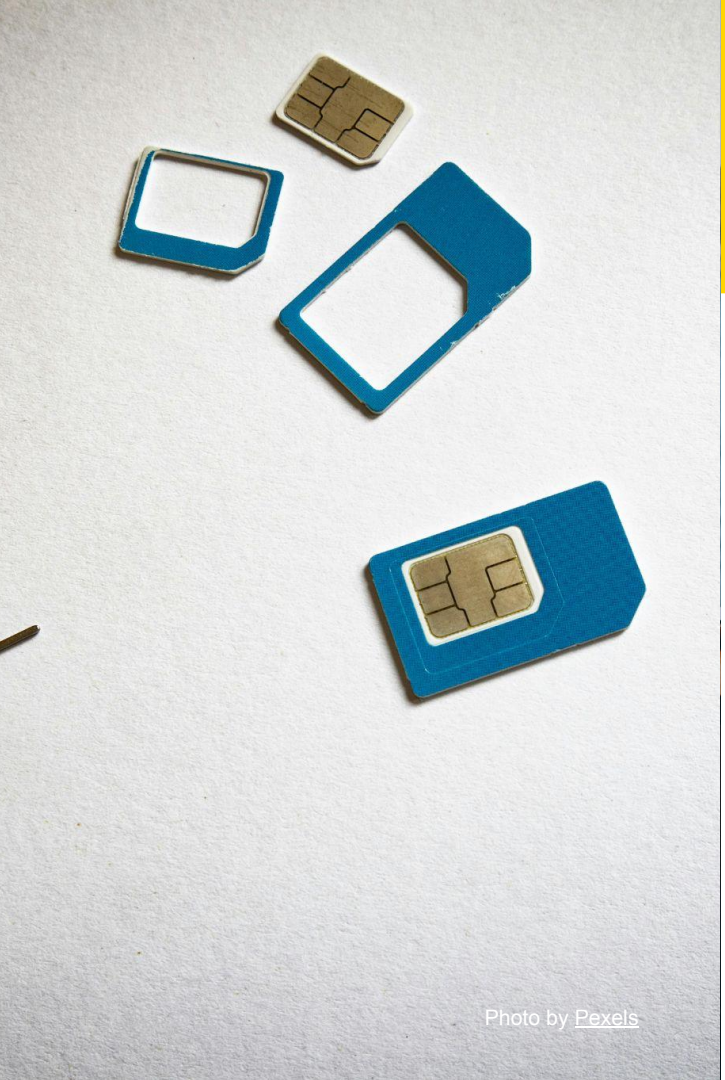
SIM Swap Scams: When Criminals Steal Your Phone Number

A Simple Guide to Protecting Your Mobile Number, WhatsApp, and Bank Accounts

Created By: Fadhl Etty

Table of Contents



1

What Is a SIM Swap?

Your Phone Number Is the Target

- A SIM swap happens when criminals move **your phone number** to a SIM card they control - without your permission.
- Once they have your number, they can: receive your calls and SMSs, get **bank OTPs and verification codes** and take over your **WhatsApp and other apps**
- **Simple Analogy:** It’s like someone stealing your mailbox key - suddenly, they receive all your private mail.

Photo by Pexels

2

How Criminals Take Control of Your Number

It Starts With Personal Information

- Criminals gather your personal details through: phishing emails or SMSs, fake calls pretending to be from banks or mobile networks and data leaks or social media oversharing.
- They then contact your mobile provider and pretend to be you, claiming they've lost their SIM and need a replacement.
- Once the SIM is swapped, your phone loses signal - and theirs comes alive.
- **Simple Analogy:** It's like someone convincing a security guard they're you, and being handed the keys to your house.

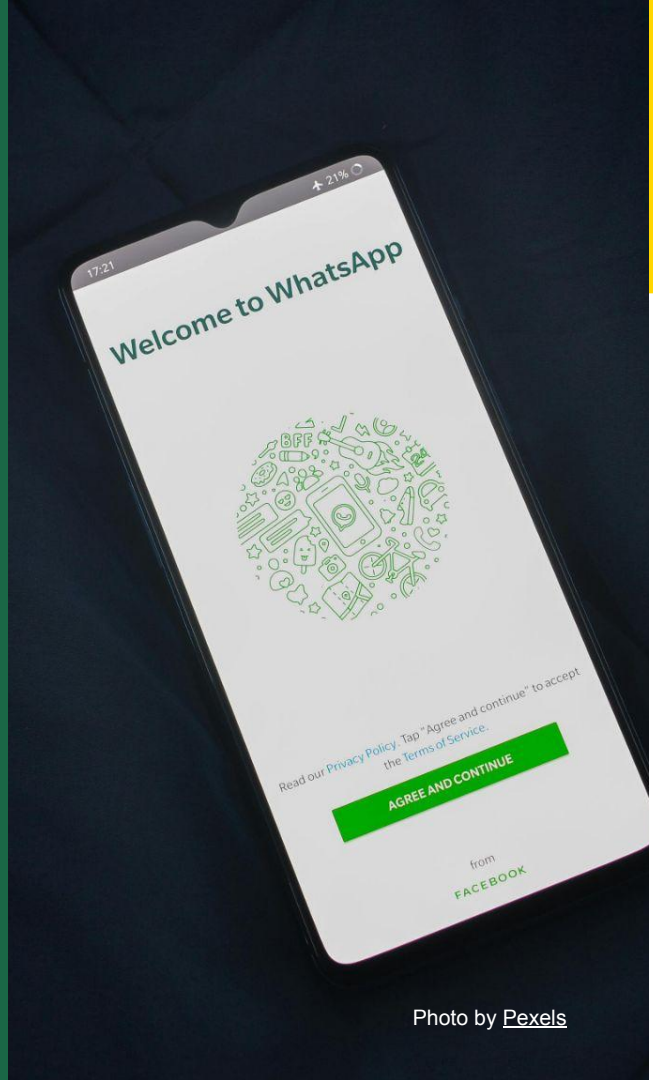


Photo by Pexels

Common SIM Swap Scams

What Usually Happens Next

- After a SIM swap, criminals often: reset your **banking app passwords,** approve transactions using OTPs, take over **WhatsApp** to scam your contacts, drain accounts via **eWallet, Cash Send, or instant EFT.**
- You may also see messages sent from *your* WhatsApp asking friends or family for money.
- **Simple Analogy:** It's like a thief stealing your phone, your wallet, and your ID - all at once.


Photo by Pexels

4

Warning Signs Your Number Has Been Taken

Red Flags You Should Never Ignore

- Your phone suddenly shows **“No Service”** or “Emergency Calls Only.”
- You stop receiving calls or SMSs unexpectedly.
- Your bank alerts you to password changes or new devices.
- Friends say they received strange messages from your WhatsApp.
- Your mobile network says a SIM swap was done - and it wasn’t you.
- **Simple Analogy:** Like coming home and finding the locks changed - something is seriously wrong.

5

What To Do If You're SIM Swapped

Act Fast - Minutes Matter

- Go **immediately** to your mobile provider (Vodacom, MTN, Telkom, or Cell C) with your ID.
- Ask them to **reverse the SIM swap** and block further changes.
- Contact your **bank's fraud department** right away.
- Change all banking, email, and WhatsApp passwords.
- Warn friends and family not to trust messages from your number.
- **Simple Analogy:** If your house keys are stolen, you change the locks immediately - this is the digital version of that.

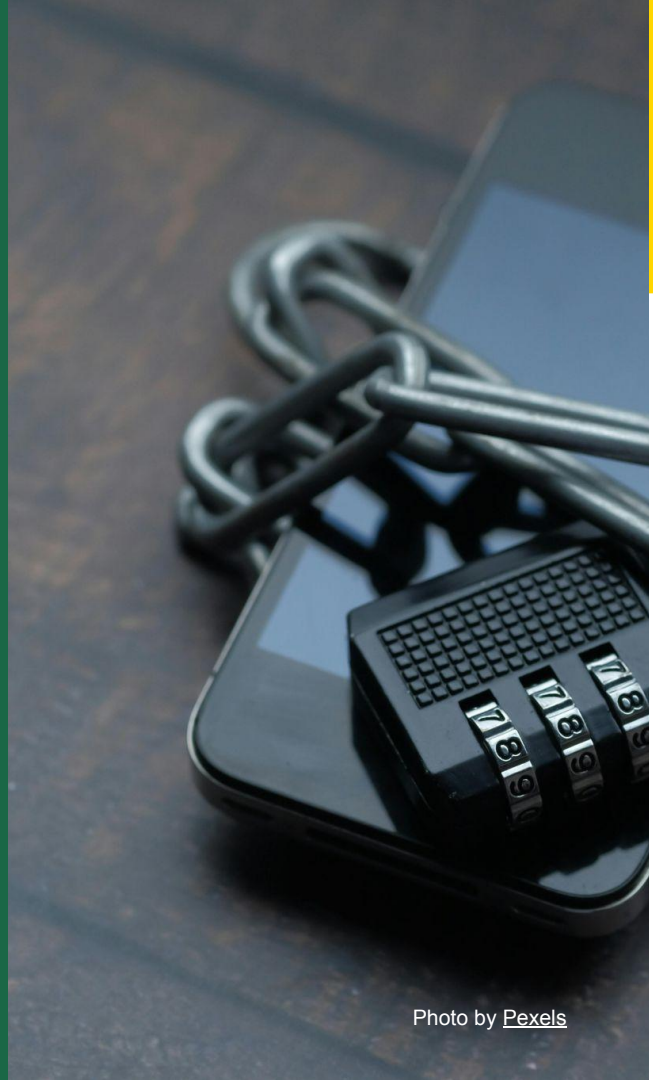


Photo by Pexels

6

Protecting Your Number Going Forward

Prevention Is Your Best Defence

- Set a **SIM swap PIN** with your mobile provider
- Never share OTPs, ID numbers, or banking details.
- Be cautious of calls claiming to be from banks or networks.
- Lock down social media - criminals use it to gather info.
- Enable extra security on banking apps and WhatsApp (like two-step verification).