**Man in the Middle Attacks and How to Avoid Them**

A Man

**<<**

A man-in-the-middle attack (MiTM) happens when an attacker modifies a connection so that it goes through their computer. They can steal sensitive information and change data on the fly.

For example, imagine that someone takes over your connection when you log into your online bank account or when you buy something online. They will not only learn your login credentials or credit card number but they may also change the account number when you initiate a transfer of funds. An attacker may also use this technique to steal your personal information for identity theft and scams or steal your session cookies to be able to impersonate your login later.

Most types of man-in-the-middle attacks are aimed at websites or web applications. However, this technique can be used for other types of communication as well. There have been cases of MiTM email hijacking, for example.

**Where Is the Man-in-the-Middle?**

You risk a MiTM attack the most when you connect to any public networks. This means any public WiFi connections, WiFi hotspots, free WiFi at cafes, or any other networks with no access restrictions. It is easiest for the attacker to become a man-in-the-middle on local area networks and WiFi networks because a lot of MiTM attack techniques work best at this level.

The second most common entry point for MiTM attacks is your own computer. If you are not careful, you may install malware that is able to monitor and modify your internet connections (for example, man-in-the-browser). Attackers may also use phishing techniques to hijack your connections by luring you to visit sites that act as the man-in-the-middle.

The third potential risk is your home router. Very often, the home router is supplied by your internet service provider. Often, default security is not enough, for example, most routers supplied by ISPs use default admin credentials (such as *admin*/*password*). Their firmware is often outdated, too. If a certain router model is found to be faulty, this may become a chance for a MiTM attack.

When you are connected to a private home or work network, when you update your router software regularly, and when you are careful what you install on your computer, you can feel safe. In such cases, the risk of becoming a victim of a MiTM attack is very low.

## How To Avoid MiTM Attacks?

The key to avoiding man-in-the-middle attacks is the same as with most other attacks: be careful and keep your systems updated. Here are some tips and tricks:

* Be wary of links that you click to avoid phishing attempts that lead to MiTM attacks.
* Keep your operating system and your browser always up to date. This way, the attackers will not be able to use exploits to install malware on your computer.
* Use a secure WiFi protocol on your router (WPA2, WPA3 if available), use a secure WiFi key, change default login credentials for your router and update your router firmware. This way, attackers won’t be able to compromise your local area network.
* Limit your sensitive activity on public networks or use a VPN connection on public networks. A VPN will add an extra layer of security.
* Make sure that the DNS servers (DNS caches) that you use are secure. Check the configuration on your router (DNS cache addresses are usually provided via DHCP). If in doubt, use Google public DNS caches: 8.8.8.8 and 8.8.4.4.
* If you have a website or web application, regularly [**scan it**](https://www.netsparker.com/web-vulnerability-scanner/) for vulnerabilities and resolve issues. Other vulnerabilities may lead to a potential MiTM attack on your users.

If you have a website or web application, enable [**HSTS (HTTP Strict Transport Security)**](https://www.netsparker.com/whitepaper-http-security-headers/#HTTPStrictTransportSecurityHSTSHTTPHeader). If you do, your site will enforce HTTPS connections. This will protect your users against SSL stripping.