MyHomeWorks

Tips to Make Your Connected Home Secure

Could your Connected Home be hacked and taken over? The answer is a resounding YES!

How can you make sure that this does not happen to you? There are a few basic steps that every homeowner can and should take to improve their home security.

Change the 'default' password: All routers/firewalls come with a preset 'default' password. These passwords are well known and well documented. Change each admin password to a strong complex password. Use upper and lowercase characters. Including at least one 'special' character will help ensure that brute-force cracking will be harder to do. In addition to the password, if possible, you should also change any default usernames. This is the top recommendation on just about every security list.

Disable guest access: Allowing guests to access your home network may seem like a nice convenient thing to do however, you should be very wary about allowing any "non-authenticated" users to access your network.

Change the 'default' network name: Home routers/firewalls often set the default SSID to something that describes the specific hardware i.e., (Linksys). From a hackers perspective, knowing the specific hardware platform that you're attacking makes the job easier. Use a random, innocuous name. Also, do not use any personally identifiable information in the name (i.e., "Smith Family"). In addition to changing the network name, another more advanced measure would include 'hiding' or not broadcasting the SSID.

Use the WPA2 to secure the network: The older WEP protocol has serious weaknesses and is easily compromised. While WPA2 isn't infallible, it does provide a higher level of security and is significantly harder to compromise.

Firewall everything: Set your router/firewall to restrict all incoming connections. Only open ports that are specifically needed for a device.

Setup a 2nd Wi-Fi network: If your router supports it, setup a 2nd Wi-Fi network specifically for home automation devices. Separating the two networks will ensure that if a home automation device gets compromised it will not jeopardize your primary network.

Disable remote management: If you do not plan to manage your router/firewall remotely then you should disable remote-management access.

Once the Wi-Fi network is secured, take a look at each home automation device. Securing specific devices will depend on the individual capabilities of each specific device. At a minimum, the approach should include the following.

Generic email: If the device has the capability to notify you via email, setup a generic email account. Do not use your personal email account or email server.

Mobile security: Install mobile security software on the devices used to control the home automation devices (i.e.; mobile phone). It is often easier to exploit a mobile application instead of hacking the device directly.

Patching and updating firmware: Check for firmware updates on a regular basis and install updates as soon as possible.

Internet access: If the home automation device doesn't need access to the internet, disable its access within your firewall.

What is the industry doing to enhance security?
Devices are more and more frequently being manufactured with Pin codes, two-factor authentication, data encryption and sandboxing in an effort to prevent hackers from breaking into devices.