Stand-in fact sheet for wireless networking on mobile devices.

What's happening here?

This artwork uses a thing called a 'KARMA attack' to trick your phone into making a wireless connection with the book. An 'attack' might sound very nasty—and they can be—but in cryptography, any method used to break a code is called an attack. Some attacks are very intrusive, some aren't. What's happening here, in the KARMA attack, is pretty simple impersonation: the book gets the name of a Wifi network from your phone. Imagine we all walk around shouting the names of our friends and family. This is kind of what your phone does: it broadcasts a Preferred Network List (PNL) into the air, and anyone can listen for them. In a KARMA attack, a computer listens for those lists of preferred networks and creates a new Wifi network with one (or more) of the names it hears. That's it—the device thinks the network is familiar and it connects.

Going back to the analogy where we walk around shouting the names of friends and family, it's a bit like someone coming up to you and saying they're your best friend, Sandra (having just heard you call Sandra's name). You begin a conversation and because you know Sandra, you might not careful about what you say. The KARMA attack is similar—it doesn't do anything much on its own, but it can be used to eavesdrop on other conversations. Now, this analogy is quite silly—you'd be able to tell Sandra from a random stranger by looking at her face or listening to her voice. As silly as it sounds, that's how phones (and laptops and so on) used to behave, they were easily fooled into connecting to a malicious network. These days, most devices have been updated so they need to match other information as well as the name. However, the other information can be faked too. Databases like Wigle (https://wigle.net/) can be used to guess the channel and ID number that your network uses for broadcast.

Who's at risk from this?

Realistically, not many people. For a hacker to take the time to impersonate your network, you'd need to have something the hacker wants. Usually, they're after money or sensitive information, so corporate or government networks are more likely to be at risk. If you work for a big corporation or you have access to restricted government information, hopefully you'll have been trained on all this stuff already!

What's the threat? and what can people do to minimise risk?

If someone tricks your device into connecting to a network, there's not a whole lot they can do except eavesdrop on your internet traffic. If you're doing something sensitive like banking or shopping, it pays to be mindful of which wireless network you're using. Otherwise, there's not much risk. It's a good idea to go through your device's settings and make sure any option to automatically join new networks is off. If you want to be really safe, switch of Wifi when you're not using it.

Some general tips for safety and privacy

Computer security people talk about everyone having a threat 'surface area'. A large attack surface area might be like having a big house with lots of doors and windows: to stop the house being burgled, you should make sure that all of the doors and windows are secure. A small apartment with a single door and two windows is much easier to secure.

- The number one best thing you can do to reduce your attack surface area is to keep all of your software up-to-date. It might seem like a hassle that new versions come out all the time, but that's because new threats are reported all the time.

If you want to reduce your attack surface area further, there are a few things you can do. Some require diligence, some only need thoughtfulness:

- Turn things off when you're not using them. Shut down Bluetooth and Wifi and only switch them on when you want them. Close any apps you're not using.
- Keep the apps on your phone or computer to a minimum, and do your best to make sure your apps come from reputable providers.