HJIA
Member, H.C. Murray Group

How to Avoid Public Wi-Fi Security Risks

People who use public connections may be compromised by hackers, but there are several safeguards available to save you from becoming a victim.

The recent availability of free Wi-Fi has been a great benefit for businesses and consumers alike, and there are free connections in almost any hotel, restaurant, or coffee-shop. Since no authentication is required to establish a connection to a free network, hackers have an easier time stealing data. Hackers position themselves between a person with an unsecured deice and the connection point, which means that the device's information is sent to the hacker instead of the hotspot. Emails, search requests, and credit card information are just a few examples of information that may be sent. With this information, a hacker may be able to access even more of the user's personal information.

Many hackers also use unsecured connections to send out malware. For those who allow sharing, it is easy to be infected by malware. Some hackers target the connection point, which creates a popup window while the computer is connecting. It offers a "free upgrade" for a certain type of program that most people use, and clicking on the fake offer automatically installs the malware. It is very easy to fall for this trick. As public Wi-Fi becomes more common, expect to see hackers step up their game. Security issues for free Wi-Fi networks will continue to increase, but this does not mean that people shouldn't use *any* free connections. It is simply a reminder of the available safeguards and the importance of using them.

Always use a VPN. A virtual private network serves as a buffer between the Wi-Fi connection and the mobile device or computer. Any transmitted data is then encrypted and becomes too much work for the hacker to attempt to figure out. Use a trusted and reputable VPN provider. While some providers charge a fee of around $10 or more for monthly service, others are free.

Use SSL connections. Although most people are not as prone to use a VPN, they can easily add encryption to communications by enabling the "**always use HTTPS**" feature on their computers or mobile devices. This ensures a secure connection to sites, and it is vital for any site where financial credentials are entered.

Turn off automatic Wi-Fi when it is not in use. When a phone is not connected to Wi-Fi, an automatic search will still transmit some data while looking for available networks. To stay safe, disable Wi-Fi after you are done using it.

Turn off sharing capabilities. Access the control panel on your device to do this. Allowing sharing will give people who have the ability to use it access to information and data on your device.

Issues may still arise even with the best safeguards in place. Taking the above-mentioned precautions, however, will help reduce the likelihood or frequency of security breaches. Be vigilant! We will continue to do our best to keep you up-to-date on the best ways to avoid public Wi-Fi security risks.