Evil twin attacks and how to prevent them

By Kaspersky

Published: 2017-10-13 · Archived: 2026-04-06 00:48:24 UTC

It's natural to use public Wi-Fi to check messages or browse online when you're out and about – shopping, traveling, or simply grabbing a coffee. But using public Wi-Fi can carry risks, one of which is evil twin hacking. Read on to learn about evil twin attacks and how to avoid them.

What is an evil twin attack?

An evil twin attack takes place when an attacker sets up a fake Wi-Fi access point hoping that users will connect to it instead of a legitimate one. When users connect to this access point, all the data they share with the network passes through a server controlled by the attacker. An attacker can create an evil twin with a smartphone or other internet-capable device and some readily available software. Evil twin attacks are more common on public Wi-Fi networks which are unsecured and leave your personal data vulnerable.

How do evil twin attacks work?

Here’s how a typical evil twin Wi-Fi attack works:

Step 1: Looking for the right location

Hackers typically look for busy locations with free, popular Wi-Fi. This includes spaces like coffee shops, libraries, or airports, which often have multiple access points with the same name. This makes it easy for the hacker’s fake network to go undetected.

Step 2: Setting up a Wi-Fi access point

The hacker then takes note of the legitimate network's Service Set Identifier (SSID) and sets up a new account with the same SSID. They can use almost any device to do this, including smartphones, laptops, tablets, or portable routers. They may use a device called a Wi-Fi Pineapple to achieve a broader range. Connected devices can’t distinguish between genuine connections and fake versions.

Step 3: Encouraging victims to connect to the evil twin Wi-Fi

The hacker may move closer to their victims to create a stronger connection signal than the legitimate versions. This convinces people to select their network over the weaker ones and forces some devices to connect automatically.

Step 4: Setting up a fake captive portal

Before you can sign in to many public Wi-Fi accounts, you must submit data on a generic login page. Evil twin hackers set up a copy of this page, hoping to trick unsuspecting victims into disclosing their login credentials.

Once the hackers have those, they can log in to the network and control it.

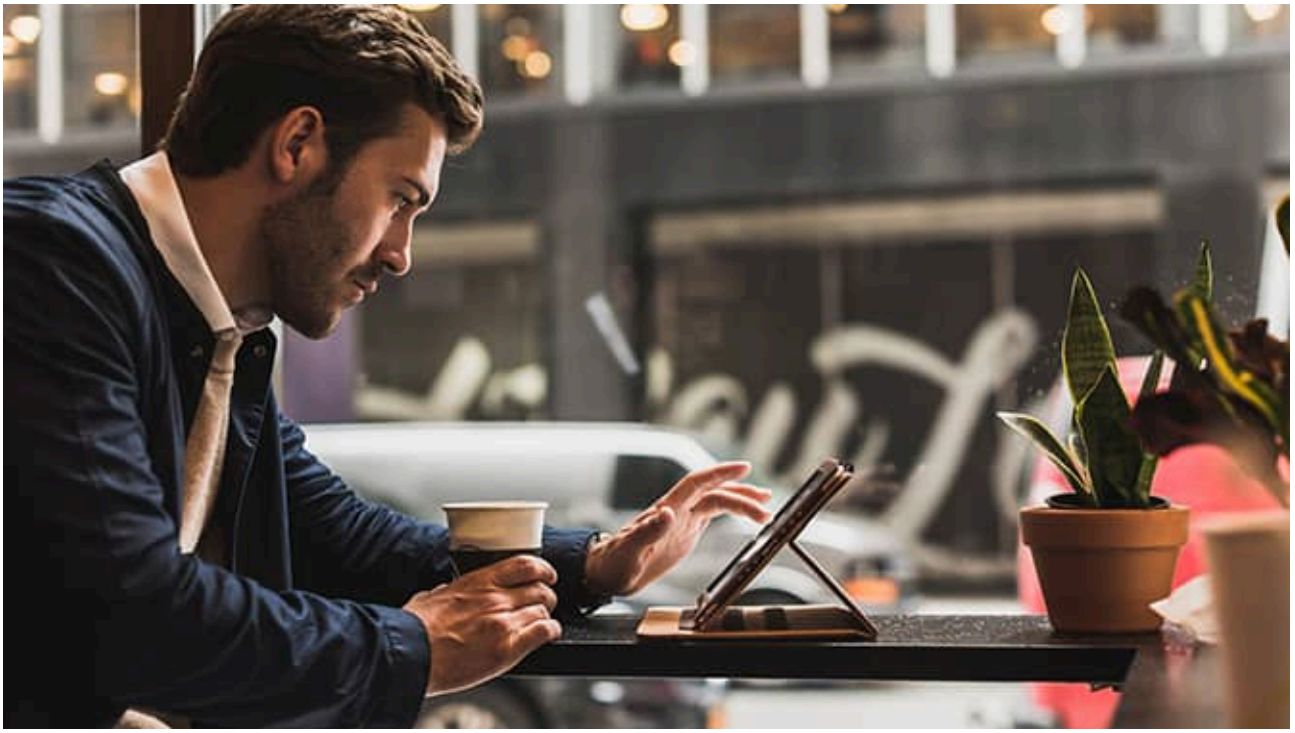
Step 5: Stealing victims' data

Anyone who logs in connects via the hacker. This is a classic man-in-the-middle attack that allows the attacker to monitor the victim's online activity, whether scrolling through social media or accessing their bank accounts. Suppose a user logs in to any of their accounts. In that case, the hacker can steal their login credentials – which is especially dangerous if the victim uses the same credentials for multiple accounts.

Why are evil twin attacks so dangerous?

Evil twin attacks are dangerous because, when successful, they allow hackers to access your device. This means they can potentially steal login credentials and other private information, including financial data (if the user carries out financial transactions when connected to the evil twin Wi-Fi). In addition, the hackers could also insert malware into your device.

Evil twin Wi-Fi attacks often don't leave tell-tale signs which could expose their true nature. They perform their primary task of providing access to the internet, and many victims won't question it. Users may only realize they've been victimized by an evil twin attack afterward when they notice unauthorized actions performed on their behalf.



Evil twin attack example

A person decides to visit their local coffee shop. Once they are seated with their coffee, they connect to the public Wi-Fi network. They have connected to this access point before without problem, so they have no reason to be suspicious. However, on this occasion, a hacker has set up an evil twin network with an identical SSID name. Because they are seated close to the unsuspecting target, their fake network has a stronger signal than the coffee shop's real network. As a result, the target connects to it even though it's listed as 'Unsecure'.

Once online, the target logs into their bank account to transfer some money to a friend. Because they are not using a VPN or Virtual Private Network, which would encrypt their data, the evil twin network allows hackers to access their banking information. The victim only becomes aware of this later when they realize unauthorized transactions have taken place in their account, causing them financial loss.

Rogue access point vs evil twin – what's the difference?

So, what's the difference between a rogue access point and an evil twin access point?

- A rogue access point is an illegitimate access point plugged into a network to create a bypass from outside into the legitimate network.
- By contrast, an evil twin is a copy of a legitimate access point. Its objective is slightly different: it tries to lure unsuspecting victims into connecting to the fake network to steal information.

While they are not the same, an evil twin could be considered a form of rogue access point.

What to do if you fall victim to an evil twin attack

If your data is breached through an evil twin Wi-Fi attack, or you suffer financial loss because a hacker stole money or accessed your banking information during the attack, then contact your bank or credit card company immediately. You should also change your passwords across the board (you can read tips on choosing a strong password here). Depending on the severity of the attack, you could contact your local police department too, as well as file a complaint with the relevant consumer protection body in your country.

How to protect your device from evil twins

To avoid falling victim to a fake hotspot or evil twin hacking, here are some precautions you can take:

Avoid unsecured Wi-Fi hotspots:

If you have to connect to a public network, avoid access points marked as ‘Unsecure’. Unsecured networks don't have security features, and evil twin networks nearly always have this designation. Hackers often rely on people not knowing the risks and connecting to their network anyway.

Use your own hotspot:

Using your own personal hotspot instead of public Wi-Fi will protect you from evil twin attacks. This is because you’ll be connected to a reliable network when you’re out and about, which reduces the risk of hackers accessing your data. Set a password to keep your access point private.

Check warning notifications:

If you try connecting to a network and your device alerts you to something suspicious, take notice. Not all users do, which can have negative consequences. Instead of dismissing those seemingly annoying warnings, pay attention because your device is trying to protect you from danger.

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. Instead, disable the auto-connect feature whenever you’re out of the home or office and let your device ask for permission first before connecting. That way, you can check the network and approve or disapprove.

Avoid logging into private accounts on public Wi-Fi:

Where possible, avoid carrying out financial or personal transactions on 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 multi-factor authentication:

Multi-factor authentication is when two or more steps are required to log into a system. You may combine a password requirement with a code sent to your mobile phone that you need to enter to proceed. This provides an

added layer of security between hackers and your information. Where accounts offer multi-factor authentication, it's worth setting it up.

Stick to HTTPS websites:

When using a public network, make sure you only visit HTTPS websites, as opposed to HTTP. (The ‘s’ stands for secure.) An HTTPS website will have end-to-end encryption, which prevents hackers from seeing what you are doing.

Use a VPN:

A VPN or Virtual Private Network protects you from evil twin attacks by encrypting your data on the internet no matter the network you are using. A reliable VPN such as Kaspersky Secure Connection encrypts or scrambles your online activity before sending it to the network, making it impossible for a hacker to read or understand.

You can also make sure to have a comprehensive security product installed. Kaspersky Internet Security protects your device from a wide range of cyberthreats.

Kaspersky Internet Security received two AV-TEST awards for the best performance & protection for an internet security product in 2021. In all tests Kaspersky Internet Security showed outstanding performance and protection against cyberthreats.

Related articles:

- Public Wi-Fi safety tips
- Good cyber hygiene habits to help you stay safe online
- Personal online privacy tips
- Messaging app security
