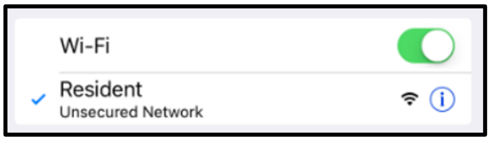
RESIDENT WI-FI SECURITY

inviacom
innovative wireless communications

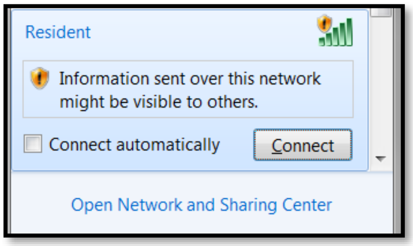
UNSECURED NETWORK?

Each time you connect to the Resident Wi-Fi at your community, you may see a prompt that says you are connecting to an ***"Unsecure Wi-Fi Network"***. Why is that? The Inviacom BlanketWiFi℠ is secured in a ***different*** manner than a traditional Home Wi-Fi system.



Wi-Fi

✓ Resident
Unsecured Network



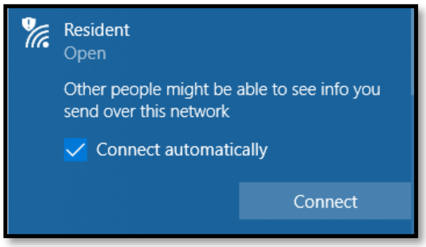
Resident

Information sent over this network might be visible to others.

□ Connect automatically

Connect

Open Network and Sharing Center

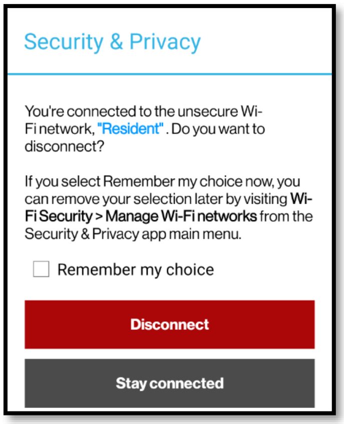


Resident
Open

Other people might be able to see info you send over this network

☑ Connect automatically

Connect



Security & Privacy

You're connected to the unsecure Wi-Fi network, "Resident" . Do you want to disconnect?

If you select Remember my choice now, you can remove your selection later by visiting **Wi-Fi Security > Manage Wi-Fi networks** from the Security & Privacy app main menu.

□ Remember my choice

Disconnect

Stay connected

Here's a brief summary of the differences between the Inviacom BlanketWiFi℠ and a traditional Home Wi-Fi system.

TYPICAL HOME WI-FI

Traditional Home Wi-Fi systems typically utilize WPA/WPA2 Security Protocols. These WPA-secured networks require one single password to access the network. Once this password is entered into the system, all devices are connected to the same network and are therefore "visible" to all other devices on the network. This is not ideal for a network which hosts hundreds (or thousands) of devices in multiple homes.

INVIACOM BLANKETWIFI℠

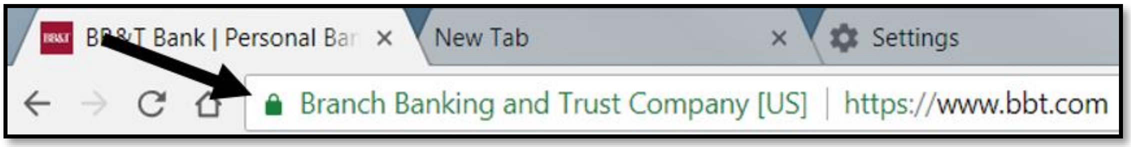
Inviacom BlanketWiFi℠ is capable of handling thousands of devices spread out over multiple access points across campus. In these scenarios, traditional WPA/WPA2 security is not good enough for our users. Instead of one password for all devices, each user is provided a separate username and password to access the network. Once these credentials are entered, the Inviacom network creates a Private Network for all devices authenticated.

This allows Inviacom to keep the network both simple and secure for all devices, while simultaneously allowing users to utilize peer-to-peer functionality such as wireless printing. Your printer will only be visible to your devices and will be segmented from other users on the network. **Keep in mind that all wireless security is local only**, meaning that both WPA and Inviacom's BlanketWiFi℠ security are in place to secure devices on the local network, not the Internet.

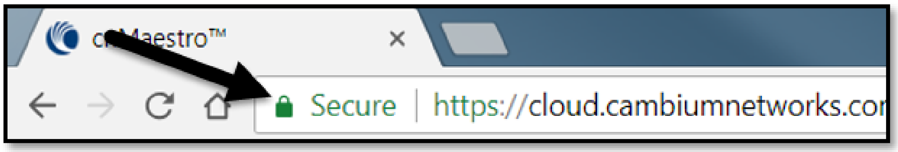
OTHER ONLINE SECURITY STEPS TO TAKE

Once your data leaves the property and enters the Internet, it is out of the hands of Inviacom. You are responsible for securing personal devices on the Internet. Please ensure that your devices are utilizing antivirus, spyware, and malware protection. Many newer devices have this protection enabled by default. The methods will vary based on manufacturer and operating system. Inviacom also recommends using an ad-blocker while browsing the Internet.

WHAT IS THIS LOCK ON MY WEBPAGES?



This is what is known as **SSL Encryption**. Most websites use this, especially sites that hold sensitive data such as bank accounts and email addresses. It is very important to ensure that this lock is enabled and matches the company of the site you are visiting. This will ensure that all data sent to the server is fully encrypted.



WHAT ELSE CAN I DO?

Another method to secure Internet traffic is to use a Virtual Private Network (VPN) service. This will encrypt **all** traffic between your device and the remote server. There are many paid VPN services available. *NordVPN* and *PrivateInternetAccess* are two reputable VPNs that are widely known to be great at securing Internet traffic. Please visit their respective websites for more details. The downside to using a VPN is that you will likely experience slower speeds on downloads and web browsing. This is because all of your Internet traffic is routed through the VPN.