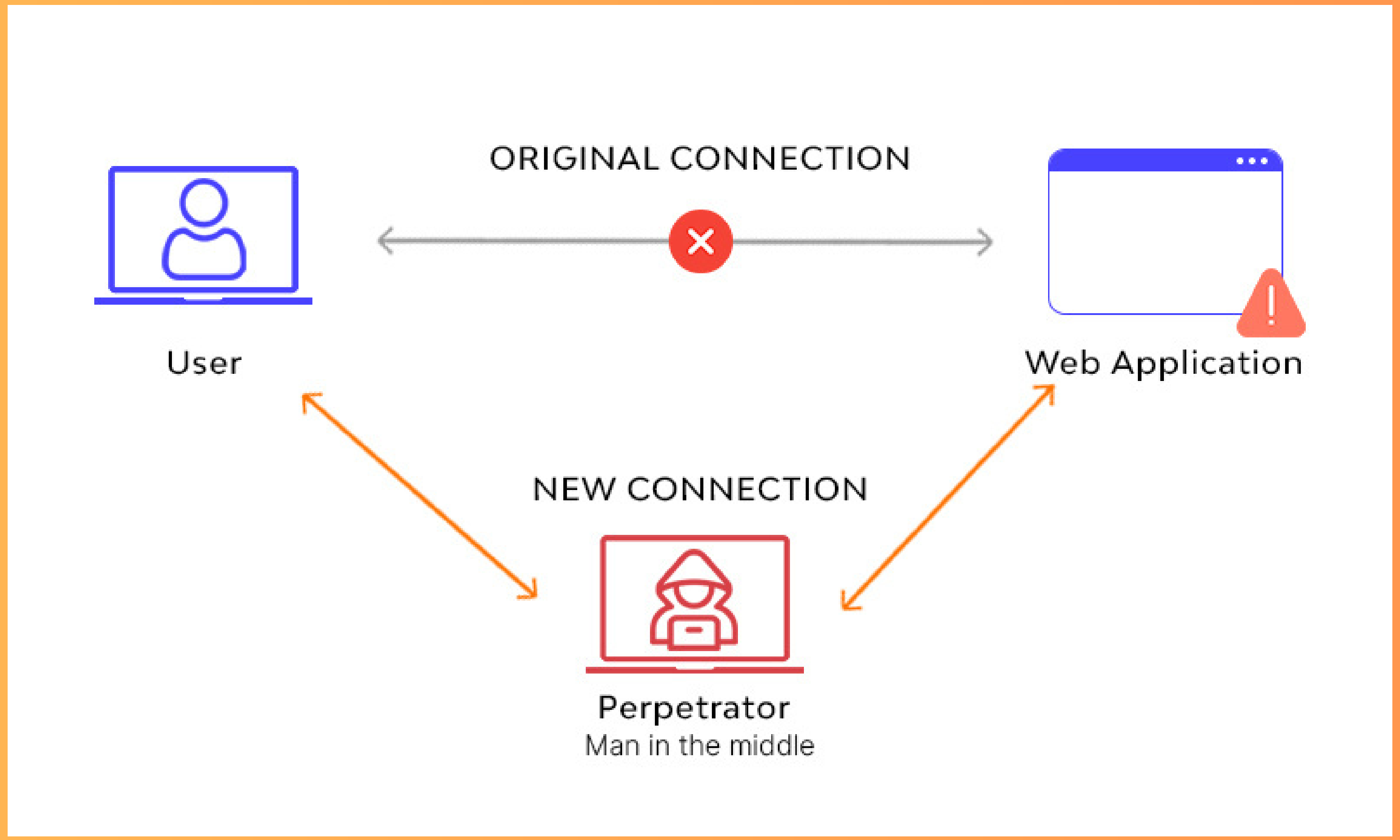
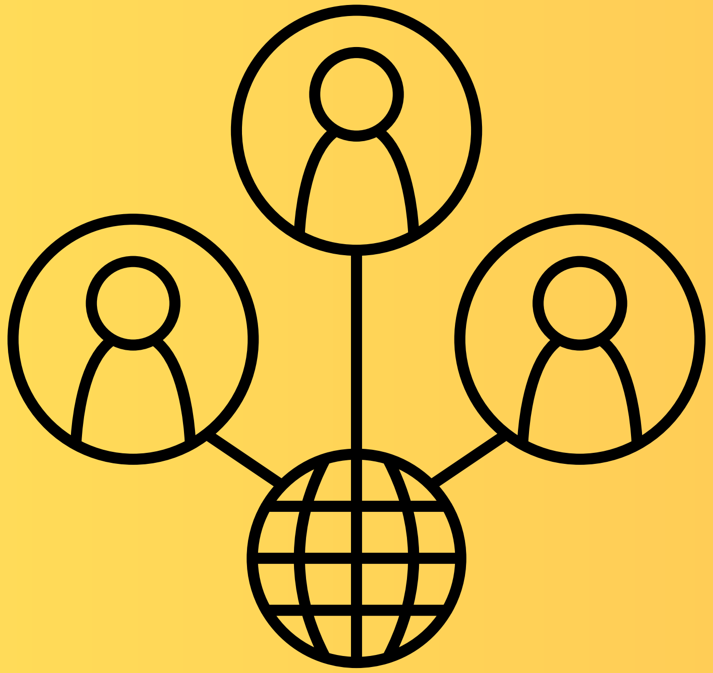
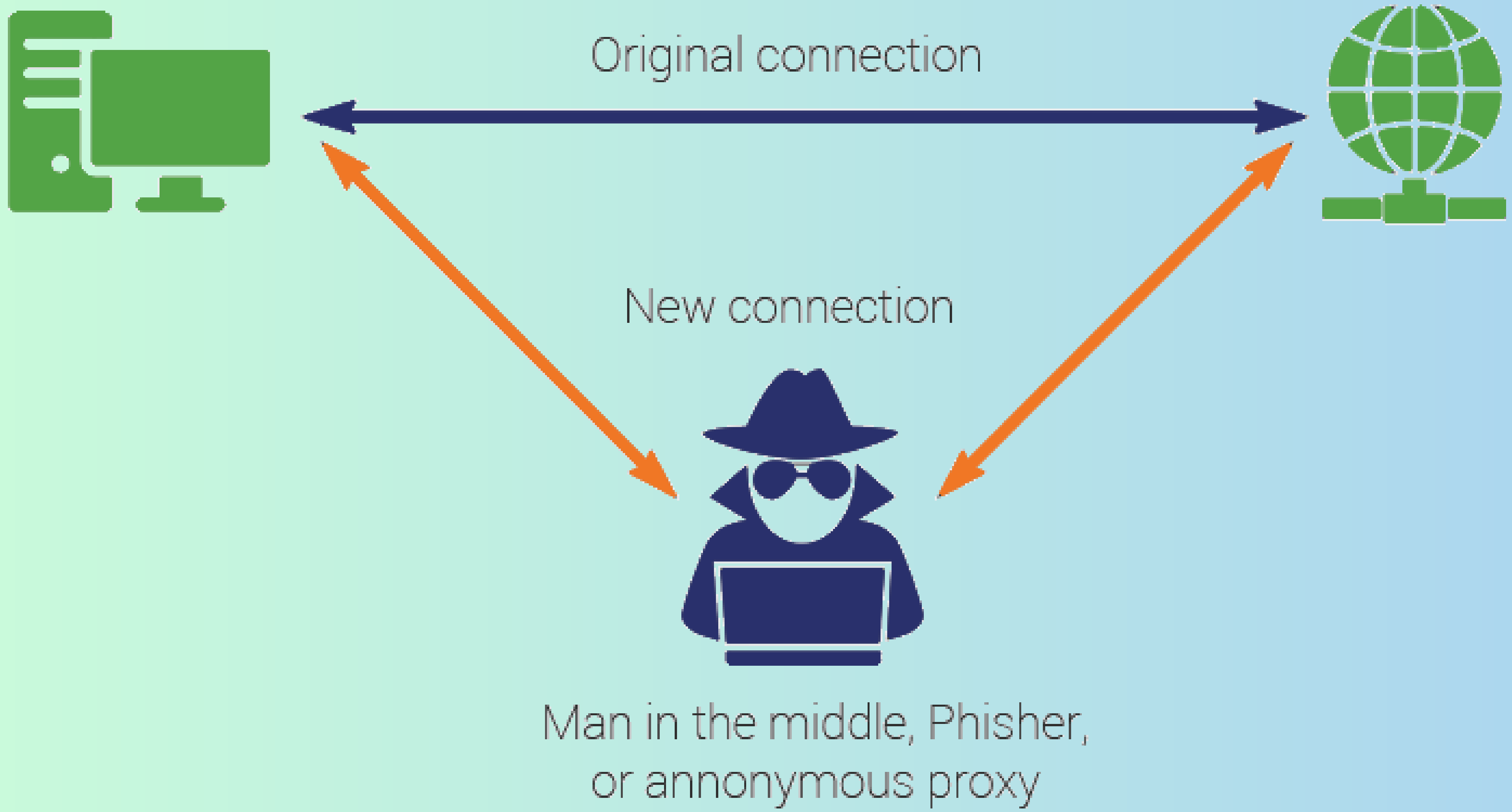
2023

Man in the Middle Threats in Public Wifi



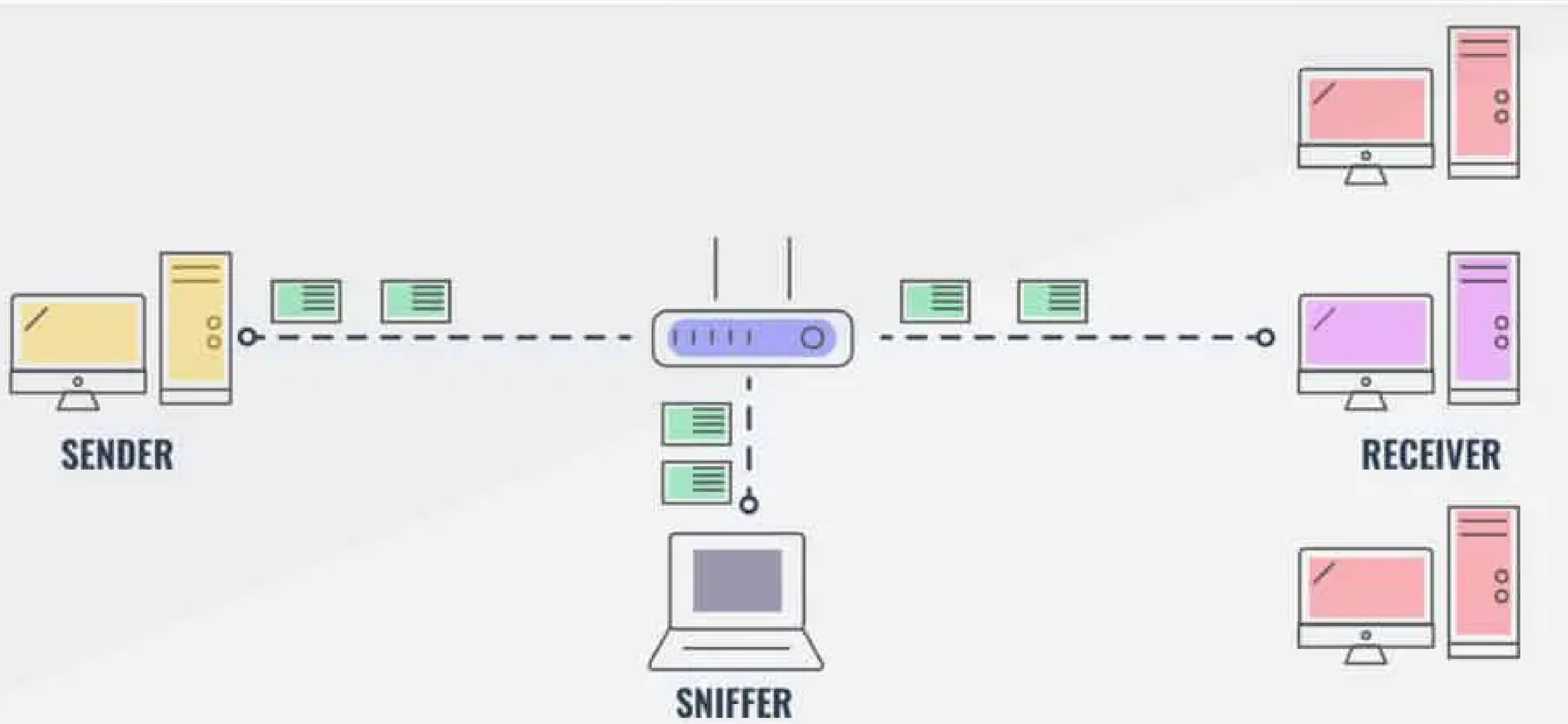


Man in the Middle



- Networks packets are intercepted by the attacker who can see and alter its content
- Attacker impersonates another actor
- Stealing information

Sniffing / Eavesdropping



- Sniff packets in a network
- Dangerous if network is unencrypted
- Messages, passwords, emails, could be visible to sniffer

Router Spoofing

- Attacker creates a fake wifi impersonating a legitimate wifi
- When a user is connected, the attacker can monitor every activity
- Steal data
- Cheap and easy to setup a fake wifi

Demonstration

Sources

https://www.byos.io/blog/how-to-prevent-man-in-the-middle-attack#:~:text=Man%2Din%2Dthe%2Dmiddle%20attacks%20(MITM)%20are,data%20to%20another%20malicious%20party.

https://www.geeksforgeeks.org/risks-associated-with-public-wi-fi/

https://www.youtube.com/watch?v=10VTmrXGHyU&t=103s