# HOW CAN SHARING OF HOTSPOT LAND YOU IN JAIL

You can get arrested for sharing your hotspot connection with someone else, because there are some risks to it which will be stated below; but before then, let's explain what and how a hotspot works

A hotspot is something that a device creates in order to give other devices internet access. It does this by creating a Wi-Fi network of its own using cellular data. Therefore, one of the most common ways to get a hotspot is through your phone. When you turn on your hotspot, any devices that are connected to it will share a local area network called a LAN and due to the nature of this connection, it is possible for another person to initiate a LAN attack on your device which could be very compromising for you.

## WHAT ARE THE RISKS?

When you let someone use your hotspot, you are enabling them to use the Internet that was provided to you by your service provider. If skilled in hacking, they can access any of your personal data, phone number or have any sort of control over your phone.

### 1) YOU CAN BE ARRESTED:

For example, a stranger or a friend connects to your hotspot and unknowingly, he accesses unauthorized sites on his phone to scam people through those sites. He can be tracked through the network (your hotspot) and since it is your connection to the service provider, you will be the one they can point the source to, and in no time, you can be traced and arrested as the culprit just because you shared your hotspot. To them you are the scammer because they tracked your network as the source provider.

### 2) YOUR PHONE CAN BE IN THEIR CONTROL:

There are some resources hackers use like CSTN devices (Command System Through Network), that can give commands to lock, Reset, Block, delete contacts and also to self-destruct if your phone has that feature. But you wouldn’t know who a hacker is so therefore its best not to share your hotspot with anyone

**3) YOUR INFORMATION CAN BE INTERCEPTED:**

Anytime you send information, texts or email, with the proper skills, it can be intercepted by anyone connected to your hotspot. There are several ways that this could be done, such as a man-in-the-middle attack or intercepting the transmission via packet sniffing. When someone connects to your hotspot, you are creating a two-way street. If you're the one providing access, you may be open to attack from your guest.

**4) THEY CAN INITIATE A LAN ATTACK ON YOUR DEVICE:**

Every device that connects to the internet has an IP (Internet Protocol) address. The IP address, which is composed of a series of numbers separated by decimal points, looks something like "198.169.0.100." This number is used to help devices talk to each other and exchange data. Your network router has its own IP address, of course, as does every device on your network. But because these identifiers are so important, that means a hacker can potentially take certain actions against your network. For example

I) BLOCK YOU FROM ACCESSING WEBSITES

It is possible to use your IP address to prevent you from performing certain online activities. The most common example of this is blocking your ability to reach a certain site, or to post messages in forums or the comment section of web sites.

In fact, this is the most common way that website administrators ban rulebreakers. It's often referred to as an "IP Ban."

Your IP address can also be used to block or ban you from playing online games on some gaming services.

II) LEARN YOUR GENERAL GEOGRAPHIC LOCATION

Your IP address can reveal your geographic location. In most cases, this won't be any more specific than your city and state. It also carries the name of your Internet Service Provider (the company that gives you internet access — MTN, AIRTEL etc.), and can be combined with details from other sources to piece together data about your identity.

III) PERFORM A DENIAL-OF-SERVICE ATTACK:

Knowing your IP address, a malicious user may be able to perform a Denial of Service (DoS) attack, in which your network is flooded with data. It prevents normal traffic from getting through and overloads the network's ability to function.