What is an Evil Twin Attack?

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.

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.

Read on to learn how an evil twin attack works, tips for protecting yourself and what you can do if you fall victim to an attack.

How an Evil Twin Attack Works

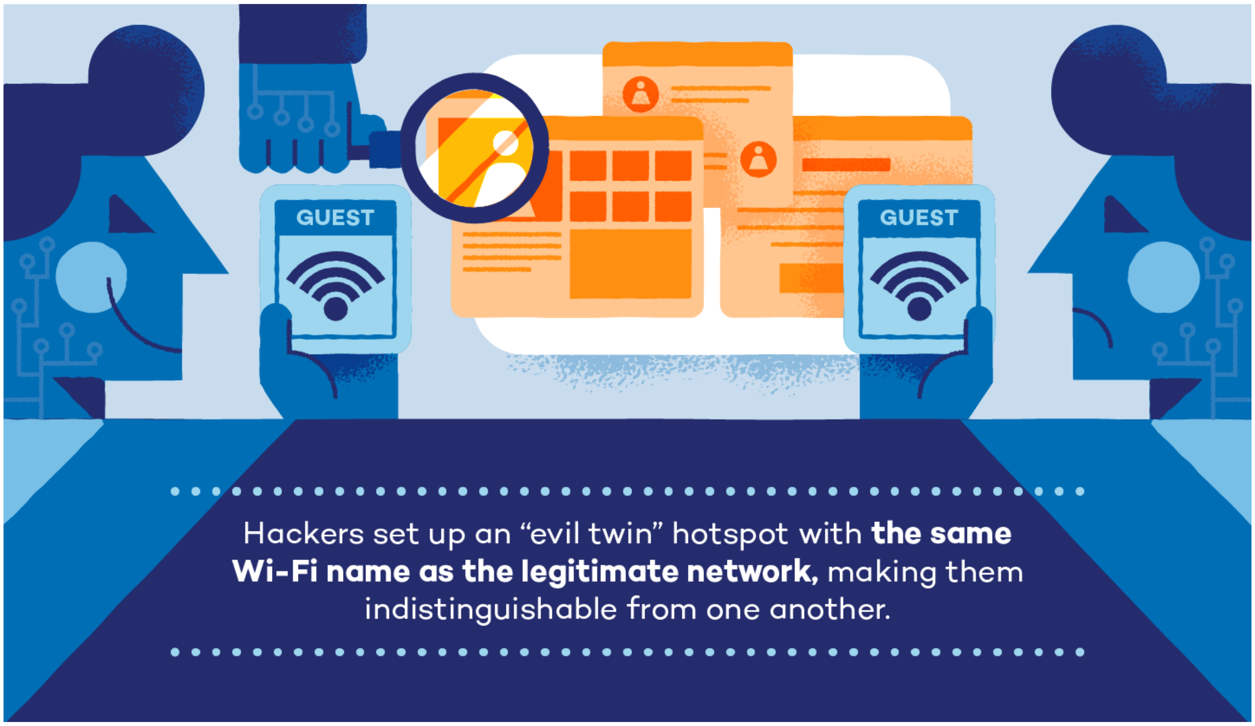
The most dangerous evil twin attacks work by tricking victims into thinking that they are connecting to a reliable public Wi-Fi network. To make the attack as believable as possible, hackers typically use the following steps:

Step 1: Choosing a location with free Wi-Fi

Hackers choose a busy location with free, popular Wi-Fi like an airport, library or coffee shop to execute their attack. These places often have multiple access points with the same name, making it easier for a hacker’s fake network to go unnoticed.

Step 2: Setting up a Wi-Fi access point

Next, the hacker creates a new hotspot using the same Service Set Identifier (SSID) name as the legitimate network. They can use almost any device to do this, including phones, laptops, portable routers and tablets. Some hackers may even use a Wi-Fi Pineapple to achieve a broader range.


GUEST
GUEST
Hackers set up an “evil twin” hotspot with **the same Wi-Fi name as the legitimate network,** making them indistinguishable from one another.

Step 3: Creating a fake captive portal page

If you’ve ever logged into a public Wi-Fi network, you’ve probably encountered a captive portal page. These typically require you to enter a password or other basic information to access the network. While many legitimate networks use these, hackers can easily replicate them to trick users into sending over their login information. Unfortunately, it can be nearly impossible to tell the difference between a legitimate and fake captive portal page if the hacker knows what they’re doing.

Step 4: Setting up closer to potential victims

Once a hacker has finished setting up the evil twin access point and fake captive portal page, they may move their device or router closer to potential victims to create a stronger signal. This convinces people to choose their network over the weaker ones and forces some devices to connect automatically.

Step 5: Monitoring and stealing user data

Once a victim has connected their device to an “evil twin” network, the hacker can monitor everything they do online, from scrolling through social media accounts to checking bank statements. If a user logs into any of their accounts while connected to the network, the hacker can collect their login credentials. This is especially dangerous if the user uses the same credentials for multiple sensitive accounts.

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.

Users

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.

Hackers can use evil twin attacks to access **credit card numbers, banking information, login credentials** and other sensitive user data.

Businesses

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.

“A **VPN app encrypts your online activity** before sending it to the network, making it impossible for a hacker to read.

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 can file a complaint with the FCC Consumer Complaint Center. You should also 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.