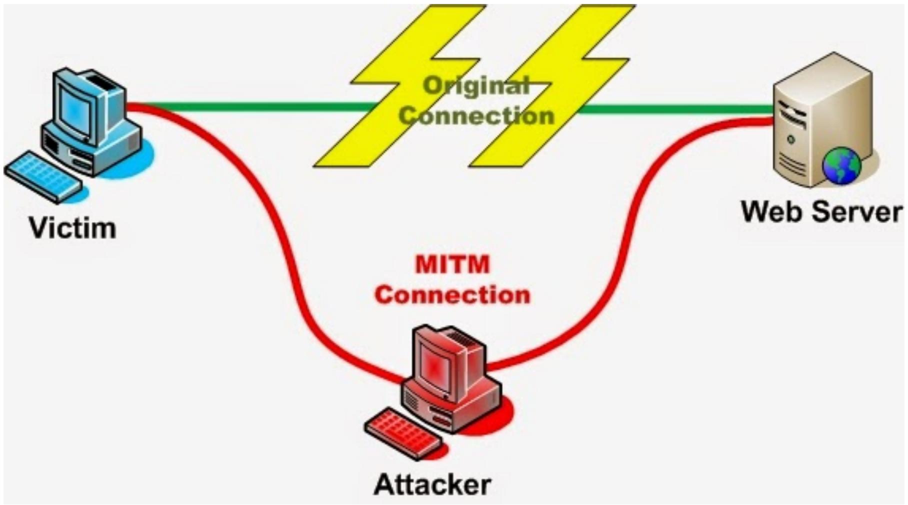
HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
WEEKLY

Volume #4 - Issue #174
August 24th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Recognizing Evil Twin Networks



Evil-Twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. (Also known has a Man-in-the-Middle attack.) An evil twin is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider.

How many people ever think twice before connecting to a free public hotspot at a coffee shop, airport, or hotel? Did you ever stop to wonder if the public Wi-Fi hotspot you just connected to is a legitimate one, or if it might be an Evil Twin hotspot in disguise? An Evil Twin Network is a Wi-Fi access point set up by a hacker or cybercriminal. It is meant to mimic a legitimate wireless network provided by a business, such as a hotel, that provides free Wi-Fi access to its patrons.

An Evil Twin network mimics a legitimate hotspot in just about every way, but its intentions are to steal information from you. Hackers create Evil-Twin networks to allow them to both eavesdrop on network traffic and insert themselves into the data conversation between the victims and the servers that the victims access. By imitating a legitimate hotspot and tricking users into connecting to it, a hacker or cybercriminal can then steal account names and passwords and redirect victims to malware sites, phishing sites, etc. They can also view the contents of files that the victims download or upload while they are connected to the Evil-Twin access point.

Victims that connect to Evil-Twin networks don't even know that they are connecting to a rogue access point because the perpetrators use the network name of the actual hotspot. The whole experience is unknown to the victim.

Hackers don't even have to setup a large hardware-based access point to create an Evil-Twin network. This can easily be done using emulating software that utilizes the Wi-Fi network adapter in their laptop, or even a mobile device. Having this level of portability and concealment allows them to position themselves nearer to a potential victim which may help them to overpower the signal coming from the legitimate access point.

There aren't a lot of ways to defend against this type of attack other than just being aware of your surroundings. One of the ways to protect yourself from Evil-Twin access points is to use a Virtual Private Network (VPN).

Using the encrypted tunnel provided by the VPN encryption process helps to secure all traffic between your VPN-capable device and the VPN server. Virtual Private Networks (VPNs) used to be a luxury that only large corporations could afford to provide their employees, but now personal VPN services are plentiful and cheap, starting at around $8 a month. We will be discussing more about a VPN and how to set one up a in an upcoming section.

Other than avoiding open public networks, you can help reduce the eavesdropping risk associated with Evil-Twin networks by only logging into your e-mail and other sites that show HTTPS at the beginning of the URL. These sites encrypt your data as soon as it leaves your device.

Bottom Line, always look at the complete WiFi network list on your device before connecting to a public WiFi. If there are two names for the place that you are at, there is a good chance one is an Evil-Twin. In this case, **DON'T CONNECT!** Use your cell phone, or the hotspot function of your cell phone for your computer. You may use more data from your plan, but that is a lot better than the alternative possibilities.

Thank you for subscribing to our email!

Home Cyber Defense Weekly

is a service of

House of File Technologies

House of File
Technologies