Understanding the Risk of Evil Twin Attacks

SUMMARY

An Evil Twin attack is a spoofing cyberattack that works by tricking users into connecting to a fake Wi-Fi access point that mimics a legitimate network. Evil twin attacks get their name from their ability to imitate legitimate Wi-Fi networks to the extent that they are indistinguishable from one another. This type of attack is particularly dangerous because it can be nearly impossible to identify, and it pose a significant cybersecurity risk for both end users and businesses.

This is often done in public settings where people are most likely to look for or connect to freely available Wi-Fi. This can be in airports, cafes, large public parks, etc., but hackers can really leverage this attack anywhere, mainly because the fake Wi-Fi can be easily set up and deployed.

Hackers often use evil twin attacks to gain access to personal user data like login credentials, bank transactions and credit card information. This is especially dangerous for users who use the same username and password for multiple accounts since the hacker could gain access to all of them by monitoring just one login attempt. If a user logs into their company's portal while connected to an evil twin network, the hacker can gain access to the company website using the employee's credentials. This poses a significant cybersecurity risk as hackers can then access company data or plant malware in the system.

The goal of this attack is to fool the victim into giving their authentication details for a legitimate Wi-Fi network. Once the hacker has these details, they can log into the network, take control of it, monitor unencrypted traffic, and perform other Man-in-the-Middle (MITM) attacks.

The evil twin is dangerous for individuals as well as organizations. While it is damaging enough for a personal account to be compromised, a data breach of a corporate account can have devastating consequences that affect thousands of people.

Every user should be conscientious when accessing public Wi-Fi in coffee shops or hotel lounges, especially if they do so without the extra protection of a VPN, personal hotspot, or multifactor authentication.

Employees should be trained to access the internet safely while working away from the office, and this is a critical component of internet security training. Employees should understand the risks so they can avoid problems whenever possible.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow these tips to understand the risk of Evil Twin Attacks:

- Do not log into any accounts on public Wi-Fi;
- Avoid connecting to Wi-Fi hotspots that say "Unsecure";
- Use 2-factor-authentication for all your sensitive accounts;
- Do not ignore security warnings;
- Use a VPN whenever you connect to a public hotspot;
- Only visit HTTPs websites, especially when on open networks;
- Avoid online banking when on public WiFi;
- Do not autosave Wi-Fi on your device; and
- Avoid using public Wi-Fi: Instead, use a personal hotspot or one that you know is secure.