

Staying Safe on The Internet of Things (IoT)

What is IoT?

IoT, or the Internet of Things, encompasses a diverse range of devices that connect to the internet, including your mobile phone. This could be anything from your car radio to your Bluetooth headset to your refrigerator! These devices are handy, but they come with their own set of security risks. Keep New Hampshire safe by understanding those risks and doing your part to reduce them.

What are the risks?

IoT devices, when connected to the internet, open a virtual "window" into your home network. Unless these devices are properly secured, threat actors can exploit the vulnerability this virtual "window" presents to gain access to your network.



The IoT Security Pathway for Home Devices

1 Evaluate

Does this device actually require an internet connection?

- ✓ Yes—Move to Step 2
- ✗ No—Consider whether or not you want to take on the risk associated with an IoT-connected device.

2 Secure

Remove unnecessary accounts if the device has them.

Admin and Guest are common and unnecessary.

Change the default password.

Many default admin passwords for IoT devices are publicly available online. By changing this to a secure passphrase of your choosing, you make it much more difficult for a threat actor to exploit the device.

3 Connect

Connect to a segment of your network devoted to IoT devices.

Most in-home Wi-Fi routers let you segment your network for specific functions. If you segment your network properly, it will act like several networks that don't interface with one another but do connect to the internet. As such, if a threat actor gains access to one segment, it is less likely they will be able to access others.

There are numerous helpful instructional materials and videos available online that provide guidance on how to do this. Most ISPs (Internet Service Providers) are also more than happy to help you set this up.

4 Patch

Ensure that you patch connected devices regularly.

Install any available patches as soon as you set up your IoT devices, and continue to check for new updates on a regular basis.

In some cases, you can set devices to automatically download and apply security patches, but not always. In any case, you should manually check for security updates to the software for your connected devices on a monthly basis.