Hack SIM: Things to know and how to avoid

Illegal entry into SIM cards or SIM exchanges has existed for a long time ago.

As we all know, the two-factor authentication (2FA) applied is a good way to keep an online user's account safe.But technology is still evolving every hour and every minute, and if this feature is sometimes surpassed it is not difficult to understand.Illegal entry into SIM cards or SIM exchanges has existed for a long time, but when our financial information and transactions are becoming more and more online. Nowadays, this problem has become much more common.Often, hackers will steal your phone number and use it to access related accounts (primarily financially).Every story becomes more and more difficult as phone service providers appear too slow and passive in strengthening their security process and because 2FA applications still have some problems. .It seems that we are still running to deal with hackers and not necessarily prevent them from being remote.

How does the process of hacking SIM cards take place?

1. Search for goals

Searching for a target is the foundation in the process of hacking SIM cards.First, attackers will conduct the collection and analysis of some personal information about potential targets.All personal data from bank login information to age, workplace, social status . It is worth mentioning that this type of information can be found online.If attackers need more information, they can use a phishing attack to trick users into revealing important personal data.

2. Phishing support techniques

After finding and identifying potential prey, hackers will now map out a specific strategy.They will call your service provider (too easy to find the operator's phone number), use the information they know about the victim to overcome security and love questions. ask the service provider to transfer the phone number to a new SIM card.With a bit of other social knowledge, hackers can completely trick the tech support representatives into sending their phones to their phones.

3. Exchange SIM card

If the second step succeeds, the service provider will provide the victim's number and SIM to the attacker, and the user may (or may not) receive a message stating that their SIM has been Update or deactivate.After that, they will not be able to make calls or send messages anymore, at that point everything was out of control.

4. Access to online accounts

When the victim's phone number is under the control of the attacker, they can use that phone number to gain access to the relevant account by using 2FA capabilities or using numbers This phone to reset the account's password.Once you have the victim's phone number in hand, hackers usually only need to know their email address and maybe some personal information that can capture that personal account.

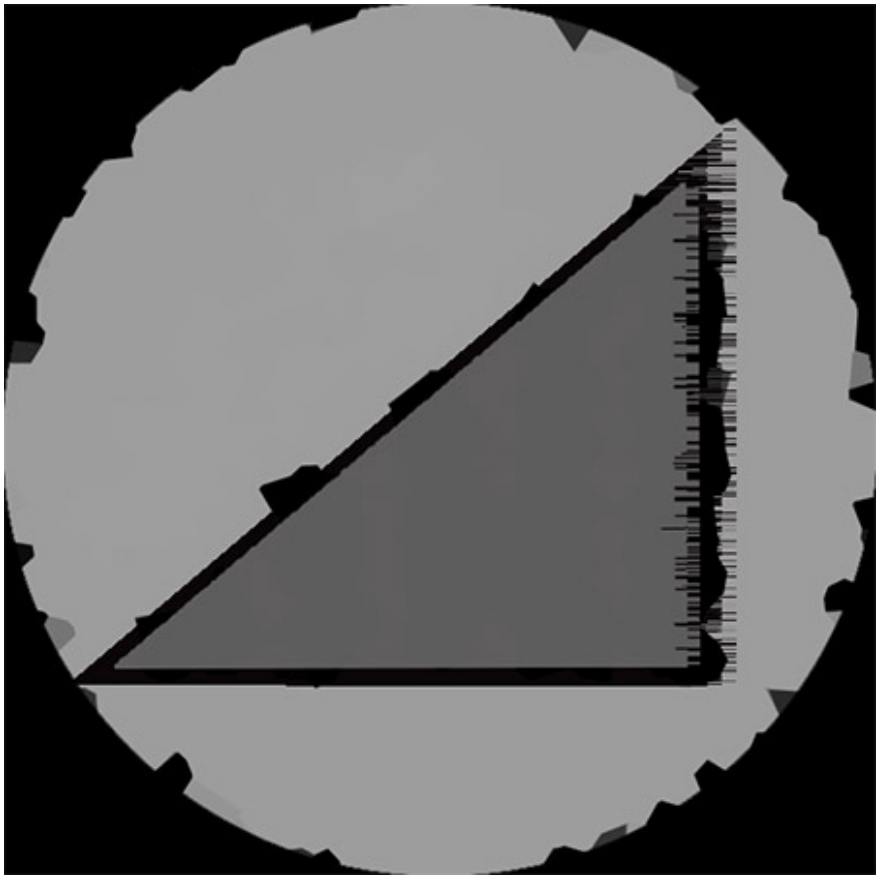
5. Account ownership

As mentioned, when logged into victim accounts, attackers will usually make changes to their passwords, email addresses, etc., in general, information that may allow users to regain their rights. Control their accounts.If the hacked account is a bank account, an electronic exchange account or another financial institution, they will take money.This control will continue until hackers get what they want or until the victim can revoke access from them.

The objects are vulnerable to attack

Today, the scope of objects vulnerable to hijacking SIM is very large and is constantly growing, in other words, anyone can become a victim, but because this is not an attack. So simple, usually only a few groups of objects can be targeted at a time.These are people with easy-to-access personal information, possessing high-end social media accounts or high-value financial accounts.But this person always has a high chance of catching the eye of the attackers, but it does not exclude the average user who has little valuable online data.Even something seemingly harmless like a normal Instagram account can still attract hackers because they can sell accounts of this type in large numbers to earn illegal profits.

How does this nightmare happen to you?



If your phone is suddenly disconnected from a place where you usually use it, you might consider contacting your service provider to check your subscription.If you suspect you have been swapped for a SIM card, you should:

1. Try to contact your service provider as soon as possible.SIM swapping is not a new scam, so if the service provider finds evidence of this fraudulent act, they may know what to do.However, you should also check back in a few hours to make sure that someone hasn't logged in to your subscription again.
2. Keep a close eye on email activities and any accounts linked to your phone number.
3. If any suspicious activity is found, remove your phone number from your accounts immediately or, if possible, change that number to a VoIP number or someone else's phone number.
4. Make sure the provider's customer service representative has locked your account and set you up for a new SIM and this SIM is protected from unauthorized changes with a PIN code.

5. Even if you are not sure which of your accounts has been compromised, you should follow the security recommendations for accounts after being hacked, as well as change your password and any sensitive information. , as the account number may be relevant.
6. Alert.If this has ever happened once, your personal information may have leaked on the Internet and may return to you again.

How to protect yourself?

Unfortunately, many service providers, companies and financial institutions have not yet implemented more effective security measures to prevent this problem.Even with additional layers of security around customer information, attackers can still work with those who work directly with customer information to provide information to them.Here are a few things you can do to protect yourself:

1. Set up additional security with your service provider.At least you must have a PIN, so anyone who wants to make changes to your account must own a PIN.
2. Use 2FA security solutions based on text or voice.Although there are still a few issues that still exist, it is better than no use, but if possible, switch to using more quality authentication applications such as Google Authenticator or Authy.These tools cannot be attacked using SIM or phone numbers, but unfortunately they are not popular 2FA options.
3. If not, start using VoIP (Voice over Internet Protocol) service like Google Voice.Because these phone numbers work via the internet instead of using SIM cards, they are immune to swapping.Replace the phone number on your SIM with the VoIP number whenever possible.

summary

Even with PIN code, authentication application and VoIP service, you are not sure if it is 100% protected because as mentioned, technology develops every second.For example, PINs may be stolen, authentication applications are not widely supported and some services will not allow you to use VoIP.In an ever-changing world of cyber security, the best thing you can do is raise vigilance, monitor suspicious activities and react quickly if any changes occur. The stronger your security shield, the less likely you are to become a target, and the faster the reaction, the less damage will be reduced.

See more:

1. Instructions for enabling 2-layer authentication for iCloud on Apple devices
2. Turn on 2-step verification for 2-layer security for Gmail, send the verification code to your phone when signing in
3. How to set up two-factor authentication on all social networks
4. How to use ASCII characters to create strong passwords

You finished reading the article "**Hack SIM: Things to know and how to avoid**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
