What is SIM-jacking?

SIM hijacking, or SIM-jacking, is a dangerous new way that fraudsters can steal information from people, by secretly controlling their phones.

SIM hijacking, or SIM-jacking, is a new, dangerous way that scammers can steal information from people, by secretly controlling their phones.

Following a growing trend, thieves are exploiting the mobile service provider's ability to transfer phone numbers between different SIM cards.

Usually this is a useful function. If a customer loses or damages a phone, they can purchase a replacement device and ask the mobile service provider to move the original phone number to the new phone.

The provider will require some confidential information to ensure the caller is the owner, before transferring the phone number to the new SIM card.

But through a series of SIM-jacking scams, people have discovered how scammers can use phone number transfer to access personal information and steal thousands of pounds.

SIM hijacking, or SIM-jacking, is a new, dangerous way that fraudsters can steal information from people.

How does SIM-jacking work?

First, the scammers must collect the necessary security information to transfer the victim's phone number. They can do this by:

- Email phishing
- Bribing employees working at the mobile carrier's company that the victim has registered

- Persuade victims to give information directly to them by trusting them.

When necessary security information or passwords are available, the crooks will impersonate the victim with the mobile service provider and persuade the service provider to transfer the victim's phone number to the new SIM card.

After that, the victim's phone will lose its network connection, all messages and reserved calls will be transferred to the phishing phone.

Why do scammers do that?

Stealing a SIM card is the first step that scammers need to gain access to personal information and steal victims' money.

If you forget your password for your email or bank account, those companies will often send you a security code via text as part of the verification process to reset your password.

But once the crooks have usurped the SIM card, they can directly receive the security codes. This security code allows them to reset the victim's password and access their social networking accounts, banks and emails.

Then the crook can start withdrawing money and stealing personal information from the victim.

Reference:

https://tipsmake.com/what-is-simjacking