Cybersecurity, Cyber Attack

The Evil Twin attack

23 May

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.

Once a user is connected to an “Evil Twin” network, hackers can access everything from their network traffic to private login credentials.

How an Evil Twin Attack Works

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.

The most dangerous Evil Twin attacks work by tricking victims into thinking that they are connecting to a reliable public Wi-Fi network.

To make the attack as believable as possible, hackers typically use the following steps:

Step 1: Set up an Evil Twin access point A hacker looks for a location with free, popular WiFi. The hacker takes note of the Service Set Identifier (SSID) name. Then, the hacker uses a tool like a WiFi Pineapple to set up a new account with the same SSID. Connected devices can’t differentiate between legitimate connections and fake versions.

Step 2: Set up a fake captive portal Before you can sign in to most public WiFi accounts, you must fill in data on a generic login page. A hacker will set up an exact copy of this page, hoping that they will trick the victim into offering up authentication details. Once the hacker has those, they can log in to the network and control it.

Step 3: Encourage victims to connect to the Evil Twin WiFi The hacker moves close to the victims and makes a stronger connection signal than the valid version. Anyone new will only see the Evil Twin, and they will tap and log in. The hacker can kick off anyone currently connected with a distributed denial of service (DDoS) attack, which temporarily takes the valid server offline and prompts mass logins.

Step 4: The hacker steals the data Anyone who logs in connects via the hacker. This is a classic man-in-the-middle attack, which allows the attacker to monitor anything that happens online. If the user logs into something sensitive (like a bank account), the hacker can see all the login details and save them for later use.

Example of an Evil Twin Attack

Let’s say that a user decides to connect to a public Wi-Fi network at a local coffee shop. They’ve connected to the access point there before, so they assume it’s safe and reliable.

This time, however, a hacker has set up an Evil Twin network with an identical SSID name and a stronger signal than the legitimate access point. The user connects to it despite it being listed as “Unsecure.”

While connected to the network, the user logs into their bank account to check their balance and later accesses their company’s portal to catch up on work.

Because the user has not set up a virtual private network (VPN) to encrypt their data, the Evil Twin network allows the hacker to access their banking information and company website.

Cybersecurity Risks

Evil Twin attacks pose a significant cybersecurity risk for both end users and businesses.

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.

Moreover, 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.

To help prevent hackers from creating networks that mimic their own, companies can identify duplicate networks using wireless intrusion prevention systems.

Businesses that offer public Wi-Fi may also provide customers and employees with a personal security key to ensure that users are connecting to the legitimate network.

How To Protect Yourself From an Evil Twin Attack

Evil Twin attacks can be difficult to identify, but there are multiple steps you can take to protect yourself when connecting to public Wi-Fi networks.

- Use Your Own Hotspot: the easiest way to protect yourself from an Evil Twin attack is to use a personal hotspot instead of public Wi-Fi whenever possible. This ensures that you always connect to a reliable network in public spaces and prevents hackers from accessing your data. Just remember to set a password to keep your access point private.
- Avoid Unsecured Wi-Fi Hotspots: if you need to connect to a public network, try to avoid any access points marked "Unsecure." Unsecured networks lack legitimate security features, and Evil Twin networks almost always have this designation. Hackers often rely on people brushing this off and connecting to their network without knowing the risks.
- Disable Auto Connect: if you have auto connect enabled on your device, it will automatically connect to any networks that you have used before once you're in range. This can be dangerous in public places, especially if you have unknowingly connected to an Evil Twin network in the past. To ensure that you always connect to the network you want, disable auto connect any time you leave your home or office.
- Never Log Into Private Accounts on Public Wi-Fi: you should avoid logging into private accounts whenever possible when using public Wi-Fi. Hackers can only access your login information if you use it while connected to their Evil Twin network, so remaining signed out can help protect your private information.
- Use a VPN to Encrypt Traffic: a VPN can help protect you from an Evil Twin attack by encrypting your data before a hacker sees it. When you download a reliable VPN app to your device, it encrypts or scrambles your online activity before sending it to the network, making it impossible for a hacker to read and understand.
- Stick to HTTPS websites: when using a public network, be sure to only visit HTTPS websites. These sites offer end-to-end encryption, preventing hackers from monitoring your activity while you use them.
- Use Two-Factor Authentication: adding two-factor authentication to your private accounts is a great way to prevent hackers from accessing them. Even if a hacker gains access to your login credentials, the two-factor authentication will prevent them from successfully accessing your account.
- What To Do if You Fall Victim to an Attack: if you discover that a hacker has breached your data through an Evil Twin attack, you should contact your local police department and your bank or credit card company if the hacker stole money or gained access to your banking information during the attack.

Evil Twin attacks are just one method that hackers use to gain access to sensitive information online.

To further protect yourself from cyberattacks, consider downloading reputable antivirus software and read up on the most common types of hackers to look out for.