International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Awareness of Sim Swap Attack

Snehal Manohar Awale[1], Dr. Praveen Gupta[2]

[1]Student, [2]Professor
[1,2]YMT College of Management, Navi Mumbai, Maharashtra, India

How to cite this paper: Snehal Manohar Awale | Dr. Praveen Gupta "Awareness of Sim Swap Attack" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.995-997, URL: https://www.ijtsrd.com/papers/ijtsrd23982.pdf

IJTSRD23982

ABSTRACT

This paper presents the awareness of Sim Swap attack among people and prevention of this attack, where the fraud person will Gain the personal information of person from different ways like fake call , sms ,Email, link, social media etc. mobile number is linked with bank and adhaar card the fraud person will gain the access of Bank account, credit card number and other personal information easily by trying various methods like MNC, Phone call, Hacking .It is difficult to undo the damage occurs.

Keywords: *SIM swap, Cyber attack, prevention*

INTRODUCTION

SIM swap is technically new form of cyber fraud where hackers gain the personal information and does illegal work with persons bank account, credit card numbers. This SIM swap attack is reported in US and Europe in 2013 and now this attack is the trend in India.

Now a days , most of the banking services are available on mobile phone for doing online transaction it needs One Time Password(OTP),Unique Registration Number(URN) which is provided through registered mobile phone number of person.

Fraud person sends phishing mail of companies/health insurers to get the legal information of person like name, date of birth, address, phone number which is their target. They collect the information from social media platforms or any other phishing link, social engineering via phone call, sms etc.

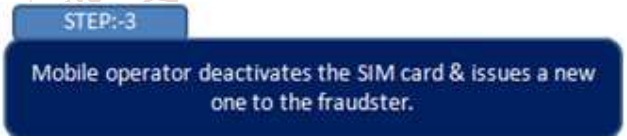
Next, fraud person will call mobile service provider of victim & request a new SIM card claiming that they have lost mobile phone, or damaged SIM card. Using the gained data the fraud person will manage and get a new SIM card issued for the registered mobile number of person. Once a new SIM card is issued, the service providers deactivate the old SIM card and from that time victim will not receive any SMS on their phone and once fraud person accessed mobile number the start doing fraud on bank accounts etc.

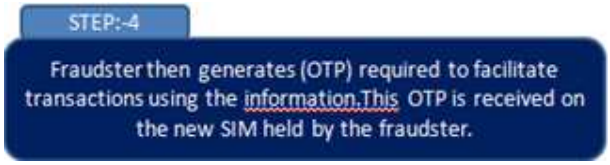
Sim Card

Its a small chip used in mobiles for telecommunications and identification and storing of contacts. It has limited memory storage.

Sim card comes in different sizes and if removed from mobile you cannot text,call or do anything on internet.
Its limited size is safe for mobile phone to insert and remove from the given slot.

Following are the steps how sim swapping happens:





Prevention from sim swap

- Don't share personal details on unknown call.
- Don't follow unknown sms ,Email,
- Unknown link in which https is not provided ,never open or browse that link.
- Never install Untrusted application.
- Set PIN or passcode for the SIM card.
- For securing online accounts SMS codes are not the most secure so instead use authenticator app such as Google Authenticator which are tied to phone number & generate unique codes for short time intervals.

- Never give details if any call from company or network operator regarding offers,system upgration,OTP etc.
- Don't give your personal information on social media.

Sim Swap techniques

1. MNP(Mobile Number Portability).[1]
2. Phone Call.
3. Hacking.

1. MNP:-

Converting from one mobile number of network service provider to another network service provider to any area in India by maintain the same mobile number.

Steps to port your mobile number:

1. Initial Preparation before initiating the MNP Process.
2. Request to operator to make the change and give the facility.
3. Approval from operator based on eligibility.

Signs of sim swap fraud:

Once SIM criminals will gathered enough information anyhow and generate the false identity,they will call victim's mobile phone provider and declare that the SIM card has lost or damaged. but the provider will not accept that request unless callers answers the security questions, but criminals are will prepared by already gained will personal data they collectecd across web.

Once they access phone number ,then criminals will target victims back accounts and also read sms and checks that with whom you are chatting. Many banks send the code to reset password to mobile phone by sending sms,and so the detailed access is already taken by attacker they can request and receive the code and access bank account.

Benefits of the MNP process

- **Freedoms of choice**: A user is free to choose a new operator without having to change to a new number.
- **Economic feasible**: Here you can notify the friends and tell them that you have changed your Mobile Number.
- **Generate competition**: When you don't get satisfactory service from service provider, then you can choose to change your operator and this is done by MNP Process. So, not to lose customers, service providers are forced to put up their best front.

SIM swap attack Process

It's a new cyber fraud for hackers to retrieve the details of particular person and take its access of bank accounts,credit card numbers,and other personal data so that this details are used for different illegal purpose.It is the latest technique to cheat mobile users.

In this sim attack, the attackers need some basic information to do attack and achieve its target.Phone number is very important component for this attack and also nned enough about the victim such as its home address or Social Security Number,and claim that he is a victim and convince a mobile provider that they have lost their SIM card and want to transfer the same number to a new SIM.

In cyberattacks the process of phishing,the SIM swappers will carry out their attack without directly involving the target.Means the victims will realize they have been the target of this attack only when their phone suddenly loses its connection to the carrier.till that it is very late.

Effect of SIM swap attack:

Every one of us have multiple email, social media accounts, messaging and other online accounts, bank accounts and credit cards. These sevices are link to a mobile phone for two factor authentication and for recovery purposes. Its a very damaging attack.

Application such as WhatsApp, Viber, Telegram which require a mobile phone number for the initial setup. That means the attacker will gain all the access to your phone number even if you have set the two factor authentication on the account.

Because of collecting the personal information of person the fraud person will misue the information for online fraud.

Cases of SIM Swap attack:

First Case:

Pune Man loses Rs 93.5 lakh in SIM swap fraud

In this the victim Dinesh kukreja got a call from hacker posing as Airtel staffer.

- He asked Kukreja to share details pertaining to his SIM card.
- Kukreja gave him details of the SIM linked with his bank account.

According to report by Hindustan Times,Dinesh kukreja got a call posing an airtel staffer.The man asked kukreja to share his information else his SIM card would get deactivated. Then he shared the details of SIM card what was linked with his bank account.

The fraud person asked kukreja to send the SMS that he had received to his mobile number.This enabled the fraudster to render kukreja's SIM card unless.This fraud person then got a new SIM card with same number and now has access to kukreja's linked bank account.

Soon after kukreja got to know that a sum of Rs 93.5 lakh had been transferred from his bank account.

Kukreja complaint with Bharti Vidypeeth police station.The police has registered according to Indian Penal Code and relevant sections of Information Technology Act.

Second Case:

The San Francisco Division of Federal Bureau of Investigation (FBI) has known the danger of this attack.

Hacker gain control of victims mobile number by porting with new sim card and once it is done they proceed to use the newly found access and resets the victims onlin accounts such as email, social media, cryptocurrency exchanges ,hacker lock the email and social media accounts to stop the owner to regaining control, and ask for the money from their digital currency accounts to be paid in bitcoin for unlock the accounts.

So FBI wants to help victim and quickly regain their accounts to prevent from damage occurs, FBI and our local law enforcement partners will investigate and bring these criminals to justice.

Conclusion and future enhancement:-

This paper will give awareness to the people about this attack.As this is increasingly daily. how this attack occurs in sim on mobile phone and how to protect yourself form this attack.This soloutions will help people from becoming the victim of sim swap attack.

References:

[1] https://www.techopedia.com/definition/23747/subscriber-identity-module-card-sim-card

[2] https://timesofindia.indiatimes.com/business/india-business/what-is-a-sim-swap-fraud-what-are-the-safety-tips/articleshow/67377708.cms

[3] https://www.knowlarity.com/blog/guide-mnp-process

[4] https://www.knowlarity.com/blog/guide-mnp-process

[5] https://bitsonline.com/fbi-warns-sim-swapping/