Sim Swap Fraud: A rising threat on the risk management horizon

August 2022 Newsletter

19th Edition

RMG

Table of Contents

What is Sim Card Fraud?

Since 2017 there has been a rise in the media on reports of Sim Card Fraud. This relatively new type of commercial crime is known by a myriad of different names, including but not limited to: Sim Jacking, Sim Swapping, Port Out Scams, and Sim Splitting but all of these names describe the basic actions of account takeover fraud that generally will exploit a weakness in multi-factor authentication.

Social engineering tactics of hackers and scammers are an ever-evolving, mutable constant that keeps up with digital security trends. A good analogy is a wall of security controls, and scammers try to breach this wall by adding rungs to their repertoire. By exploiting the SMS function in most two-factor authentication systems, the scammer needs to go to the service provider, in the case of contracted services, and be able to impersonate the rightful owner of the sim card. IdropNews states that are numerous reasons a sim card can be legitimately reissued such as the SIM card has been lost, destroyed, or stolen, but using identity theft and social engineering techniques such as Smishing and Phishing criminals can gain entry to sensitive information or systems.

To successfully pull off Sim Swop Attack, commercial criminals require some of their intended victim's personal information. Comparitech states that this personal information is obtainable through obtaining information relating to data breaches, social engineering schemes, and targeted digital attacks. The more information that the criminals can obtain on their intended victim the higher the likely hood that the attack will be successful.

Because not all criminals have the capacity to pull off multi-million currency commercial crime heists, some of the easiest ways sim jackers obtain information are through trolling social media to gain insight into the victims' life in order to impersonate them with ease.

A sim card or subscriber identity module card is used as storage for user data in the Global System for Mobile (GSM) devices, such as mobile phones. If a sim card is put into a non-GSM phone it will be unable to gain network access. These numbers are used in various industries using two-factor authentication that requires access codes that are sent to mobile devices for system access.

The steps of the attack

A Sim Swopping attack usually happens in steps that are outlined by Privacy Pros:

1. A victim is selected and targeted. During this phase of the attack the attacker collects as much personal data as possible through social media trolling, phishing attacks, malware, or even using the dark web to gain access to details.
2. The attacker impersonates the user and requests the activation of a fresh sim card. This is usually performed by calling or interviewing the sim card's service provider. Alternatively, criminals may ask for assistance in switching to a new mobile device.
3. The attacker gains access to resources, bank accounts, and other information that would make use of an SMS for two-factor authentication.

Prevention methods are further outlined by Privacy Pros, however, there is currently no fool proof method that will fully nullify the risks of sim card fraud. It is better to educate and prevent fraud than to deal with the sometimes-irreparable damage that commercial criminals can cause.

1. Educate employees about phishing scams, phishing, and smishing scams are common data collection methods that cybercriminals employ.
2. Regularly update account security, this can include using strong passwords, and further using questions and answers that

only a few individuals would have access to.

3. Add another pin code if mobile carriers allow users to choose a different passcode or PIN for communications.
4. Selecting companies that use call-backs, which is a process in which companies call customers back on a registered number to ensure that they are speaking with the relevant individual before accessing or changing accounts. This has been proven to be an effective way to keep accounts safe and identify identity thieves.
5. Making use of hardware authentication devices such as Yubikey. This is a small electronic USB device that plugs into a computer to help confirm the user's identity. Using a physical device, along with a password and turning off the SMS features will force scammers to have to steal the device and makes sim swopping a very unlikely scenario.

Forbes has reported that MitM attacks are a branch of Sim Swopping that criminals may employ. This method involves cybercriminals tricking users into visiting a fake website where the user enters credentials and triggers a multi-factor authentication request. Once the user has confirmed the push notification on their mobile device, the cybercriminals are able to intercept the authentication code and gain account entry. Further, the FBI has warned individuals through a report that was sent out in 2021 that the best measures to mitigation of Sim Swopping are prevention by not advertising information about financial assets on social media websites, and not providing a mobile number or account information over the phone to representatives on inbound calls. It is wiser to phone back by dialling the customer service line of the service provider and verifying the callers' identity. The FBI report recommended that users never store passwords, usernames, or other personally identifiable information on mobile apps if they can avoid it.

Indications of Sim Card Fraud

This Day Live has reported that according to data from the South African Banking Risk and Information Center (SABRIC), SIM swap-related fraud increased by 100 percent in South Africa between 2018 and 2019, with other African nations having an even higher percentage of increases. This shows that Sim Card Fraud has trends that it targets developing world nations that rely heavily on the internet and mobile GSM services.

Apart from preventative steps that users can take to prevent themselves, it is important to track activity to spot any anomalous traffic in accounts. Both Privacy Pros, ZD Net, and This Day Live Report that the best plan of action, once this has been identified, would be to contact the relevant service providers and confirm that an incident of sim scamming has occurred. There may be processes that the service provider would follow to verify the identity of the person calling in the commercial crime incident, but most large institutions are aware that identity thieves would not easily report fraud.

Vodacom and Nedbank have reported the “tips” to deal with sim card fraud on their webpages that include receiving SMS that a sim swop request is pending, or if someone (usually impersonating the service provider) will phone users to tell them to ignore such an SMS, or if the user suddenly stops receiving traffic on their Sim card, and that sim card will no longer be able to gain access to the network. The main recommendation from these service providers is to contact the service providers customer support line immediately to gain clarity on the issue or to raise the alarm that an incident of Sim Swopping has occurred.

Comparitech and Incognia has reported that users may notice social media posts on their accounts that they had never posted, and if a user can no longer log into their accounts as the user credentials have been changed. Further, it is reported that if such anomalies are identified, the user must check their credit card, bank, and other financial accounts for other possible unauthorized transactions or changes.

Examples of Sim Card Fraud

No-one individual is exempt from sim card fraud, as cyber criminals will target rich and poor indiscriminately. If someone has a sim card, they are immediately subject to sim swopping – even if it could be for chaotic purposes as evil does not require a purpose to lurk within the depths of man. Verizon has reported through Forbes that their research has estimated that 82% of all cyber attacks occur due to human errors that can stem from stolen credentials due to lax security, falling for phishing scams or misuse of hardware and/or hardware protocols.

Security Boulevard has reported an **example** of Sim Swopping where in 2021 a 24-year-old New York man who had bragged about assisting in the theft of over $20 Million worth of cryptocurrency from the technology executive Michael Terpin. The accused individual, Nicholas Trugulia, was part of a group who were alleged to have stolen several tens of millions through the user of Sim Swopping.

Michael Terpin has filed a civil lawsuit against Truglia with the Los Angeles Superior

Court, in which he was awarded a $75,8 Million judgement against Truglia. Though it is unknown how the threat was identified, and the theft localised to one individual, it can be said with certainty that these cybercriminals made use of Sim Swopping to finance their nefarious deeds.

A **second example** of sim swopping was reported in 2022 by Newsweek, where a Florida man has lost more than $700 000 after being targeted by a Sim Swopping scam. This follows the 2021 FBI report on Sim Swopping. The victim, Dan Clark, had stated that his phone read “no service, SIM Card”, and that he did not even know what a sim card was before the incident. The attackers had managed to drain the account of Dan Clark in a few hours and as of this report there is an ongoing investigation by the FBI into this case.

The **third example** comes from ITweb about an incident that had happened in South Africa where a woman had discovered her cell phone had no network. When the woman had enquired upon this by the service provider, she was informed that someone had done a sim swop on her number. Within a month she discovered that she had lost more than R179 000 after several fraudulent transactions. The matter was thereafter reported to the Hawks for investigation. The suspect, Enoch Khumalo, was arrested by the Hawks in 2022 for these allegations. MTN SA was listed in the article for stating that there has been a number of data breaches within South Africa that had resulted in personal information being made available to fraudsters. And that this information is being used regularly to exploit consumers of large-scale corporations.

Once again going back to the 2021 FBI report, it is warned on Make It that victims had lost $68 million within 2021 to Sim swopping scams, compared to the $12 million in the three year period between 2018 and 2020.

The biggest and most well-known example of sim swopping that occurred in 2019 targeted Jaco Dorsey, a twitter executive as reported by The Verge. A group of cyber criminals, known as the Chuckling Squad, had gained unauthorised entry to Dorsey’s account to post offensive messages. Within 15 minutes the accounts were back under

control, but the incident is a sharp reminder of the serious vulnerabilities in even the highest-profile accounts. These cybercriminals had gained entry through Twitters text-to-tweet service, which is operated by CloudHopper. As a result of this link, the cybercriminals were able to use sim swopping to gain access to Dorsey's accounts.

Conclusion

By taking preventative, and contingency measures, users can provide some degree of protection against sim swopping. Further, by performing proper financial tracking and account review users can protect themselves from cybercriminals through early identification. There does not currently exist any fool proof measure that protects against Sim Swopping, but education threats in the Information Security function may save a business should an employee fall prey to commercial crime that can spread like a canker throughout the business.

Bibliography

Wikipedia
Comparitech
Privacy Pros
This Day Live
Vodacom
Forbes
RMG
IdropNews
Nedbank
Security Boulevard
Newsweek
ITweb
Incognia
Make It
The Verge