# Pretty Fly For A WiFi

# I Love My Neighbors

- Demo (Fail ☹ )

# What's the Issue?

- Public WiFi is free AND easy, but
- Prone to attack
  - MitM
  - MitB
  - Encryption cracking

# Common Misconceptions

- Hiding the SSID
- MAC address filtering
- WEP is better than nothing
- WPA is enabled, no need to worry

# Demos: Why you should worry about wireless security (Part 1)

- Wifite (Gaining access to WiFi)
  - WEP > WPA > WPS
  - Hydra (Brute force)
  - MAC spoofing

# Demos: Why you should worry… (Part 2)

- Man in the Middle (MitM)
  - Arpspoof > Driftnet (snooping)
- Man it the Browser (MitB)
  - BeEF > Metasploit

# Now that you're concerned…

- Layered Defense
  - Always change default passwords
  - Change your SSID (something less appealing)
  - MAC filtering
  - Use WPA2 – AES (known flaws in TKIP, clear txt in wifi exchange)
  - Disable WPS (Wireless Protected Setup)
    - Enabled by default on most recent models to allow less technical folks to add new devices w/o long passphrase
    - Susceptible to brute force – allows attacker to obtain pre-shared keys
  - Instead of DHCP, use static IPs in a smaller CIDR block
- Use a VPN