The Dangers of Public WiFi

PROTECT AND DEFEND YOURSELF AGAINST CYBERATTACKS

kajeet.com

Connecting to public, unsecured WiFi connections such as those offered in airports, restaurants, hotels, and retail outlets is dangerous and can compromise your security and expose your personal data.

It can also lead to serious system downtime, reduced efficiency, higher incident response costs, and significant brand and reputation damage. Here we talk about the dangers of public WiFi, common public WiFi attacks, and how to stay safe when you work online.

According to a recent study, global cybercrime is expected to inflict damages of up to $6 trillion in 2021. This figure is expected to grow by 15% every year over the next five years and will cross $10.5 trillion annually by 2025. To put this figure in context, cybercrime causes more damage than natural disasters every year and, according to Cisco, is worth more than the global trade of all major illegal drugs combined.

A recent survey by McAfee found that over 65% of surveyed companies suffered some kind of cyber incident in 2019. System downtimes as a result of breaches and attacks averaged about 18 hours, each at a cost of over $500,000 per incident. Some of the biggest losses and the most serious cyber threats to companies come in the form of IP theft and financial crime, which account for about 75% of cyber losses. In addition to these threats, businesses and individuals face losses in the form of brand damage, lower efficiency, identity theft, stalking, and more. Despite the dangers, however, over 50% of respondents in the McAfee study admitted to not even having an incident response plan in place to handle security breaches.

There are many ways in which your devices or networks can be compromised and vulnerabilities can enter an otherwise secure system.

A lack of worker training and experience, outdated IT protocols, weak incident response plans, poor network management, and poor IT/network leadership can all lead to serious security issues and substantial business and personal losses.

One especially dangerous aspect of security is the use of public WiFi. There are many ways in which using public WiFi can introduce threats to your device or network, but fortunately there are also many relatively straightforward fixes that can mitigate or eliminate these risks.

What Is Public WiFi?

A public WiFi connection is any publicly available connection that allows you to connect to the Internet. These connections are usually free and are typically found in public areas such as airports, malls, restaurants, hotels, and coffee shops. These free WiFi connections are extremely common, and are usually given as a courtesy to guests so that they can stay connected wherever they are. Connecting to them, however, can be very risky, as we discuss below.

Common Risks

Business owners and service providers offer free WiFi connectivity with the belief that they are offering a useful service to their guests and customers, but that goal is not always the reality. Most free public WiFi connections have lax or nonexistent security, leading users to face a set of common risks - which we will now discuss.

Man-in-the-Middle Attacks

This is a form of eavesdropping in which a “man” (or device) in the middle of a connection between your device and the router, service, or website you connect to via free public WiFi intercepts the data transmitted to and from your device. Anything you transmit over the unsecured connection – from photos, contact information, and financial data to logins, passwords, and access permissions is at risk. Man-in-the-middle attacks usually involve snooping or sniffing, and there are cheap, widely available, and easy-to-use devices and software that malicious actors can utilize to perpetrate a man-in-the-middle attack, making it a low-cost and highly common type of attack.

Unsecured Networks

Since public WiFi is usually offered as a free service, the routers used in these networks often have their factory defaults and lack basic encryption. Without encryption, any data you send or receive over the connection can be read by anyone who can intercept or eavesdrop on that data.

Malware

If your device or system has a software vulnerability, a hacker may be able to slip malware or viruses to you over an unsecured connection.

Malware is malicious software that gives an unauthorized user access to a system, device, or network. Malware is commonly used for theft or sabotage, and there are many different types and ways in which malware or other unauthorized programs, files, or data can be introduced into a network (such as through phishing, email attachments, and download links). Social engineering and contaminated devices such as flash drives can also be used to install malware on your system.

There are many types of malware, including:

- **Ransomware**, which prevents a victim from accessing his or her data or systems until a ransom is paid - often with cryptocurrency.
- **Fileless malware**, which affects operating system files that your system will recognize as legitimate.
- **Spyware**, which captures user data like passwords, pins, and personal or financial information without the user's knowledge or consent.
- **Adware**, which tracks a user's browsing activity to determine what kinds of ads to serve them.
- **Trojans**, which disguise themselves as software offering some kind of service or benefit but are actually designed to infect a user's system or device in other ways once installed.
- **Viruses**, which are pieces of code that insert themselves into applications and run when the application is run. Viruses can be used to perform the kinds of malicious activity that many of the examples above perform, such as stealing sensitive data.
- **Rootkits**, which give an attacker remote control of a victim's system with full administrative privileges.
- **Keyloggers** monitor user activity like keystrokes, allowing a hacker to crack your passwords or unlock other sources of private (and valuable) information.

Malicious Hotspots

A malicious hotspot is a rogue connection that tricks victims into thinking that it is a legitimate network. Think of a free WiFi connection at an airport called "Airport_Lounge" that is actually run by a hacker. You may connect to it believing that it is the airport's complimentary WiFi connection, but it is really an illegitimate and dangerous connection.

War Driving

This is a type of exploit that involves driving around neighborhoods to gather unsecured or unencrypted data from wireless networks that are in use in the target area. The information gathered can then be shared online or may be used to target individuals living in the area.

Denial of Service

A Denial of Service (DoS) attack over WiFi occurs when an attacker overwhelms the network you are on, causing your system to crash.

DoS attacks (sometimes called jamming attacks) are of three main types:

- **Constant jamming,** in which a random radio signal is constantly transmitted to prevent legitimate users from accessing a channel and sending data packets. The source of the signal can be easy to detect since its signal does not have a packet structure of its own.
- **Deceptive jamming,** in which an attacker injects regular packets to a system, preventing the system from switching from the receive state and preventing it from transmitting packets of its own.
- **Reactive jamming,** which only starts jamming when the network is active.

A DoS attack is mostly a nuisance, but it is another danger of connecting to an unsecured WiFi network.

KARMA Attacks

KARMA attacks exploit WiFi weaknesses and a lack of access point authentication to access, control, or deliver malware to target devices connected to the network.

Your Preferred Network List (PNL) is a list of WiFi networks that your device automatically trusts. If your device is not secured, it can broadcast your PNL, along with the SSIDs of access points it previously connected to and may automatically reconnect to. These broadcasts are not encrypted and can be captured by WiFi access points within range.

To perpetrate a KARMA attack, a malicious access point will receive your PNL and give itself an SSID from that list, making it an "evil twin" of an access point that your device already trusts. (Evil twin attacks that work in much the same way as KARMA attacks are a separate yet well-documented type of WiFi network attack.)

WiFi Pineapple

The WiFi Pineapple can be used to perpetrate many of the attacks above. The device was initially built for network auditing and penetration testing, but it provides an easy way for hackers to set up false access points to perform attacks like man-in-the-middle and malicious hotspot attacks.

In this hack, a device connects to the user's system via USB or Ethernet cable and can pose as a wireless access point. Any unprotected traffic of users who connect to the network can be monitored by the hacker.

There are many readily available scripts and apps that work on the Pineapple, and hackers can use these plug-n-play applications to steal a variety of information from unsuspecting users. It has an easy-to-use web-based interface that even novice hackers can use, and there are many websites that Pineapple owners can use to get started with hacking without any prior hacking knowledge. The device is cheap as well - some models are available for less than $100.

Staying Safe on Public WiFi

As a rule of thumb, the best thing to do to avoid unsafe public WiFi issues is to avoid using public WiFi altogether. However, if you must connect to a network, do the following.

- **Update your Preferred Network List.** Hackers can create rogue access points with the same name or network IDs that your device trusts, so you should delete (have your device "forget") WiFi networks you do not regularly access or need to access.
- **Never use hidden networks.** Normal WiFi access points send beacons containing the information that nearby devices need to discover and connect to the network, such as the network SSID and the type of encryption it supports. Hidden networks do not do this, instead requiring the user to have prior knowledge about the network. If you have devices that are configured to connect to a trusted hidden network of your own, those devices will constantly call out the name of the network you hid, making the network an open target for anyone who can capture those beacon transmissions.
- **Isolate users to their own subnets.** Many small businesses who offer WiFi to their customers may make the potentially costly mistake of failing to restrict guests to their own subnet. With proper subnet isolation, each user should only be able to communicate with the router, and will not be able to scan other devices on the network or connect to any open ports.
- **Disable file sharing.** Files may be automatically sent and received if you have file sharing on, and a hacker could try to upload malicious data or code to your system via a file or application that your system would accept via open file sharing.
- **Only visit sites that use HTTPS and only use SSL connections.** Sites that use HTTP can be unsafe, so making it a rule to only visit HTTPS or SSL sites reduces your chances of being attacked.
- **Make sure to log out of your accounts** when you are done using them.
- **Use a VPN** so that your WiFi connection, even if it is unsecured, is private. We cover more about VPNs and how they work in the next section.
- **Do not allow your system or device to automatically connect** to any networks.
- **Avoid using sites that require the input of sensitive information**, such as your banking webpage, while on public or unsecured WiFi networks.
- **Purchase or enable a firewall** and turn on network encryption in your network settings.

More On VPNs

Virtual Private Networks (VPNs) provide two key benefits.

The first is privacy, as a VPN hides and prevents many different types of data (such as your IP address and search history) from being tracked or recorded by websites you visit and other unauthorized devices or systems.

Secondly, VPNs can protect your data while it is in transit. Your VPN provider creates a secure tunnel through which you connect to the Internet, and the data that you send or receive via this tunnel will be encrypted and secured from unauthorized and/or malicious access.

VPNs offer many benefits, including the following:

Escape data and bandwidth-throttling: Your Internet Service Provider (ISP) can slow your service or limit your access to bandwidth once you have used a certain amount of your data, but a VPN will shield you from your ISP and can save you from data caps (although your VPN provider may have caps of their own).

Access blocked services and avoid censorship: VPNs can be used to provide access to geo-blocked content and avoid censorship by hiding your IP address and/or changing it to an address that is allowed access or is not blacklisted/censored.

Reduce support costs: With the right VPN solution in place, you can reduce the downtime associated with security breaches and the expenses associated with 3rd-party security and maintenance.

Despite these benefits, it is important to understand what a VPN does not do. A VPN will not completely anonymize your traffic, and many websites that you visit using a VPN can still track you using cookies, online trackers, malicious/ unauthorized downloads, and a host of other tricky tools.

In summary, using a VPN does not mean you can forget about other security basics. Even though some VPN services can block a variety of malware, you should still exercise caution when connecting to or consuming online content and be smart about creating passwords, maintaining your system, and avoiding suspicious sites and links.

Understanding WEP vs. WPA vs. WPA2

Wireless Equivalent Privacy (WEP) was an early security algorithm for wireless networks that aimed to provide data confidentiality comparable to that of a traditional wired network, but it proved to be easy to crack.

WiFi Protected Access (WPA) was developed to replace the vulnerabilities of the WEP standard. It came with better security and encryption and included message integrity checks to determine whether an attacker had captured or altered packets that were transmitted between an access point and a user. It also implemented a per-packet key system called the Temporal Key Integrity Protocol (TKIP) that was far safer than the fixed key system used by WEP. The TKIP, however, recycled certain elements that were used in the WEP system (to make it easier to roll out to existing WEP systems) that were ultimately exploited as well.

WiFi Protected Access II (WPA2) was officially implemented in 2006, and replaces TKIP with even more advanced protocols such as AES algorithms and Block Chaining Message Authentication Code Protocols. It is the safest protocol of the three.

If your WiFi connection uses WPA2, it will be more secure than connections that use WEP or WPA, but using WPA2 is more costly for the provider of the wireless network and does not inherently protect anything of value of the provider - which explains why many public access WiFi providers may be unwilling to pay for it. Furthermore, to connect to such networks, the passphrase is often publicly provided, so anyone with the passphrase and a device SSID can decrypt traffic on the network if they can capture the initial 4-way handshake used to establish a secure connection to a network.

Additional Steps

In addition to the above, there are certain things you can do – and should make a habit of – to lower the chances that you will suffer an attack or breach on a public WiFi connection.

- Be aware that public WiFi is inherently insecure, so exercise caution in everything you do online and treat all WiFi links with a healthy amount of suspicion.
- Remember that any device can be at risk.
- Avoid using default passwords and easy-to-guess passwords.
- Do not let your device announce its presence. By switching off your service set identified (SSID), your wireless device will not announce that it is online and will be less likely to be found on a network. You should also change your device's name from the manufacturer's default.
- Use your mobile phone instead of a WiFi connection on your laptop or use your mobile phone as a hotspot. It may be worthwhile to invest in an unlimited data plan so that you never have to resort to unsecured public WiFi.
- If you run a business, it may be worthwhile to invest in a PLTE (Private LTE) network in which you own and/or control or enjoy some level of preferential treatment with respect to bandwidth from your carrier. This can permanently eradicate the need for public WiFi and you and your teams can enjoy fast, secure, and cost-effective connectivity wherever you may be.

Final Thoughts

When it comes to network and device security, there is no substitute for robust and comprehensive IT policies that protect your devices, networks, systems, services, and teams from malicious attacks. From designing and deploying a safe and secure network and maintaining your infrastructure to training teams on how to be safe and investing in better connectivity, there is a lot that you can do to prevent the attacks that too many people fall prey to on public WiFi connections. The good news is that these solutions are easy to deploy and can be tailored to your specific needs. They can even prevent the incidental attacks that are bound to otherwise occur, such as social attacks or system vulnerabilities introduced by human error.

A Kajeet Solutions Specialist can help you design and deploy a managed IoT solution that is tailor-made for your needs and is secure across your entire network surface.

Visit us at kajeet.net/contact-us/ to learn more.