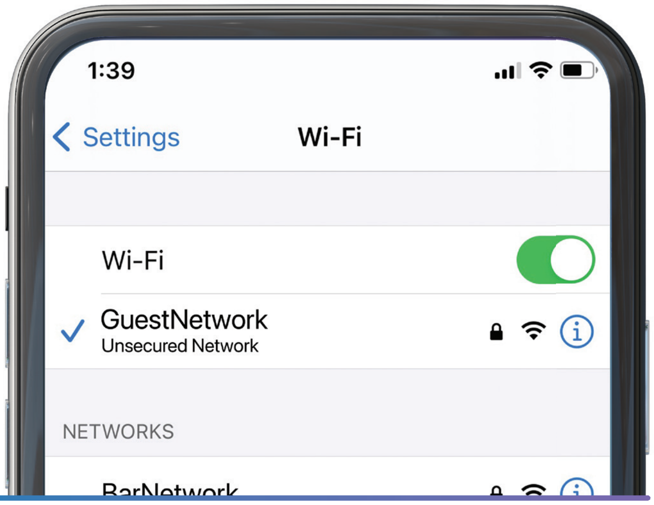
Shaw) Business

WIRELESS NETWORK SECURITY IN A SHAW BUSINESS MANAGED PUBLIC NETWORK.

UNSECURED NETWORK

Many devices warn users that they are connecting to a “Unsecured Network” if the wireless network does not require a WPA2 wireless network password. This is a common occurrence when users are connecting to wireless networks in public areas like hotels, multi-tenant facilities, airports and coffee shops, since these networks do not usually use a WPA2 password. **However, this does not mean that the wireless network is not secure**.

Explore frequently asked questions relating to the security protection of a public Shaw Business managed wireless network.



WHY IS THE WIRELESS NETWORK CONSIDERED “UNSECURE” BY A USER’S DEVICE (IE: CELL PHONES, TABLETS, ETC.)?

In most cases, mobile devices “expect” users to connect to an encrypted wireless network and will warn users whenever they attempt to connect to a network that does not seem encrypted **regardless of any other security features configured on that network**.

The vast majority of public networks work without encryption to ensure that even older client devices can connect. Furthermore, wireless encryption usually works with a common key that all users must know before being able to connect to the network. Devices consider that an encrypted network is “safe” as soon as a key is required to connect. In reality, the network is only encrypted for devices that do not have the key; but any device connected to the network has the key and can decrypt or “see” all the traffic on that network. This makes sense in a home or office network where only a limited number of trusted users have access to the key but does not make sense in a public network (like a hotel or multi-tenant facility) where hundreds of users all use the same key all the time.

IS MY SHAW BUSINESS MANAGED WIFI NETWORK SECURE?

Yes. Even though most hotel and multi-tenant networks do not use wireless encryption, Shaw Business provides robust security for all users connected to the WiFi network. The following security protection measures are in place:

1. The network is configured to isolate devices from one another. Each device can connect to the Internet, but they cannot see the other devices on the network. This prevents the exchange of viruses and direct hacking within the wireless network.
2. An enterprise-grade firewall is installed which controls access between the Internet and the wireless network, preventing Internet-based devices from accessing devices connected to the wireless network.
3. Guest/resident devices are prevented from communicating with corporate devices, like front desk computers, servers, etc.
4. Internet access requires either a different passcode per user (guest/resident/employee) or unique login using last name/ room number, which limits access to the network to authorized users only.

HOW CAN WIRELESS NETWORK USERS MAKE SURE THEIR CONNECTION IS SECURE?

Even with the wireless encryption provided by a WPA2 key, typical networks allow devices sharing the same key to communicate with one another. This is not the case with a Shaw managed wireless network; each user device is isolated from one another regardless of whether a WPA key is used or not. This network client isolation feature is a big step in securing the network. Regardless, wireless network users should always exercise caution when sharing sensitive information over any network, especially public ones. They can do so by:

1. Only communicating sensitive information when connected to secure HTTPS websites that they trust and/or when connected to an encrypted virtual private network (VPN).
2. Having an up-to-date personal firewall and anti-virus on each device they use.
3. Ensuring their operating system and browsers are up to date: many users do not install updates which can correct security flaws that are regularly discovered in software such as operating systems and browsers.

IS A WIRELESS ENCRYPTION PASSWORD (WPA2 KEY) THE SAME AS THE “WIRELESS CODE” THAT IS USED TO ACCESS THE WIRELESS NETWORK?

No. The “wireless code” that is provided to authorized users controls whether a device can access the Internet, but it does not provide any encryption. The “wireless code” can be different for each user, while a WPA2 key is usually the same for all users. WPA2 keys only controls access to the wireless network itself, not access to the Internet.

Many Shaw Business managed wireless networks at hotels now use PMS login (last name/room number) instead of the “wireless code”; this works in a similar fashion to and does not encrypt traffic either.

WHAT IS HTTPS?

HTTPS is a secured or encrypted version of the HTTP protocol used to display webpages. Many of today’s websites, including Google and Facebook use HTTPS for most of their data exchange to ensure data privacy, even when connecting from unsecure networks. Banks have been using HTTPS for years to protect user data. Even if a user’s device is connected to an unencrypted network, any information sent through an HTTPS website is encrypted and therefore “invisible” to all other users on the network they are connected to and on the Internet. Most Internet browsers now clearly indicate whether you are connected to a website encrypted in HTTPS.

WHAT IS WPA OR WPA2?

WPA is the common term used to describe the WPA and WPA2 wireless security protocols, which are used to encrypt data over wireless networks. A WPA2 password must be at least 8 characters long but can be as long as 63. For WPA2 to be considered secure, most security specialists recommend that it is **at least** 12 characters long, completely random and not based on any word or phrase. This is one of the reasons why using a WPA2 password in a hotel or multitenant network is cumbersome: for it to be effective, it needs to be a complex string that many users will have a hard time entering on their mobile device.

WHY ISN’T WPA ENCRYPTION ENABLED ON THE SHAW BUSINESS MANAGED WIRELESS NETWORK?

Certain older devices cannot connect to networks configured with WPA encryption.

Most major hotel brands do not recommend using WPA encrypted networks for guest WiFi. Enabling WPA could prevent certain user devices from connecting to the network altogether. Furthermore, it can be complex/difficult to change the WPA key on a regular basis across the entire network. If the key is changed, all devices that are connected will instantly lose access and must enter the new key before being able to access the network again. In most networks, all users share the exact same key, if the key would happen to be known, anyone who has it in his possession could connect to the network. If unauthorized users learn the WPA2 password, the security offered by the WPA2 key becomes almost useless.