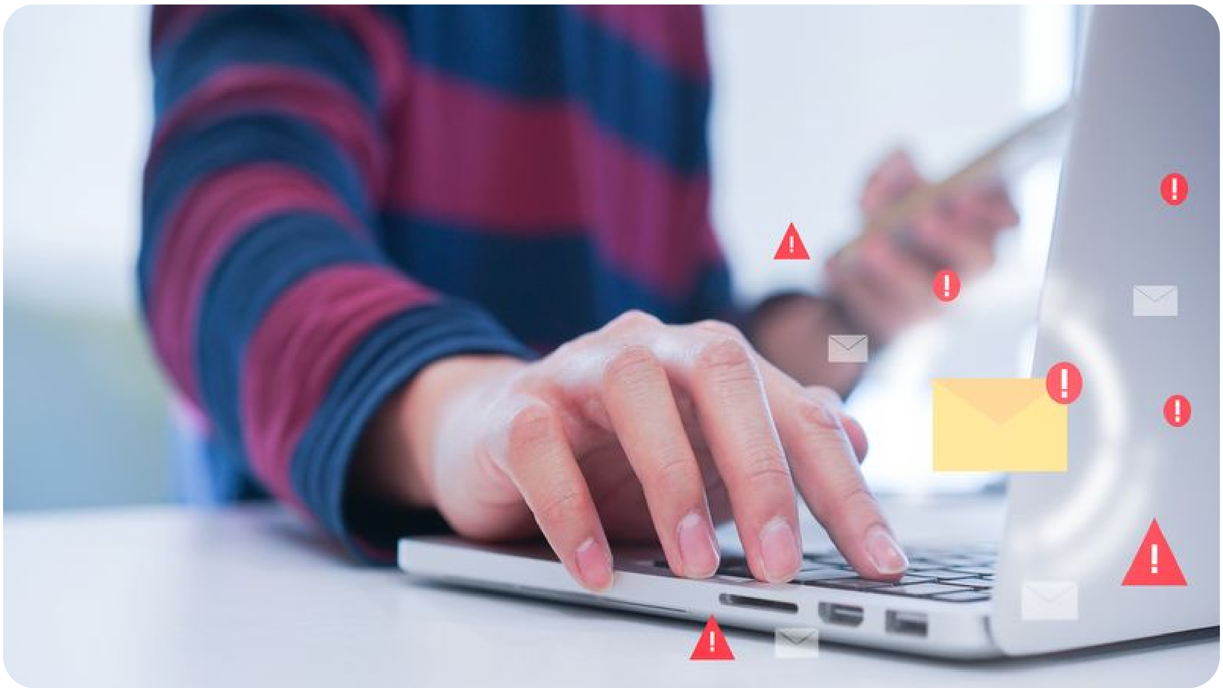
What is a Man-in-the-Middle (MitM) attack?

Man-in-the-Middle attacks give bad actors a way to intercept and redirect your online browsing. Read this blog to learn what these attacks look like and how to reduce the chance you becoming a victim of one.

December 4 2023 by

Liarna La Porta



Chances are, your mobile device doesn’t have the same security defenses as your work laptop or desktop computer. That’s why it’s important that you, the end user, do all you can to protect yourself from cyber threats. This article will focus on man-in-the-middle (MitM) attacks: how to recognize if your mobile device is impacted, how it happens and what to do next.

What is a man-in-the-middle attack?

A man-in-the-middle attack occurs when the communication between two systems is intercepted by a third party, aka a man-in-the-middle. This can happen in any form of online communication, such as email, web browsing, social media, etc.

The man-in-the-middle can use a public Wi-Fi connection to either listen in on your conversation or try to inject data into your connection to gain access to your browser or app that is trying to move data, or compromise the entire device. Once they gain access to the device, the damage they can do is endless; they can steal credentials, transfer data files, install malware or even spy on the user.

How do man-in-the-middle attacks work?

There are different types of MitM attack techniques. Below are some examples:

- **Sniffing**: Bad actors use packet capture tools to inspect packets or, by using a wireless monitoring device (which is available on Amazon for less than $100), they can see packets that are addressed to other hosts.
- **Packet injection**: Bad actors can then also use the monitoring device to inject malicious packets into data communication streams, disguising them as part of the communication.
- **Session hijacking**: If a bad actor cannot view your password, they can still take over an existing session to online services like social networking accounts.
- **SSL stripping**: Bad actors use SSL stripping to intercept packets and alter their HTTPS-based address requests to go to the HTTP version of the requested site.
- **Evil twin Wi-Fi network attacks and rogue access points:** These simulate known networks, like multiple networks named “StarbucksFreeWiFi” in the same location. In this scenario, one might be fake and could be used to hijack user traffic in a MitM attack.
- **ARP spoofing/poisoning:** Bad actors send illegitimate ARP packets that link a device’s MAC address to an IP address of a device on their LAN, allowing the bad actor to send that device's traffic to their own device. Bad actors can also “poison” an organization’s ARP table by falsifying MAC maps and affecting other computers.
- **DNS spoofing:** A bad actor may modify a server’s DNS software, directing users to malicious sites that appear legitimate.

What are the signs of a man-in-the-middle attack?

A few warning signs that you’re at risk of a man-in-the-middle attack include:

- Open/public Wi-Fi networks
- Suspicious SSIDs (Wi-Fi network names) that don’t look right

Once your connection has been intercepted, a threat actor can inject various things into your device using the connection. Here are some signs your connection has already been intercepted:

- Pop-ups or captive portal pages asking for credentials
- Login pages appear that don't look legitimate
- Fake software update pop-ups
- Certificate error messages
- Slower connection speeds

What to do if you think you have been compromised by a man-in-the-middle

So you've got a man-in-the-middle snooping on your connection, what now?

- Switch off Wi-Fi and use a cellular connection instead.
- Switch connection to your corporate VPN (virtual private network) or ZTNA (zero trust network access) solution, if you have one available.
- Watch out for identity theft warnings and put a fraud alert on your credit account.
- Do not log into unsecured websites.
- Be on the lookout for phishing sites that may have been substituted for trusted web pages.

How to prevent a man-in-the-middle attack

Since man-in-the-middle attacks are so difficult to detect, the best remediation is prevention. Reduce your risk of man-in-the-middle attacks by following this guidance:

- Limit connections to public Wi-Fi.
- If you need to do online banking in a public place, turn off your device's Wi-Fi and use a cellular connection instead.
- Use a VPN or ZTNA solution if available.
- Disable auto-connect features by changing the configuration settings so your devices don't automatically connect to Wi-Fi by default.
- Check for encryption — you can tell if a website is encrypted by looking for the HTTPS and lock symbol at the beginning of the URL, but keep in mind that this is not a guarantee of safety, only that the site has a legitimate certificate.
- Don't visit any websites that contain private or sensitive information while connected to public Wi-Fi.
- If you must connect to an open Wi-Fi network, have your device 'forget' the network so it doesn't automatically connect.