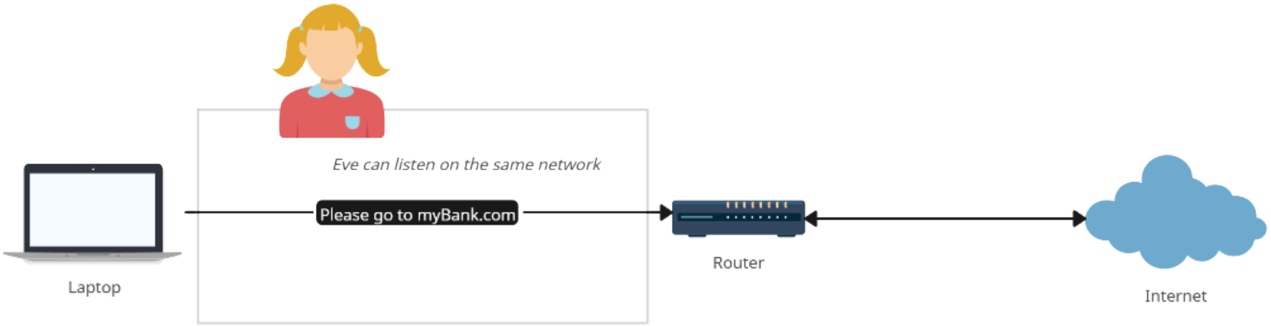
Public Wifi: Dangers, Myths, and Misconceptions

By Nathan Parker, Alden Harcourt, and Elek Thomas-Toth

Using public wifi networks is inevitable in today's world of constant online activity. Whether it's messaging family members, playing mobile games, browsing the web, or doing a more significant task such as checking your bank account info, worrying about the security of your connection is only natural. So how worried should you really be? Can hackers really steal your data just by being on the same network as you? Before answering those questions, it is important to understand how network traffic works.

When you visit a webpage, your computer talks to your router, who connects you to the broader internet. Then, your request is sent to the website's server, who sends back the information that you want. If someone is on the same wifi network as you, they can theoretically see the requests you make to other websites.



Typically, most of the information in your request will be encrypted. That is, someone listening in can see that you are sending a request but they can't see what is in it. To know how likely it is that someone is listening on your network, we need to know about different categories of wifi and their varying levels of security.

Different Kinds of Wifi, Different Amounts of Security:

First, we have "random" wifi. Random wifi is by far the least secure type of wifi, and is something akin to a wifi that you would just connect to as it popped up on your device. Random wifi is neither password protected nor does it have a known source. Without these two factors, it is quite possible that you are directly connecting your device to a malicious actor - who could leverage any number of vulnerabilities in an attempt to steal your information, passwords, or infect your computer with malware. Random wifi should be avoided in all situations, and only be used in times of true desperation.

Our second type of wifi is “public” wifi, and is the type we will be most commonly be concerned with throughout this piece. Think of public wifi as the wifi you have access to at your local coffee shop. It has a known source, and is usually password protected. Although, that password is publicly available, so anyone could connect. Public wifi is still fairly secure, as the source is known to be a trusted entity, and although anyone could be listening on it, the types of attacks available to a malicious actor connected to the same network as you are much more limited than by someone who actually controls the network itself. Even though the password is known by the public, the fact that it exists at all is still a deterrent for hackers. This means that they most likely would have to visit the establishment to obtain the password, a risky move that could lead to them being caught.

Finally, we have “private” wifi. Private wifi is by far the most secure, as it is something like your home network. Its source is fully known and trusted, and its password is secure and unknown to the public. Theoretically, not only are there not many users on the network, but every user is trustworthy and won't attempt any form of attack. On a private network, you should be able to assume total wifi security for even your most sensitive activities.

Common Myths:

There are lots of myths surrounding the insecurity of public wifi. Most of these myths do have shreds of truth to them, but in reality, public wifi is much less likely to compromise you than commonly thought. One of the largest myths surrounding public wifi is the prevalence of adversary-in-the-middle (AITM) attacks. In an AITM attack, a malicious actor impersonates the website/person/etc that you intended to connect to. For example, if a hacker had enough control over a network, they could redirect a connection to your bank website to a fake version, and then steal your login credentials once you enter them on their site. However, it turns out that these attacks are not very common. As it currently stands, AITM attacks are difficult to execute, and the amount of effort needed to complete one would be wasted on an insignificant target such as the typical coffee shop wifi user. However, high level targets, such as government officials, high ranking corporate employees, elected officials, etc, should be more cautious. Another reason these attacks are fairly uncommon is due to the fairly robust nature of web security. Almost every organization's website has unique certificates that are used to verify their identity, especially websites where consequential data is exchanged, such as a bank or government website. These certificates are extremely hard to fake, and again, would take more effort to spoof than simply attempting a different, possibly even more potent kind of attack, such as a phishing email.

Another common myth surrounding public wifi is that hackers could “hijack” computers simply by being connected to the same network as a target. The truth is, this is just not really the case. Fully taking over control of a target’s computer is a very difficult task, and takes much more than just being connected to a common wifi network. Usually, an attack like this would involve having the target download some form of powerful malware onto their machine - and it is not feasibly possible to remotely download such a file onto a target computer simply by being on the same wifi as them. Although new vulnerabilities are constantly being discovered, it is highly unlikely that anything of this nature would happen if you keep your devices up to date.

The myth with the most truth to it though is the fear of packet sniffing. Packet sniffing is the practice of connecting to a wifi network, and then using software programs to monitor, intercept, and read the data that is being sent over it. Before the widespread adoption of HTTPS, these attacks were actually fairly frequent due to their extreme ease. Because of the unencrypted nature of standard HTTP connections, it was possible for attackers to intercept and read almost all data being transmitted over a shared wifi network. However, in current times where HTTPS is used by the overwhelming majority of websites, these attacks are fairly non-existent. It is relatively impossible to intercept and read significant data sent over a secure connection because of the strong encryption protocols utilized by HTTPS. Another reason for the infrequency of these attacks are their risk factors. For the most part, a hacker would need to be very close to the source of the network (e.g. inside of the coffee shop) in order to successfully monitor a public wifi, increasing the likelihood of their identity being compromised, leading to their arrest. As with other attacks, it is also true that for the average person, they are simply not a high enough value target to warrant being attacked by a hacker.

Real Dangers:

In practice, there are a few ways in which attackers can use public wifi to gain access to data being transmitted over the network. One attack which is particularly easy for an attacker to perform is the evil twin attack. In the evil twin attack an attacker sets up a public wifi network which mimics another wifi network in the area. The attacker’s goal is to have victims connect to this network and steal, or alter their network activity. So how do they perform the attack? Typically, an attacker will start by finding a popular location that already has a public wifi network. They will take note of the existing Wi-Fi’s SSID and with that SSID use a tool such as a Wi-Fi Pineapple to create a new account under the same SSID. While initially created as a tool for security professionals, attackers can use a Wi-Fi Pineapple to intercept communications over a network. Since most devices can’t differentiate between legitimate and fake connections if they use the same SSID, it is quite possible for a victim’s device to unintentionally connect to the fake network connection. After the connection is made an attacker might push a pop-up typical of public networks to the device, possibly asking for login credentials. Alternatively, an attacker can then monitor network traffic or even boot users off of the network with a DDoS attack. While most network traffic is now encrypted using HTTPS, an attacker could still see victim’s metadata, including what sites a user is connected to or how much data is being sent.

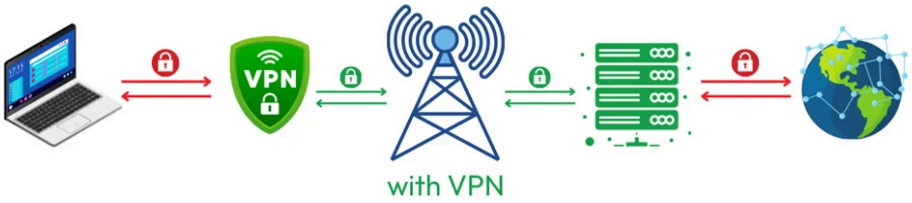
While the damage from evil twin attacks can largely be mitigated through the use of end-to-end encryption, attacks that target a network’s management interface can be quite harmful. One way an attacker can gain access to a network’s management interface is through a password cracking attack. These are typically performed through brute-forcing a large number of combinations of usernames and passwords. While trying every possible username and password could take unfathomable amounts of time, there are common username and password lists which can be used to make this process more efficient. Wi-Fi networks which retain their original usernames and passwords can be especially vulnerable to this attack. If an attacker gains access to a networks management interface they can change network settings, possibly restricting access to the network, they can monitor or redirect traffic, they can install backdoors to possibly retain access to the network if the interface’s username and password are changed, or even configure a rogue DNS which could lead to phishing or malware infections. For a public network, a password cracking attack is not attempting to gain access to the network, it is trying to gain access to the management interface which controls the network.

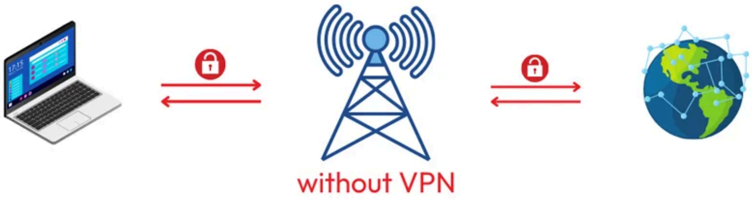
A real example of a public Wi-Fi attack is the Darkhotel attacks. In 2012 the FBI released information on these AiTM attacks, which seem to date back to 2007, occurring primarily in luxury Asian hotels. Though details of exactly how the attack was performed are limited, it is believed that the attackers started by gaining physical access to the wifi routers, either directly or through hotel staff cooperation. Then, once a high level business executive would come to stay in the hotel and connect to its Wi-Fi the attackers would use the now modified Wi-Fi network to trigger what would appear to be a routine software update for legitimate software the victim already had installed. The group used highly advanced Flash zero-day exploits, essentially a vulnerability in the Adobe Flash Player which was unknown to vendors or antivirus software, to trigger this fake update. In actuality, this update would install spyware on the computers of the targeted business executives, allowing the attackers to gain access to sensitive company data. Interestingly, the attackers were quite cautious and implemented a number of measures to dampen any suspicion of a hack. They designed the spyware such that it waited 180 days before sending any information back to the attackers. Additionally, the program was made to self-destruct if the system’s language was turned to Korean.

What about a VPN?

VPN’s are often touted as the solution to all of these problems. Large sponsorships, ads, and “help” articles written by VPN companies assure you that any web browsing puts you at a serious risk of being hacked unless you buy *their* product. To understand how true this is, we need to understand what it is that a VPN actually does (and doesn’t do).

A VPN, or virtual private network, creates a secure network for you to access the internet. Typically, this means that a VPN will encrypt your data before it leaves your computer. Then your data is sent to the VPN server, who forwards it to the website you wanted to visit all along. The process goes in reverse to get the response from the website back to your computer. This means that someone listening to your network traffic can see you access your VPN, but nothing else.

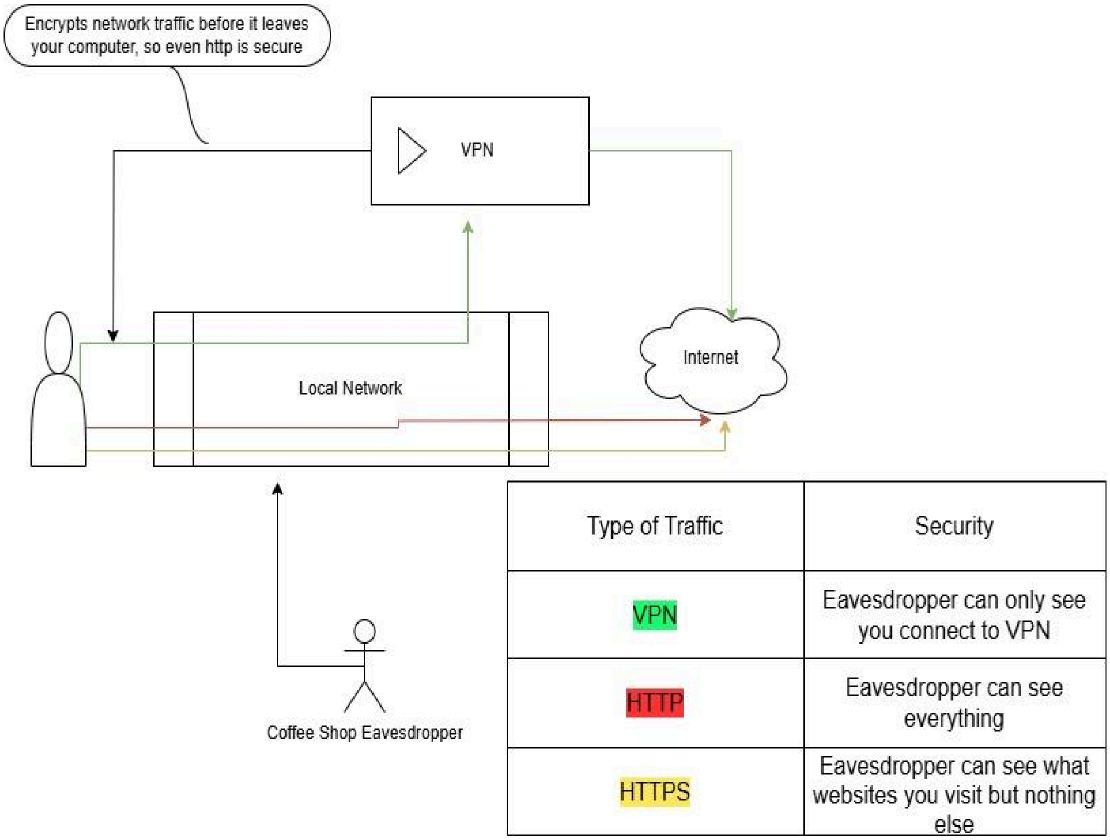




The red padlocks in the above diagram are slightly misleading, as we will get into, but for now you can interpret them as meaning that someone can see you visiting a particular website/server.

A common claim that VPN companies make (as in the above picture) is, if you don't use a VPN, your web traffic is unencrypted. Thankfully, this is mostly not true. If you have ever typed out a URL by hand (a process becoming more and more uncommon every day) you may have noticed some urls starting with "https://…." while others start with "http://….". HTTP and HTTPS stand for HyperText Transfer Protocol and Hypertext Transfer Protocol Secure respectively. They are both web protocols, that is, a language for a client (e.g. your computer) to talk to a web server (e.g. amazon.com).

The major difference between the two is that when your computer makes a request to a web server using HTTPS, the communication is encrypted using Transport Layer Security (TLS). The upshot of this is that your web traffic (when using HTTPS) is encrypted. That is, someone listening could not see what information you are sending to or requesting from the website. For information like your passwords or banking information this is a good thing. If you are visiting a website using HTTPS then your data is encrypted regardless of if you are using a VPN.


Encrypts network traffic before it leaves your computer, so even http is secure
VPN
Internet
Local Network
Coffee Shop Eavesdropper

Type of Traffic	Security
VPN	Eavesdropper can only see you connect to VPN
HTTP	Eavesdropper can see everything
HTTPS	Eavesdropper can see what websites you visit but nothing else

Does this mean that a VPN does nothing? Definitely not. Although HTTPS protects the data you send back and forth, it cannot protect all of the metadata. Information like what website you are visiting or what IP address you are communicating with are not protected. With a VPN, you connect first to VPN and the VPN connects you to the website you want to visit. If someone were to look at your network traffic, they would only see that you are connecting to the VPN, not which website.

To decide if a VPN is necessary for you, there are a couple of factors to consider. 1) how likely are you to connect to a website using HTTP, 2) what kinds of information are you sending across, and do you care if someone knows what website you visit, 3) how likely is it for someone to listen to your traffic.

Given that almost 90% of websites, and all major websites, use https by default, it is very unlikely that you are going to be connecting to a website (particularly one that you would send sensitive information to) via HTTP. This makes sitting in a cafe on the free wifi, waiting for someone to send some sensitive information across, an unattractive proposition for a would-be attacker. Someone who really wants to get your information is much more likely to attempt a phishing campaign or something else that would require less effort and have a higher chance of success. VPNs have their uses, but you aren’t likely to be hacked because you didn’t use one on free wifi. If you are regularly logging into sensitive accounts from public wifi over http connections, or are at particular risk of being targeted by hackers, a VPN may be worth considering. If you are going to use a VPN, it is also worth considering the two main categories of VPNs. The ones you pay for with money, and the ones you pay for with your information. Although some VPNs might claim to be free, they sustain this business model by selling aggregated information about users. Fortunately, just about anyone who deals with enough sensitive information to make a VPN necessary is provided one by their job.

What does this mean for me?

Although public wifi does have some real dangers, most people expose themselves to far greater risks of being hacked by reusing passwords or not updating their software when prompted. Some of the stigma around public wifi can certainly be attributed to the early internet, before the advent of HTTPS. The last 20 years have seen a considerable increase in security considerations, making the default behavior for most websites relatively secure. Hopefully this gives you some insight into how network traffic works and assuages some concerns about using public wifi. Could you be hacked? Yes. Will you be hacked? No.

References:

https://www.reddit.com/r/hacking/comments/qmj7bm/what_is_exactly_is_hackable_from_a_shared_public
https://www.aura.com/learn/dangers-of-public-wi-fi
https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know
https://www.linkedin.com/pulse/public-wifi-insecurity-myth-reality-ts-dr-suresh/
https://securelist.com/the-darkhotel-apt/66779/
https://www.kaspersky.com/blog/darkhotel-apt/6613/
https://www.theguardian.com/technology/2014/nov/10/hotel-wi-fi-infected-business-travellers-asia-kaspersky
https://www.washingtonpost.com/technology/2022/09/26/public-wifi-privacy/
https://techspective.net/2021/09/10/debunking-wi-fi-security-myths-public-wi-fi-hotspots-are-insecure/#google_vignette
https://www.krackattacks.com/
https://www.okta.com/identity-101/evil-twin-attack/
https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple
https://krebsonsecurity.com/2017/10/what-you-should-know-about-the-krack-wifi-security-weakness/
https://www.sciencedirect.com/topics/computer-science/management-interface
https://w3techs.com/technologies/details/ce-httpsdefault#:~:text=The%20websites%20redirects%20visitors%20to,https%3A%2F%2Fexample.com%2F.&text=80%25%20of%20all%20websites%20now,from%2022.5%25%20five%20years%20ago.