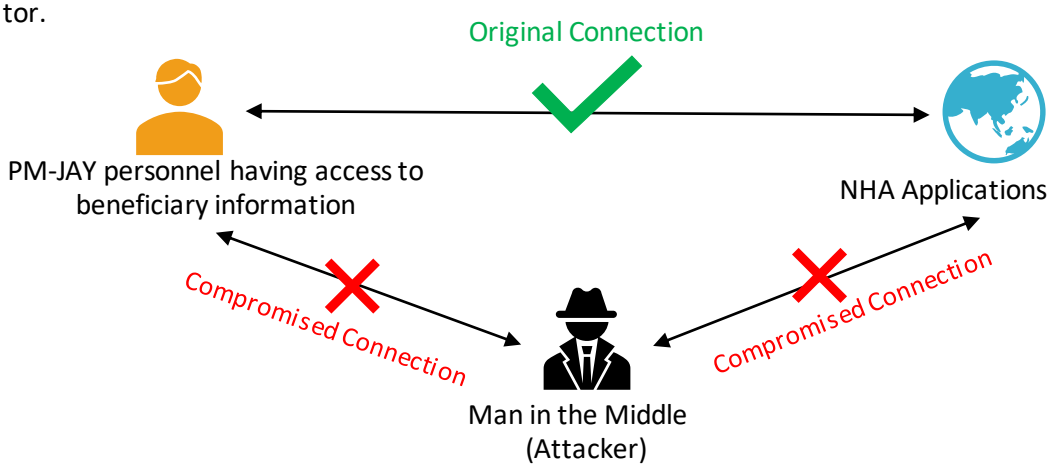
# Man-in-the-Middle (MitM) Attacks

## What are Man-in-the-Middle attacks?

A man-in-the-middle (MitM) attack occurs when an attacker intercepts communication between two parties either to secretly eavesdrop or modify traffic travelling between the two. Attackers might use MitM attacks to steal login credentials or personal information or health information, spy on the victim, sabotage communications or corrupt data.

## How can we identify a MitM attack?

If an attacker puts himself between the two communicating parties, a Man-in-the-Middle (MITM) attack occurs. This form of assault comes in many different ways. For example, a masquerader might try to extract sensitive data like Aadhaar information or health information of PM-JAY beneficiaries by acting as a moderator.




## How can we prevent MitM attacks?

All PM-JAY personnel must follow the following guidelines to prevent MitM attacks and safeguard beneficiaries' data and NHA's privacy:

**Wireless Access Point (WAP) Encryption**
Strong encryption standards like WPA2 and complex passwords on access points eliminates chances of illegitimate access to network just by being in close proximity to the router. vulnerable system of protection will enable an intruder to brute-force his way into the system and start attacking as MitM.

**Virtual Proxy Network (VPN)**
Use a VPN to encrypt the web traffic. An encrypted VPN severely limits an attacker's ability to read or modify web traffic.

**Strong Network and User Credentials**
Ensuring that the default login is modified to a strong and complex sequence of alpha-numeric and special characters is extremely essential. When an attacker intercepts the wireless router login details, they can switch the fraudulent servers to the DNS servers and execute large scale cyber attacks.

**Two-Factor Authentication**
Enabling two-factor authentication is the most powerful way to avoid MitM attacks. It implies that you'll have to give another protection factor, in contrast with your login credentials. One instance is the conjunction of a login credential and a text to your device from NHA.

**Using proper hygiene for network protection on all platforms**

- Since phishing emails are the most popular attack vector when lookout a spam email. Analyze the references cautiously before opening.
- Install applications from trusted sources.
- Reduce the chance of exploits by logging out of inactive accounts.
- Execute a security scan if you anticipate an attack.