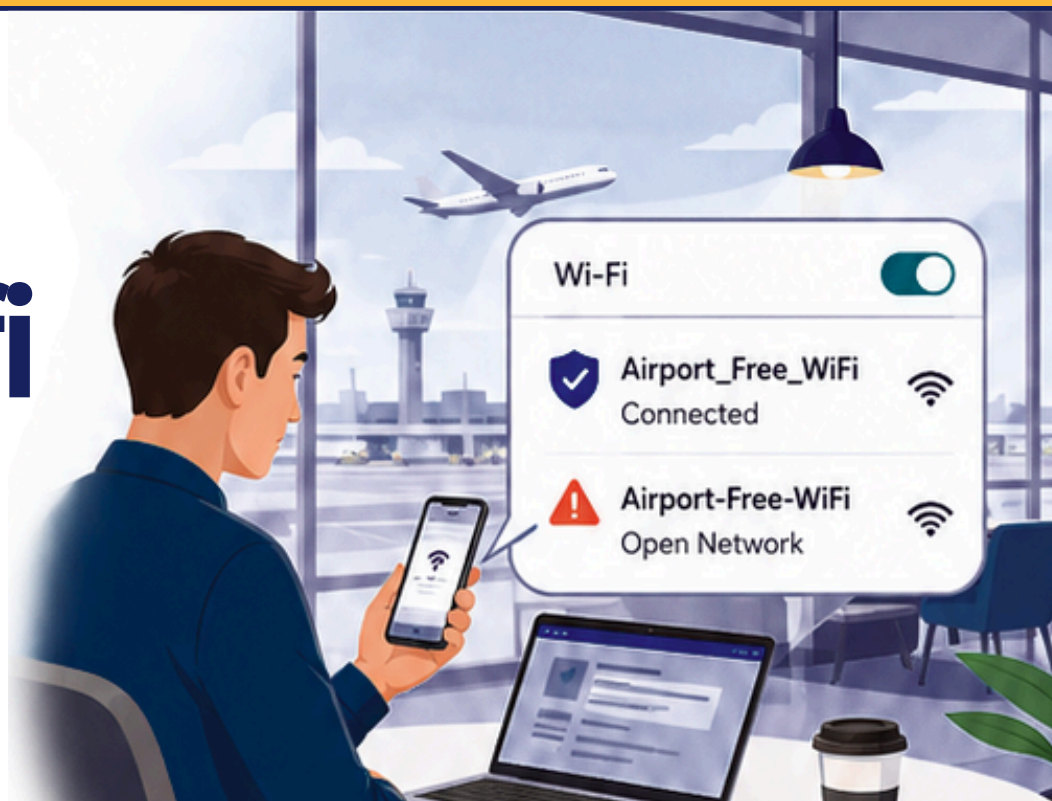


“Evil-Twin” Wifi

SPOT THE FAKE NETWORK
BEFORE IT CATCHES YOU OUT

A quick employee guide from Apex Computing



What is an “Evil-Twin” WiFi network?

An “Evil-Twin” is a fake WiFi network set up to look like a real one. It’s designed to trick you into connecting so an attacker can capture login details, monitor activity, or redirect you to fake websites.

Why it matters



Stolen
passwords and
login details



Exposure of
company emails
and files



Redirection to fake
or malicious
websites



A higher risk of
malware or
compromise

What to look for



- ✓ Two networks with nearly identical names
- ✓ A public WiFi that is suddenly open or has no password
- ✓ A login page asking for your Microsoft 365 or work email password
- ✓ Spelling mistakes, odd formatting, or generic names like “Free WiFi”
- ✓ Unexpected pop-ups asking you to download software or certificates
- ✓ Browser warnings saying a site isn’t secure



The Golden Rule

If you’re unsure which WiFi network is genuine, ask a member of staff before you connect!

How to Stay Safe on Public WiFi

SIMPLE STEPS EVERY EMPLOYEE SHOULD FOLLOW



A practical checklist from Apex Computing

6 ways to stay safe



Check the network name

Confirm the official WiFi name with venue staff before you connect



Turn off auto-join for WiFi

Stop your device from reconnecting to public networks automatically



Use a trusted hotspot or VPN

Mobile data or secure VPN access is safer than unknown public WiFi



Avoid sensitive tasks

Do not access banking, payroll, or confidential work systems on public WiFi unless necessary



Watch for browser warnings

If a site says it's not secure, stop and do not proceed



Use multi-factor authentication

MFA adds an extra layer of protection of a password is stolen

If you think you connected to a fake network...

1



Disconnect immediately

2



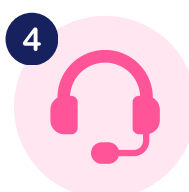
Forget the network

3



Change your password if you entered it

4



Report it to your IT team

5



Run a device security check



Need help protecting remote workers?

Apex Computing helps businesses secure Microsoft 365, devices, remote access, and cyber awareness training