful links:
  - Sign up for our **Let's Talk Fraud** quarterly webinars
  - View additional risk resources

Need assistance or want to request a consultation?
Contact our risk specialists atrisk_specialist@alliedsolutions.net