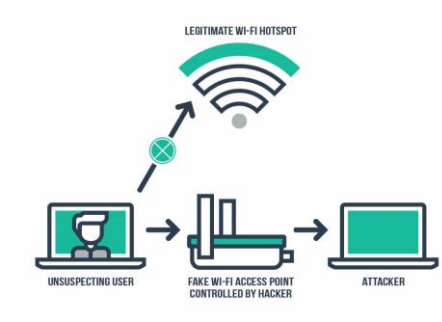
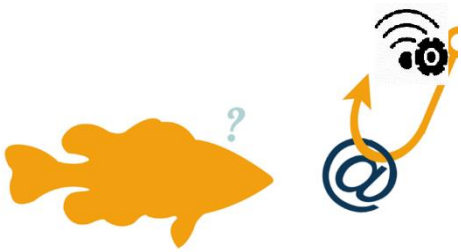
9. **Evil Twin APs:** The access point can be easily advertise the same network name (SSID) as the legitimate access point, causing nearby Wi-Fi clients to connect to them. Evil Twins are not new, but easier to use, hacker tools have increased your risk of running into one. Tools like Karmetasploit can now listen to nearby clients, discover SSIDs they're willing to connect to, and automatically start advertising those SSIDs. Once clients connect, DHCP and DNS are used to route client traffic through the Evil Twin, where local (phony) Web, mail, and file servers execute man-in-the-middle attacks. The only effective defence against Evil Twins is server authentication, from 802.1X server validation to application server certificate verification.



10. **Wireless Phishing:** The Hackers continue to develop new methods to phish Wi-Fi user day by day. It is possible to poison Wi-Fi client Web browser caches, so long as the attacker can get into the middle of a past Web session, such as by using an Evil Twin at an open hotspot. Once poisoned, clients can be redirected to phishing sites long after leaving the hotspot, even when connected to a wired enterprise network. One technique for mitigating this threat is to clear your browser's cache upon exit. Another possibility is to route all hotspot traffic (even public) through a trusted (authenticated) VPN gateway.



Wi-Fi security has significantly improved over the years. Today's enterprise WLANs can be effectively hardened against intrusion and misuse. However, end-to-end security still cannot be assumed; just enabling the Wi-Fi encryption will not make applications running over wireless networks safe as you think. Wi-Fi technologies, products, and attacks will continue to emerge day by day. Security admins still need to keep abreast of new threats, assess their business risk, and take appropriate action.