Man-in-the-Middle (MitM) Attack

(**U) This infographic provides an overview of Man-in-the-Middle (MitM) Attacks.** In a MitM attack, an attacker secretly intercepts and manipulates communications between two parties, whether a user and an application or trusted system. As the U.S. military conducts operations along the U.S.-Mexico border, soldiers and government personnel risk exposing their mobile devices to foreign networks, making them more vulnerable to unauthorized access and espionage. Therefore, safeguarding their communications is essential for maintaining security and operational integrity.

Techniques:

- Phishing
- Malware
- ARP spoofing
- DHCP spoofing

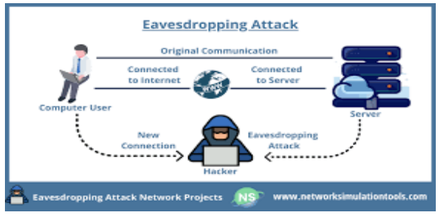
Consequences of MitM Attacks:

- Data Theft
- Financial Loss
- Reputation Damage
- System Compromise

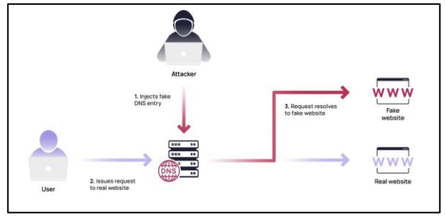
Prevention Strategies:

- Use Encryption
- Verify Certificates
- Employ Two-Factor Authentication
- Keep Software Updated
- Install Anti-Virus Software

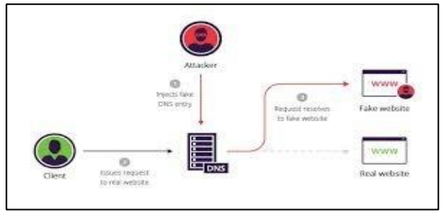
Types:



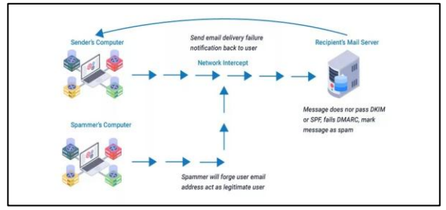
Wi-Fi Eavesdropping



HTTPS Spoofing



DNS spoofing

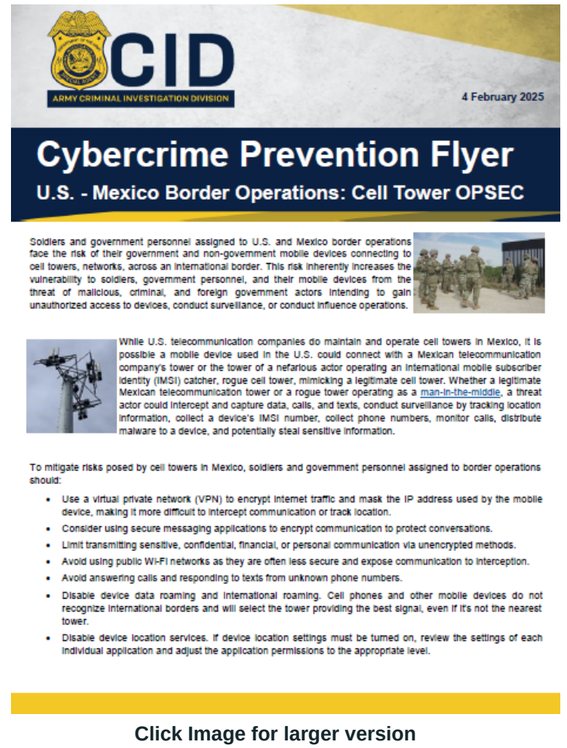


Email Interception

SSL Stripping

Click on underlined text or image for definition

Warning of potential MitM attack at US/Mexico Border


CID
ARMY CRIMINAL INVESTIGATION DIVISION
4 February 2025

Cybercrime Prevention Flyer

U.S. - Mexico Border Operations: Cell Tower OPSEC

Soldiers and government personnel assigned to U.S. and Mexico border operations face the risk of their government and non-government mobile devices connecting to cell towers, networks, across an international border. This risk inherently increases the vulnerability to soldiers, government personnel, and their mobile devices from the threat of malicious, criminal, and foreign government actors intending to gain unauthorized access to devices, conduct surveillance, or conduct influence operations.

While U.S. telecommunication companies do maintain and operate cell towers in Mexico, it is possible a mobile device used in the U.S. could connect with a Mexican telecommunication company's tower or the tower of a nefarious actor operating an international mobile subscriber identity (IMSI) catcher, rogue cell tower, mimicking a legitimate cell tower. Whether a legitimate Mexican telecommunication tower or a rogue tower operating as a man-in-the-middle, a threat actor could intercept and capture data, calls, and texts, conduct surveillance by tracking location information, collect a device's IMSI number, collect phone numbers, monitor calls, distribute malware to a device, and potentially steal sensitive information.

To mitigate risks posed by cell towers in Mexico, soldiers and government personnel assigned to border operations should:

- Use a virtual private network (VPN) to encrypt internet traffic and mask the IP address used by the mobile device, making it more difficult to intercept communication or track location.
- Consider using secure messaging applications to encrypt communication to protect conversations.
- Limit transmitting sensitive, confidential, financial, or personal communication via unencrypted methods.
- Avoid using public Wi-Fi networks as they are often less secure and expose communication to interception.
- Avoid answering calls and responding to texts from unknown phone numbers.
- Disable device data roaming and international roaming. Cell phones and other mobile devices do not recognize international borders and will select the tower providing the best signal, even if it's not the nearest tower.
- Disable device location services. If device location settings must be turned on, review the settings of each individual application and adjust the application permissions to the appropriate level.

Click Image for larger version

MitM attacks are a significant threat in the digital world. By understanding how they function and taking effective precautions, you can greatly reduce your risk of falling victim to these digital eavesdroppers.

Source: Man-in-the-Middle (MITM) Attack: Definition, Examples & More **(strongdm)**