MITM Defense Field Guide

Personal + enterprise controls. Public Wi-Fi survival. Zero trust.

Six MITM Techniques — Know What You're Facing

ARP SPOOF	DNS POISON	SSL STRIP	EVIL TWIN	SESSION HIJACK	BGP HIJACK
LAN	L3-7	L7	WiFi	L7	Global

Public Wi-Fi Survival — Coffee Shop / Airport / Hotel

- ☐ **VPN ON**
  Every session. Every network. Non-negotiable on untrusted Wi-Fi.
- ☐ **Disable auto-connect**
  Do not let device silently join 'known' SSIDs like 'Airport_WiFi'.
- ☐ **Verify SSID at counter**
  Ask the venue. Evil twins use identical or near-identical names.
- ☐ **HTTPS only in browser**
  Check the lock. If it disappears, disconnect.
- ☐ **No banking on public Wi-Fi**
  Even with VPN. Use cellular data for high-stakes activity.
- ☐ **Forget the network after**
  Prevents future auto-connect to spoofed replicas.

Enterprise Controls — Deploy These

NETWORK
- ☐ 802.1X port auth
- ☐ Dynamic ARP Inspection
- ☐ DHCP Snooping
- ☐ Wireless IDS

DNS
- ☐ DNSSEC on your zones
- ☐ DoH / DoT internal
- ☐ Monitor for encrypted DNS
- ☐ Alert on new resolvers

WEB
- ☐ HSTS with preload
- ☐ Certificate pinning
- ☐ CT log monitoring
- ☐ TLS 1.3 only

ARCHITECTURE
- ☐ Zero trust roadmap
- ☐ Micro-segmentation
- ☐ Continuous auth
- ☐ Encrypted E-W traffic

Detection Signals — Where MITM Reveals Itself

- ☐ **Duplicate MACs / IPs**
  Same IP maps to different MAC — ARP spoof signature
- ☐ **Cert issuer changed**
  Site's TLS cert suddenly signed by different CA — investigate
- ☐ **DNS TTL mismatch**
  Local response TTL ≠ authoritative — cache poisoning
- ☐ **Rogue DHCP**
  Second DHCP server offering leases — rogue on-network device
- ☐ **Same SSID, different BSSID**
  Evil twin fingerprint — wireless IDS should flag
- ☐ **Bettercap / MITMproxy signatures**
  IDS/IPS rules exist — deploy them

If You Suspect You're the Victim

Disconnect	Verify	Rotate	Revoke	Report
Kill the network connection immediately	Check ARP tables, certs, DNS — from a trusted network	Change any credential used since suspected compromise	Kill all sessions, OAuth tokens, and app-specific passwords	Notify security team and network operators of venue